ID: 435310
Sample Name: DOC0798.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:57:41
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

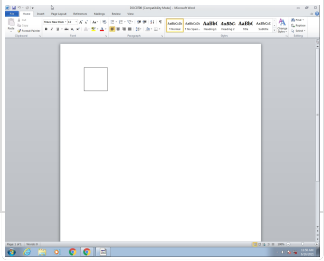
Windows Analysis Report DOC0798.doc

Overview

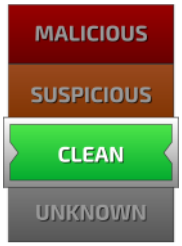
General Information

Sample Name:	DOC0798.doc
Analysis ID:	435310
MD5:	51a19560ad005f1.
SHA1:	660adab2960c1e..
SHA256:	00175c704e4d53..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

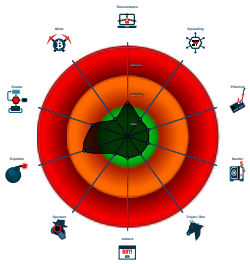


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- May sleep (evasive loops) to hinder …
- Office Equation Editor has been star…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2596 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2628 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- EQNEDT32.EXE (PID: 912 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

No Sigma rule has matched

Signature Overview

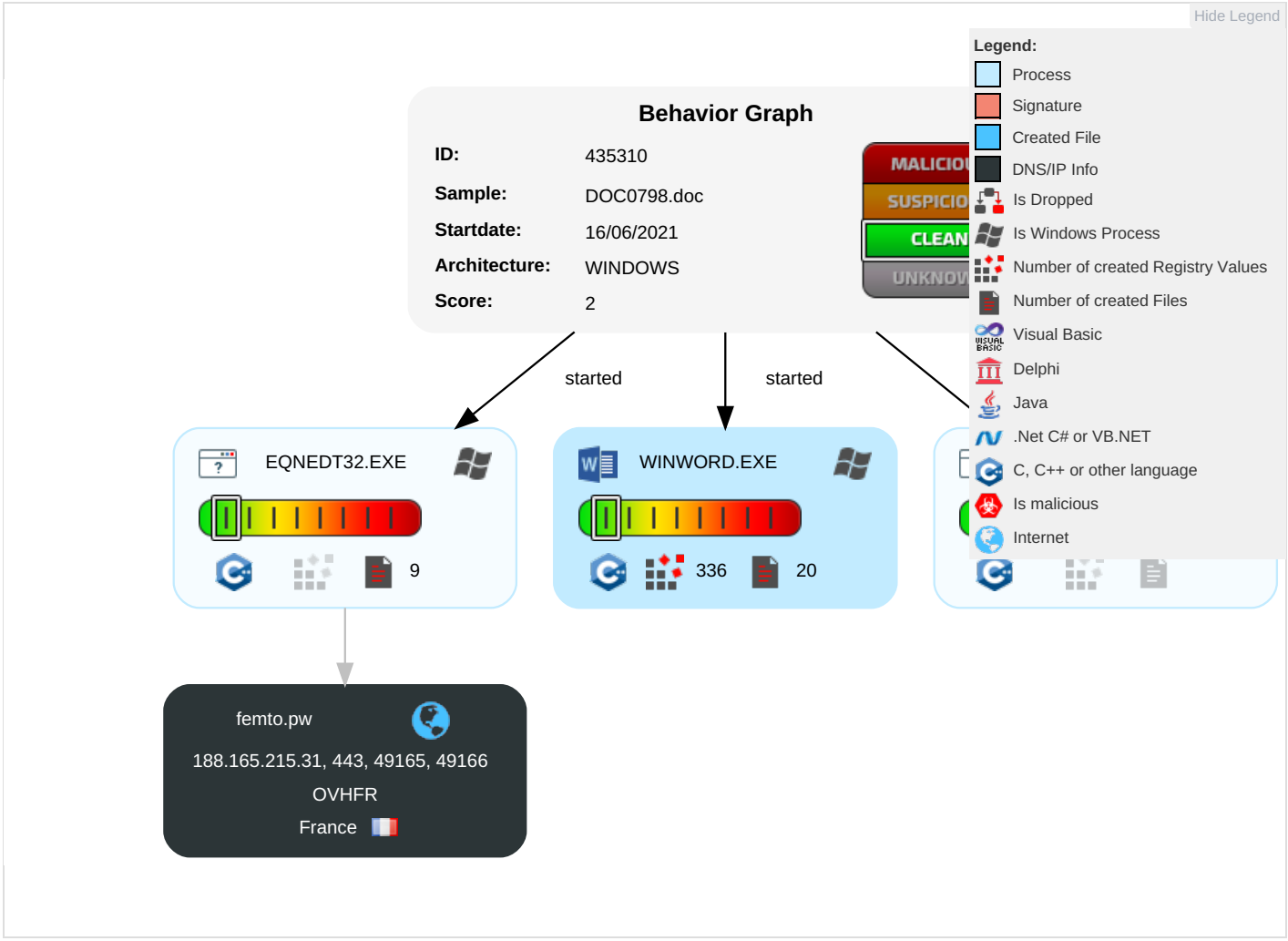
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Exploitation for Client Execution 3	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotel Track D Without Authoriz
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotel Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

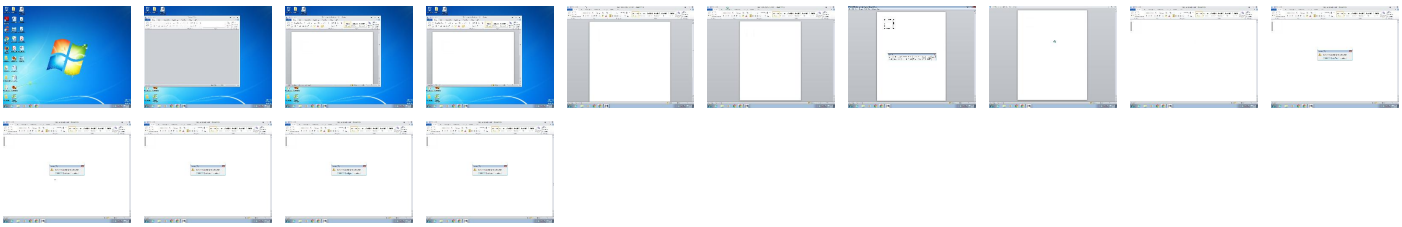
Behavior Graph

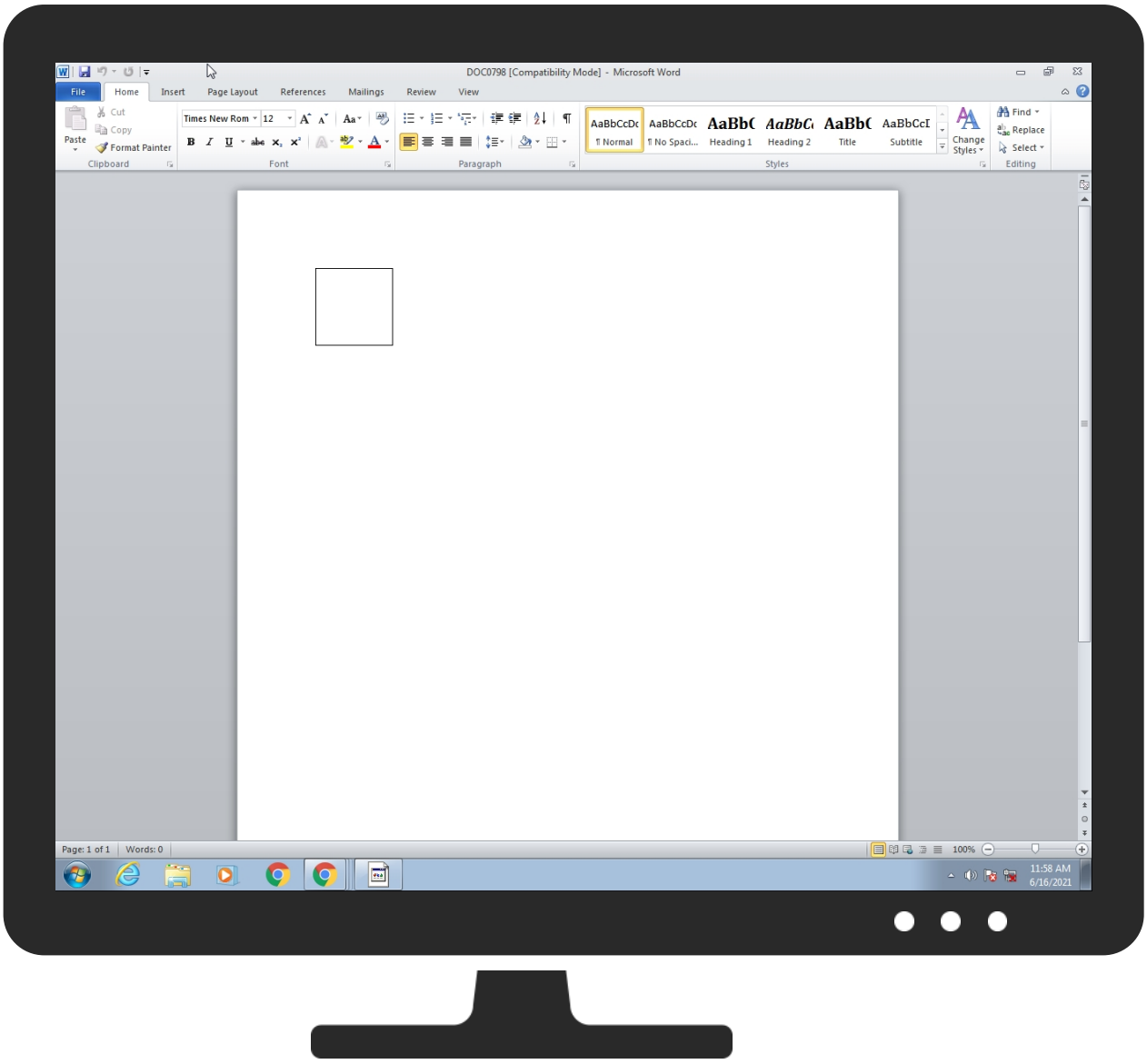


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
femto.pw	188.165.215.31	true	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.165.215.31	femto.pw	France		16276	OVHFR	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435310
Start date:	16.06.2021
Start time:	11:57:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DOC0798.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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.winDOC@3/6@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:58:34	API Interceptor	246x 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
OVHFR	jqJ9rVHXq0LCZ6R.exe	Get hash	malicious	Browse	• 54.36.120.230
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 198.245.49.191
	RFQ Products.xlsx	Get hash	malicious	Browse	• 167.114.158.9
	DocumentCopy_pdf.exe	Get hash	malicious	Browse	• 213.186.33.5
	Proforma Invoice & Bank Swift Copy.exe	Get hash	malicious	Browse	• 51.79.149.34
	Profoma Invoice1506021.exe	Get hash	malicious	Browse	• 158.69.138.23
	kkaH2ZEdQ1.exe	Get hash	malicious	Browse	• 213.186.33.5
	LDOsa1uqyb.exe	Get hash	malicious	Browse	• 176.31.56.216
	Quotation.exe	Get hash	malicious	Browse	• 192.99.208.14
	LSMD.exe	Get hash	malicious	Browse	• 37.187.95.110
	IHdviiaZ7h.exe	Get hash	malicious	Browse	• 51.195.61.169
	7#U1d05.html	Get hash	malicious	Browse	• 51.89.21.20
	03soKqWLfN.exe	Get hash	malicious	Browse	• 51.89.96.41
	bpkuoAqilk.exe	Get hash	malicious	Browse	• 176.31.95.228
	Wire_receipt.exe	Get hash	malicious	Browse	• 5.135.115.129
	Shipping Doc578.exe	Get hash	malicious	Browse	• 213.186.33.5
	URGENT REQUEST FOR QUOTATION (RFQ REF R 2100131410).exe	Get hash	malicious	Browse	• 51.91.236.193
	Reference No. # 3200025006.exe	Get hash	malicious	Browse	• 213.186.33.5
	Cancellation_Letter_2137859823_06112021.xlsm	Get hash	malicious	Browse	• 51.254.164.254
	Cancellation_Letter_2137859823_06112021.xlsm	Get hash	malicious	Browse	• 51.254.164.254

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6899A86A-6F93-4194-97B0-E6749671AC21}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6899A86A-6F93-4194-97B0-E6749671AC21}.tmp	
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E42C9A4D-C73B-45F3-859A-E103BFD96442}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.8014421130618178
Encrypted:	false
SSDEEP:	3:gl2lfgREqAWlglqlg7tlNl7lY2l/Dlll8v0lglwZbvt3UlglwZel8gl7vll8:zNgREqAWlgFJMSDlll8vlwBZFwQFrB
MD5:	D70B341E158CD3F9AF4E8246EA1FB74B
SHA1:	E07659B1ABDC722BF44A78BF03342D86C1B2DDFE
SHA-256:	CEC933B996CAF6ABE607DD8E4E4F304D81C0B8D19F95151C67C5B670B7830639
SHA-512:	A6906A6FA406C73A4A98BA680A753FB7D572559B1F611C6EAF5E673F3C2981E78F5F04A0AB1B060496BFCDBC3DE2D595DDFCC01B155916105C2EF67100005A5
Malicious:	false
Reputation:	low
Preview:	=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....j....CJ..OJ..QJ..U..^J..aJ.. .j.etd...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\DOC0798.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Wed Jun 16 17:58:32 2021, length=1613819, window=hide
Category:	dropped
Size (bytes):	1994
Entropy (8bit):	4.534337781841879
Encrypted:	false
SSDEEP:	48:83T/XT0jFiHZ3FAo4Qh23T/XT0jFiHZ3FAo4Q/:83T/XojFIZqbQh23T/XojFIZqbQ/
MD5:	CA61F9522E5DA54B48B58DBDF25FDECE
SHA1:	7C57459FA07531DEBAE847109DD9BD9EA9B8C698
SHA-256:	7A1C9267069AA243179BD1EDAE3260321D9726A7F8AE8C698CEBB9B9F11A5C43
SHA-512:	3C250489EC60FA7996892B86FD0FFD7F725677A0B30929F77D772BFEE85752B88EB1C894ED6BAA9054CAF6BFC38E4F741F8944E66BBF19760B744D7C93A380AF
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....q..{....q..{....Q..b.....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.....^.2.....RQ. .DOC0798.doc.D.....Q.y.Q.y*...8.....D.O.C.0.7.9.8...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\571345\Users.user\Desktop\DOC0798.doc."....\....\....\....\....\.D.e.s.k.t.o.p.\.D.O.C.0.7.9.8...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.....571345.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.1702223972093195
Encrypted:	false
SSDEEP:	3:M18iSsd25d4sd2mX18iSsd2v:M+ocfqoI
MD5:	3C8E4AC54FF66878DC3446F616641670
SHA1:	FD8694B9B068C7CBE20128AF8398A92669E869AD
SHA-256:	1D9989644C7811E99A3B44DBB966432BFC35FDC656481E38001C0BF030F7F4BF
SHA-512:	2713B9AEFFDBC95FE7F55369AF848A67F13C0A37D547957BE15FE39D3F2E229149825C07F0BDA8159552D781D04B05B310A3BBFB708EABE2EBDC06B2E4C2928E
Malicious:	false
Reputation:	low
Preview:	[doc]..DOC0798.LNK=0..DOC0798.LNK=0..[doc]..DOC0798.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVysAiJNGlzgYGwg32LbO/ln:vdsCkWthASq+l
MD5:	4CDEC46BF4C5E1435E277CB4821D6306
SHA1:	506F3E77835A2AE504189833D4EF30799A0ACE45
SHA-256:	39A3F2156450758ACBBCB3D8E9461BB4CDD93F41A3EC3A4013F4EB8D2A906537
SHA-512:	7039ED1E181A8368526A65F6F0D2F70E5BCEBD37BB3BFD8E270BB305F405DB0D843B1CAF6E4E05F6CF1D203A8AA326A1316CDDDD085DD59DB15A82A26E6FA75
Malicious:	false
Reputation:	low
Preview:	.user..A.l.b.u.s.............p.......................................P.....................z...............x...

C:\Users\user\Desktop\~$OC0798.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:vrJlaCkWtVysAiJNGlzgYGwg32LbO/ln:vdsCkWthASq+l
MD5:	4CDEC46BF4C5E1435E277CB4821D6306
SHA1:	506F3E77835A2AE504189833D4EF30799A0ACE45
SHA-256:	39A3F2156450758ACBBCB3D8E9461BB4CDD93F41A3EC3A4013F4EB8D2A906537
SHA-512:	7039ED1E181A8368526A65F6F0D2F70E5BCEBD37BB3BFD8E270BB305F405DB0D843B1CAF6E4E05F6CF1D203A8AA326A1316CDDDD085DD59DB15A82A26E6FA75
Malicious:	false
Reputation:	low
Preview:	.user..A.l.b.u.s.............p.......................................P.....................z...............x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.5119546202634186
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	DOC0798.doc
File size:	1613819
MD5:	51a19560ad005f1dfaf49d959c2dbe7a
SHA1:	660adab2960c1e726e610223e3032595f49f7e74
SHA256:	00175c704e4d534a072f8d777bbb5413dfa32d51fd6b922 e88e980c02357b0f1
SHA512:	e27f5a1dfa095b4219f19866eca67fd4289ea0a72bb1b8c 9532f48d204dab9d4c595efe9382a450633104204e88eb6 ad43b8e2fce60ff8e323d16fda8921a576
SSDEEP:	12288:ZZ2nkYR5UxLEpyI28DpDwHVfsDpEq3EnCpug3 P:akYR5UwyI9pg5Y2q38Cz/
File Content Preview:	{\rtf8561{\object\objautlink67039725\objw4045\objh7166 {*\objdata.3dbf9512020000000b0000004551556174696 6e2e33000000000000000000ab4f0c00037e01eb470a01 05c02e5cec00000000000000000000000000000000000 0000000000000050064500000000000000000000000000 0000000000000

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000003Dh	2	embedded	EQUation.3	806827				no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 11:58:29.816647053 CEST	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	femto.pw	A (IP address)	IN (0x0001)
Jun 16, 2021 11:58:29.883074045 CEST	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	femto.pw	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 11:58:29.882754087 CEST	8.8.8.8	192.168.2.22	0x71dd	No error (0)	femto.pw		188.165.215.31	A (IP address)	IN (0x0001)
Jun 16, 2021 11:58:29.945027113 CEST	8.8.8.8	192.168.2.22	0x71dd	No error (0)	femto.pw		188.165.215.31	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2596 Parent PID: 584

General

Start time:	11:58:33
Start date:	16/06/2021
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:	0x13f320000
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 Show Windows behavior

File Created

File Deleted

File Moved

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2628 Parent PID: 584

General

Start time:	11:58:34
Start date:	16/06/2021
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: EQNEDT32.EXE PID: 912 Parent PID: 584

General

Start time:	11:58:53
Start date:	16/06/2021
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly