ID: 406072
Sample Name: Giam Gia Dien dich Covid-19.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:48:35
Date: 06/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

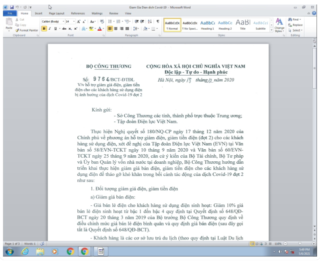
Analysis Report Giam Gia Dien dich Covid-19.docx

Overview

General Information

Sample Name:	Giam Gia Dien dich Covid-19.docx
Analysis ID:	406072
MD5:	3a5ea4602985f1d.
SHA1:	165975dd8d3965..
SHA256:	3d63156060c756..
Infos:	

Most interesting Screenshot:



BỘ CÔNG THƯƠNG

Số: 9764/BCT-ĐTĐL
V/v hỗ trợ giảm giá điện, giảm tiền điện cho các khách hàng sử dụng điện bị ảnh hưởng của dịch Covid-19 đợt 2

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 18 tháng 12 năm 2020

Kính gửi:
- Sở Công Thương các tỉnh, thành phố trực thuộc Trung ương;
- Tập đoàn Điện lực Việt Nam.

Thực hiện Nghị quyết số 180/NQ-CP ngày 17 tháng 12 năm 2020 của Chính phủ về phương án hỗ trợ giảm điện, giảm tiền điện (đợt 2) cho các khách hàng sử dụng điện, xét đề nghị của Tập đoàn Điện lực Việt Nam (EVN) tại Văn bản số 58/EVN-TCKT ngày 10 tháng 9 năm 2020 và Văn bản số 60/EVN-TCKT ngày 25 tháng 9 năm 2020, căn cứ ý kiến của Bộ Tài chính, Bộ Tư pháp và Ủy ban Quản lý vốn nhà nước tại doanh nghiệp, Bộ Công Thương hướng dẫn triển khai thực hiện giảm giá bán điện, giảm tiền điện cho các khách hàng sử dụng điện để tháo gỡ khó khăn trong bối cảnh tác động của dịch Covid-19 đợt 2 như sau:

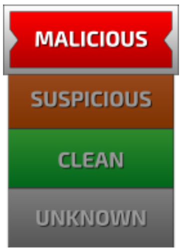
1. Đối tượng giảm giá điện, giảm tiền điện

a) Giảm giá bán điện:

- Giá bán lẻ điện cho khách hàng sử dụng điện sinh hoạt: Giảm 10% giá bán lẻ điện sinh hoạt từ bậc 1 đến bậc 4 quy định tại Quyết định số 648/QĐ-BCT ngày 20 tháng 3 năm 2019 của Bộ trưởng Bộ Công Thương quy định về điều chỉnh mức giá bán lẻ điện bình quân và quy định giá bán điện (sau đây gọi tắt là Quyết định số 648/QĐ-BCT).

- Khách hàng là các cơ sở lưu trú du lịch (theo quy định tại Luật Du lịch

Detection



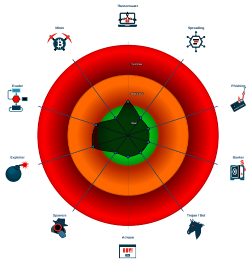
Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm…

Allocates a big amount of memory (p…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 1796 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

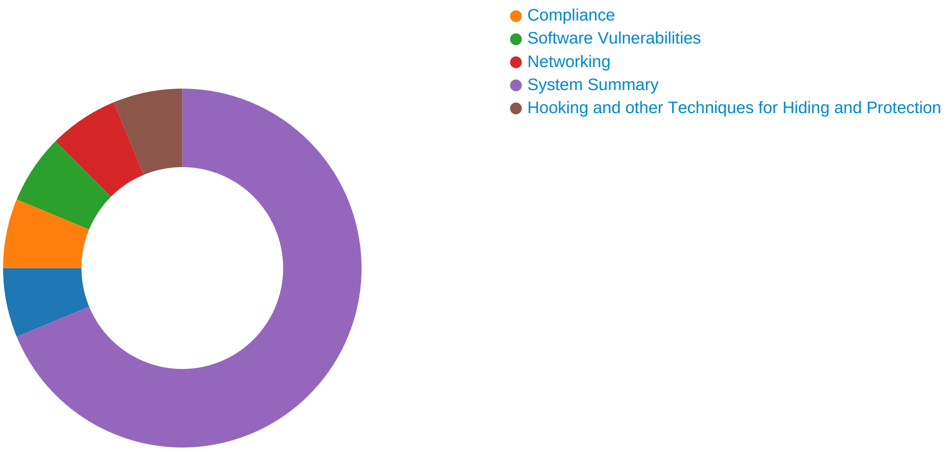
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● AV Detection



Click to jump to signature section

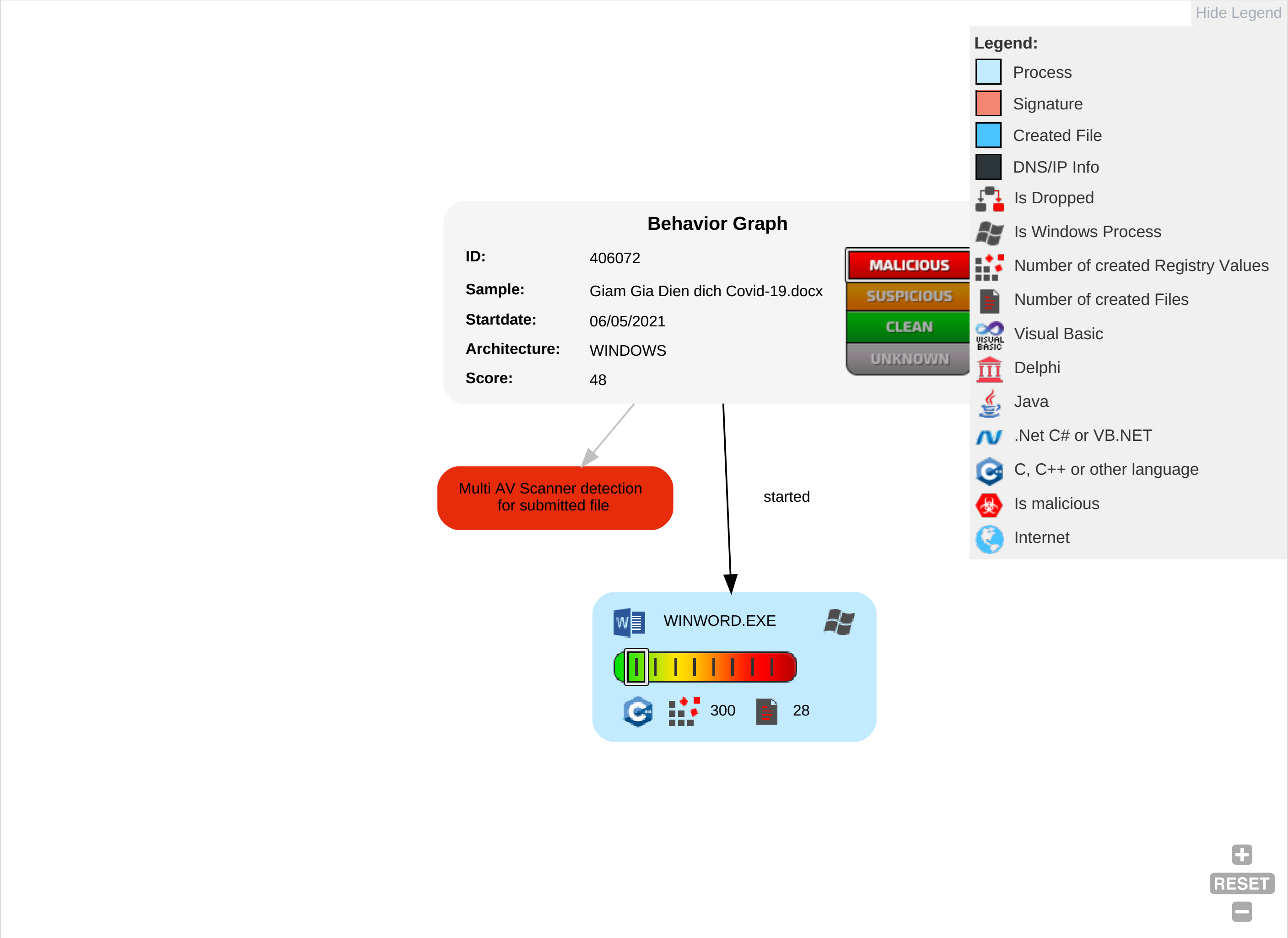
AV Detection:

Multi AV Scanner detection for submitted file

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Behavior Graph



Behavior Graph

ID: 406072

Sample: Giam Gia Dien dich Covid-19.docx

Startdate: 06/05/2021

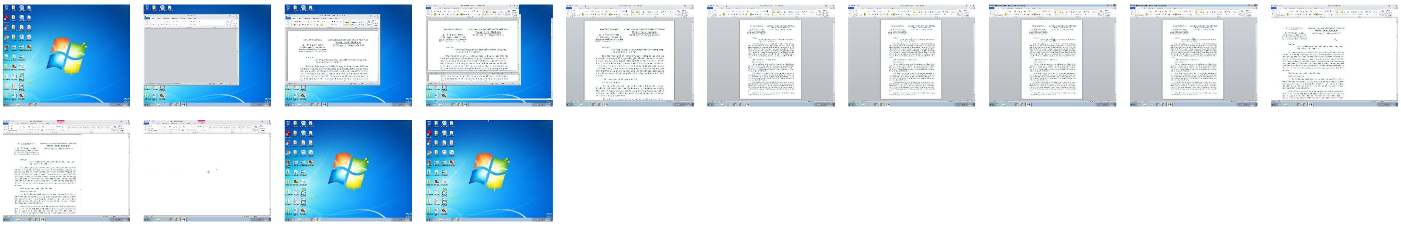
Architecture: WINDOWS

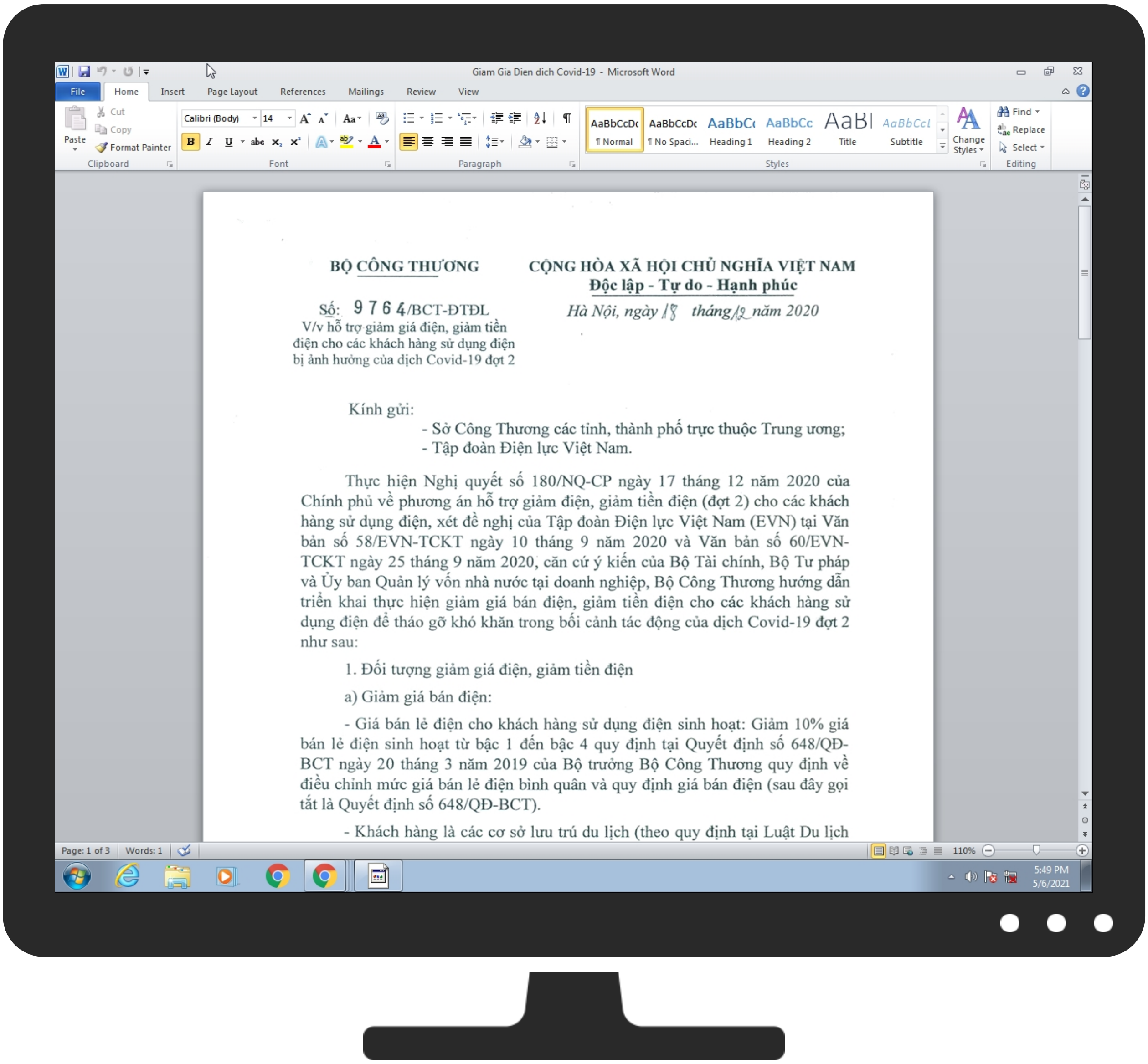
Score: 48

Screenshots

Thumbnails

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





BỘ CÔNG THƯƠNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 9764/BCT-ĐTĐL
V/v hỗ trợ giảm giá điện, giảm tiền điện cho các khách hàng sử dụng điện bị ảnh hưởng của dịch Covid-19 đợt 2

Hà Nội, ngày 18 tháng 12 năm 2020

Kính gửi:
- Sở Công Thương các tỉnh, thành phố trực thuộc Trung ương;
- Tập đoàn Điện lực Việt Nam.

Thực hiện Nghị quyết số 180/NQ-CP ngày 17 tháng 12 năm 2020 của Chính phủ về phương án hỗ trợ giảm điện, giảm tiền điện (đợt 2) cho các khách hàng sử dụng điện, xét đề nghị của Tập đoàn Điện lực Việt Nam (EVN) tại Văn bản số 58/EVN-TCKT ngày 10 tháng 9 năm 2020 và Văn bản số 60/EVN-TCKT ngày 25 tháng 9 năm 2020, căn cứ ý kiến của Bộ Tài chính, Bộ Tư pháp và Ủy ban Quản lý vốn nhà nước tại doanh nghiệp, Bộ Công Thương hướng dẫn triển khai thực hiện giảm giá bán điện, giảm tiền điện cho các khách hàng sử dụng điện để tháo gỡ khó khăn trong bối cảnh tác động của dịch Covid-19 đợt 2 như sau:

1. Đối tượng giảm giá điện, giảm tiền điện

a) Giảm giá bán điện:

- Giá bán lẻ điện cho khách hàng sử dụng điện sinh hoạt: Giảm 10% giá bán lẻ điện sinh hoạt từ bậc 1 đến bậc 4 quy định tại Quyết định số 648/QĐ-BCT ngày 20 tháng 3 năm 2019 của Bộ trưởng Bộ Công Thương quy định về điều chỉnh mức giá bán lẻ điện bình quân và quy định giá bán điện (sau đây gọi tắt là Quyết định số 648/QĐ-BCT).

- Khách hàng là các cơ sở lưu trú du lịch (theo quy định tại Luật Du lịch

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Giam Gia Dien dich Covid-19.docx	44%	Virustotal		Browse
Giam Gia Dien dich Covid-19.docx	37%	ReversingLabs	Document-Word.Trojan.MacroLess	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	406072
Start date:	06.05.2021
Start time:	17:48:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Giam Gia Dien dich Covid-19.docx
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:	3
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:	MAL
Classification:	mal48.winDOCX@1/11@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8D7893DF.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1632x2248, frames 3
Category:	dropped
Size (bytes):	463122
Entropy (8bit):	7.941005620963689
Encrypted:	false
SSDEEP:	12288:guWH4ewApn1KVgYW4MuQPMMvoIcqSKNOOTH/L1PVd:DWOu0VDWV+hqSKNZH/p
MD5:	8DC6D650D41EF0AEE460EA408CFFB095
SHA1:	519D87A644B924FF2843E56E76516000C1C58D03
SHA-256:	3E6B27C4EF54DAEDBEB5364CC83CD0B311145D22F6FFCAB803846116E2E89FC3
SHA-512:	6D23FC0478F6869198180FF70B6AEBDE815FD3133FFBDB3A853D618884E95FB5B01AE11CC4F9490AF88BBA261130A11A2CF677FC087C1354B32726C56239799E
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C................................... $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222........`..".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?...(...(...(......P..(...(...(...)...*A....@.t....]s...i.f.."...].s.h........K.g...k#H.......`g...PH. ERHP3.b..9.H....n..&...F(U.`.../\..EE.....1...(.aE.P...H..#$.J\s.(.QE..(...(.E.....R.1@.......f) ..8..(4.O(.1C:.7.f....G!R.W...R*...Q.P....<Q..0(....).4r.($t.j].....R..`...E1.F.9P]z.............@.R.4.h.4.f..P..K@4P0..(...-.P.I.Z1@.....F.......!...;..P(..(.0..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD15C54.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1632x2248, frames 3
Category:	dropped
Size (bytes):	179149
Entropy (8bit):	7.498989359361687
Encrypted:	false
SSDEEP:	3072:InZv8DVPECilPPurliFX4zeqyFswxmLNv/Ovlf6r:IiDVcCixmkdywg4k
MD5:	CCF44CB88060891D72824C85263B8593
SHA1:	E3F073A33F58ED9A8D30FE5B40C1562B63525549
SHA-256:	A4CF4B260533B8C2E0BB48CC238E3911814C9D2A66D717F027FE7ED84F3E6CD6
SHA-512:	0C1EB2059BBEEA8544A8383222E629C9BB6DF033814EB67E8BCA1049220454C91546A1B20B2808676E34573225204A120C359B2B6888818AEE6F8EEAAA86BEAD
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C................................... $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222........`..".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?...(...(...(...(.....P.(...(...(...(..P..1KE..(......-....M&=(..@.E/Z1@..F3K.K@X@)h...(...Fih...(...(......ZZB.....L|....(...(.-..M.....wu....SB..;.....4.P...1.-.......P16...-..@1A......F) q.K@..LsN...c..J(...QE....(.bm..Q@..sK.(...........)h.....).b..m..........Q@..6.....c.4.c..4..R..Z(...2sKE.&)h...Lf...M.=(.-..n=)pii;..FF..b...B)...E.&)1.N..h.x#....Z.1F9..P0...-...R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F6DE19D6.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1632x2248, frames 3
Category:	dropped
Size (bytes):	397176
Entropy (8bit):	7.917524851464137
Encrypted:	false
SSDEEP:	12288:z3cKJJb9zQkrtlQ3pWcESs5tKvE1kylf6+Aa:tJVHOWcCtThlfaa
MD5:	A932FCE967C7DC635C60325088BE2BC5
SHA1:	7AED834D295BDD62F487DE5834A1CD118434E669
SHA-256:	7EA75C8EC7C814267F116DE05F0C56E7228E6BECF1F245B8FFEC78C6520E3D85
SHA-512:	ADF8F7F5A96699562AEC022883E706543BD676C530455AC0B0852A276E486E09F1EB5D3F7BFAF57966AB531C068D573E0AF5AAF983C71FCC172975703F57DCC
Malicious:	false
Reputation:	low
Preview:	......JFIF.............C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222........`.."..................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?...(...(...(...(...(...(...(...(.4..QE..R.Z.(..@...(...(....g....E..QE..QE..QE..QE..Ph...E......E......R.@..(.aE.P.A...@1KE..QE..R.R.}N....QE..R.Z(.QE.....(.:Q.R3H}...SI u..@...(.aE.P.E.P..P)qE.....(.......E.P0..(...E...i..-&h..-7.@..(.aE.P.E..&..`P.zR3E...b...M.9.).......Q@.(...(.....);.. ..(.QE..QGz(...(..4...Rt.B.I....Q@.N.-.P .4Sq..:.Nih.g.g.C.t.@.h... .QHh.h...4.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A7F4CFE5-FD14-491B-BD17-FD822CEDA35F}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3144
Entropy (8bit):	3.311868019564163
Encrypted:	false
SSDEEP:	48:I4lUlRNkJahZeIpcagcanTCcyf5kdadahAaaWTXPe:/mvNkJa2IpcagcanTCcG5kdadahAaao2
MD5:	A979A38409D7EDE79660F1B6E872B754
SHA1:	6739A730BB31DA293A469FD0F76B70381DFE2EC7
SHA-256:	FD656B998E0D1EEF0F952FE422EE943EB30B32F1770646254E9511033E0DBA3C
SHA-512:	3E54498415D129D784C812C0759BB1C8D231117264C0E5AB9858344F867F28DF9F02FCC0F54D305A3501B9329DB33E4127F757E9A033047D91A1B4816DCA4E30
Malicious:	false
Reputation:	low
Preview:	....!.".#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>................/.../.../......... .{. .D.D.E.A.U.T.O. .c.:.\.\.w.i.n.d.o.w.s.\.\.s.y.s.t.e.m.3.2.\.\.c.m.d...e.x.e. .. /.k. .n.o.t.e.p.a.d...e.x.e.. .}. .....D.D.E.A.U.T.O. .c.:.\.\.w.i.n.d.o.w.s.\.\.s.y.s.t.e.m.3.2.\.\.c.m.d...e. x.e. .. /.k. .c.a.l.c...e.x.e.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AD3EC32A-61B9-479D-AE81-4807857507A1}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbO:IiiiiiiiifdLloZQc8++lsJe1Mzh
MD5:	7CFD3634C8D02EF244D1B820D25997A8
SHA1:	FA12C6DAA2C16BD453746A6499866A5FDF02FB98
SHA-256:	F73B40163166405E70CE534C02409A96983CFDE4F30F121C2495B09152DB34E2
SHA-512:	80E008560E0383F43AE10E47E44E178E2F1AD9379BD0CCC08DB75DB9F9A13125DF65F98A4D7E2D2528C10BA7D1724EA7E43EA72522DB5F73D9A5EF899DE455 D
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A... ...."...&...*.......:...>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4FD7973-97C0-4A14-814E-1968BCE52029}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4FD7973-97C0-4A14-814E-1968BCE52029}.tmp

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{B91DB962-9907-4C39-AB19-BE7338F7A7B8}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.46639096299572214
Encrypted:	false
SSDEEP:	3:9l99lDKllllzNPJQ7ZlhQteolllzN+t7ZlhQtu:Q//nQ7ZUtDl/Et7ZUtu
MD5:	838749859FE611E154A7D4CB5ADB0766
SHA1:	75A019A743744CBACBACC59A9D2EEA908A22F888
SHA-256:	74DC12DFF6C772D97A23E60457906F00B353C090AAAF051B630B14C2A2680E49
SHA-512:	BD6A531C1A308BD9517B1B41E5D219639B2DB0161215D73A57BD2E61A1F61FED85D83BF5A38FADA47C03896D51F98A948AFC72DE6DC7770A4BF089E2BDA33E06
Malicious:	false
Reputation:	low
Preview:	....j.....h.x7.U..mH..nH..u.....j.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Giam Gia Dien dich Covid-19.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 May 6 23:49:34 2021, length=3831871, window=hide
Category:	dropped
Size (bytes):	2208
Entropy (8bit):	4.59498168731805
Encrypted:	false
SSDEEP:	24:8JH/XTm6GreVYePiDv3qodM7dD2JH/XTm6GreVYePiDv3qodM7dV:81/XTFGqKWRoQh21/XTFGqKWRoQ/
MD5:	FBF42810DD794888C3A101311B2AE83B
SHA1:	3827C541DA4F3BA3DAA2C0E1293089EA3D9B8527
SHA-256:	F4089CD28CC56808CBB1BF24A7D2E909F55E99AA7F1DE81756F3DDA02899E135
SHA-512:	EA227B4506386C440A129346CAD5B6B10B7502140F33963E3C7B04190A1F21FE0653A8D58565269D434EFCD07EF3C7C6884B4028F9F600C943E084C78D2B25F4
Malicious:	false
Reputation:	low
Preview:	L.................F.... ...l....{..l....{.......B..?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.......2.?x:..R2. .GIAMGI~1.DOC..n.......Q.y.Q.y*...8....................G.i.a.m. .G.i.a. .D.i.e.n. .d.i.c.h. .C.o.v.i.d.-.1.9...d.o.c.x......................-...8...[............?J......C:\Users\..#..................\\134349\Users.user\Desktop\Giam Gia Dien dich Covid-19.docx.7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.G.i.a.m. .G.i.a. .D.i.e.n. .d.i.c.h. .C.o.v.i.d.-.1.9...d.o.c.x.........:..,.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.........

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):	121
Entropy (8bit):	4.542396251693991
Encrypted:	false
SSDEEP:	3:HpWsaKtX9icA4o6yhsaKtX9icA4omxWpWsaKtX9icA4ov:HpZaKtX9/faKtX9/aZaKtX9/y
MD5:	A6A003D8A638AAD4B0740F87E1B11870
SHA1:	892CB43317BE13499D66ECA7E4A23FC4582B773E
SHA-256:	D2652ED72E15F5B44F02F36965CCEC9D59ADAB83EB71841B930741268FD7250D

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

SHA-512:	A51C9327D4D1C48FD77B2F9FF9F4A124C709E06ADA54054C32DC859E1B71E78FF7B736BD714BD8F857A5BC180820E35F3B972629CE06760CDC407D187D5828A
Malicious:	false
Reputation:	low
Preview:	[misc]..Giam Gia Dien dich Covid-19.LNK=0..Giam Gia Dien dich Covid-19.LNK=0..[misc]..Giam Gia Dien dich Covid-19.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IlID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user..A.l.b.u.s.............p.........w...............w.............P.w.............w.....z.........w.....x...

C:\Users\user\Desktop\~$am Gia Dien dich Covid-19.docx

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:vdsCkWtW2IlID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Preview:	.user..A.l.b.u.s.............p.........w...............w.............P.w.............w.....z.........w.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.986899031192039
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Giam Gia Dien dich Covid-19.docx
File size:	3831871
MD5:	3a5ea4602985f1db670f166e111aefd2
SHA1:	165975dd8d3965068f3dc0a2c5b512e5e6a9de1f
SHA256:	3d63156060c7568b2c3065820f698fdadb6e48910ec8259 3a61c306c13f5692c
SHA512:	cae1180e5a8cc0dae9d4c9c78d4fe2a6c12e229c8ce8db 2eb581dee86348aa367176fd48f27e8b34a6308a8f00699 b50d6190b32e5b06d64c5432bbbdb54e8ae
SSDEEP:	98304:JoycO1vLPTvgX9l3N6+lsNy93RcY0W7/iJg8:Joq vz8XL3N6gsU9aY0Wcd
File Content Preview:	PK..........!....F............[Content_Types].xml ...(................. ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1796 Parent PID: 584

General

Start time:	17:49:34
Start date:	06/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fa70000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD15C54.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AD3EC32A-61B9-479D-AE81-4807857507A1}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE90A9AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B91DB962-9907-4C39-AB19-BE7338F7A7B8}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEE90A9AC0	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$am Gia Dien dich Covid-19.docx	success or wait	1	7FEE90A9AC0	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
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD15C54.jpeg	0	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 ff c0 00 11 08 08 c8 06 60 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.............C...... .... $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222 2 2222222222222222222222 22222222 22222222.......`.."......... ....}........! 1A..Qa."q.2....	success or wait	3	7FEE90A9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AD3EC32A-61B9-479D-AE81-4807857507A1}.tmp	unknown	1536	0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 28 00 0d 00 41 00 6c 00 62 00 75 00 73 00 0d 00 41 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B91DB962-9907-4C39-AB19-BE7338F7A7B8}.tmp	unknown	1024	08 00 08 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....	success or wait	1	7FEE90A9AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Giam Gia Dien dich Covid-19.docx	3179977	65536	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD15C54.jpeg	0	88	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAD15C54.jpeg	0	22	success or wait	1	7FEE90A9AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8D7893DF.jpeg	0	65536	success or wait	8	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F6DE19D6.jpeg	0	65536	success or wait	7	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A7F4CFE5-FD14-491B-BD17-FD822CEDA35F}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A7F4CFE5-FD14-491B-BD17-FD822CEDA35F}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B91DB962-9907-4C39-AB19-BE7338F7A7B8}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B91DB962-9907-4C39-AB19-BE7338F7A7B8}.tmp	unknown	512	success or wait	1	7FEE90A9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A7F4CFE5-FD14-491B-BD17-FD822CEDA35F}.tmp	unknown	72	success or wait	1	7FEE90A9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7031	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI	binary	02 0B 05 02 04 02 04 02 02 03	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft JhengHei	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Microsoft JhengHei	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7031	F7031	binary	04 00 00 00 04 07 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 C2 47 06 F4 DA 42 D7 01 31 70 0F 00 31 70 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	success or wait	1	7FEE90A9AC0	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386610735	1386610736	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1386610736	1386610737	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F7031	F7031	binary	04 00 00 00 04 07 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 C2 47 06 F4 DA 42 D7 01 31 70 0F 00 31 70 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 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	04 00 00 00 04 07 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 31 70 0F 00 31 70 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 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	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 FF FF FF FF				

Disassembly