

ID: 392737
Sample Name: Covid-19 Payroll Tax Adjustment.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:41:36
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Covid-19 Payroll Tax Adjustment.docx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Persistence and Installation Behavior: 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
URLs from Memory and Binaries 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 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 15
General 15
File Icon 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 18
DNS Queries 18
DNS Answers 18
HTTPS Packets 18
Code Manipulations 19
Statistics 19
System Behavior 19
Analysis Process: WINWORD.EXE PID: 2436 Parent PID: 584 19
General 19
File Activities 19
File Created 19

Copyright Joe Security LLC 2021

File Deleted 20
File Written 20
File Read 20
Registry Activities 20
Key Created 20
Key Value Created 21
Key Value Modified 22
Disassembly 24

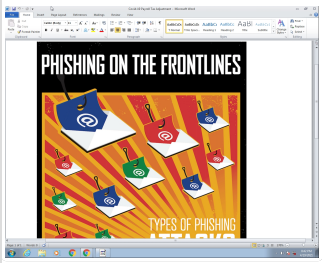
Analysis Report Covid-19 Payroll Tax Adjustment.docx

Overview

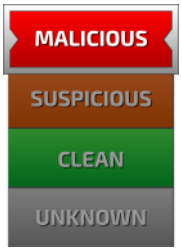
General Information

Sample Name:	Covid-19 Payroll Tax Adjustment.docx
Analysis ID:	392737
MD5:	f78e1a17152954d.
SHA1:	9ad2cffb62540c6..
SHA256:	606e7c0165678a..
Infos:	

Most interesting Screenshot:



Detection

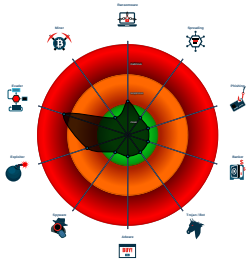


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Contains an external reference to an…
- IP address seen in connection with o…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2436 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

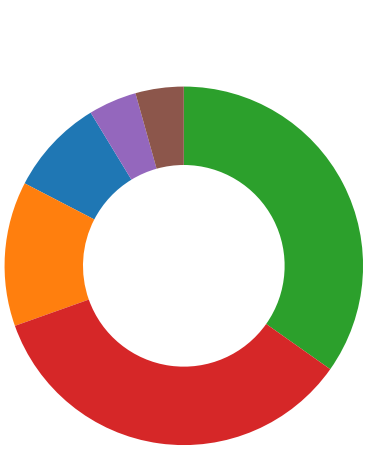
Sigma Overview

No Sigma rule has matched

Signature Overview

● Compliance

Copyright Joe Security LLC 2021



Click to jump to signature section

Persistence and Installation Behavior:



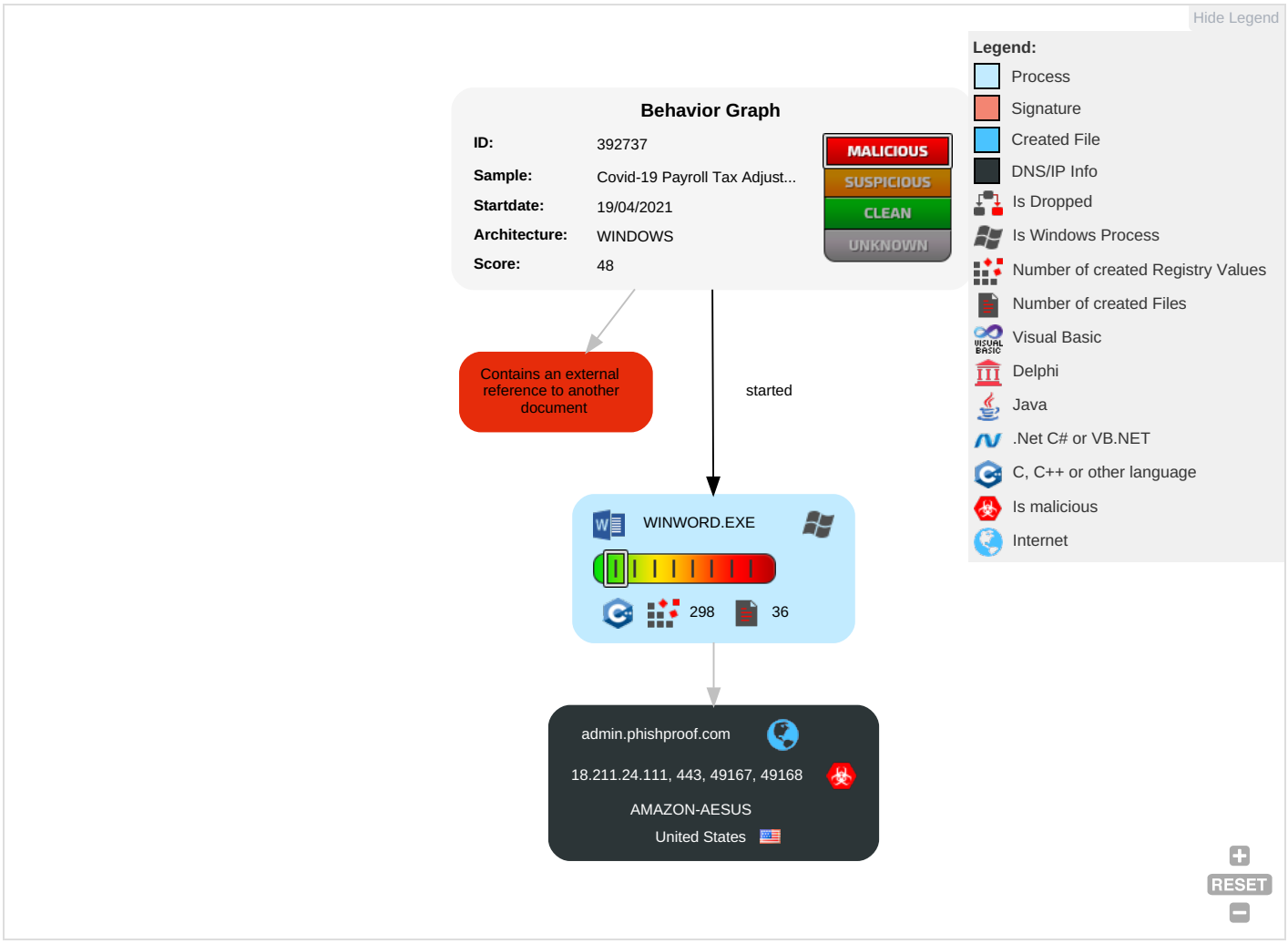
Contains an external reference to another document

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	Exploitation for Client Execution 3	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carrier Billing Fraud

Behavior Graph

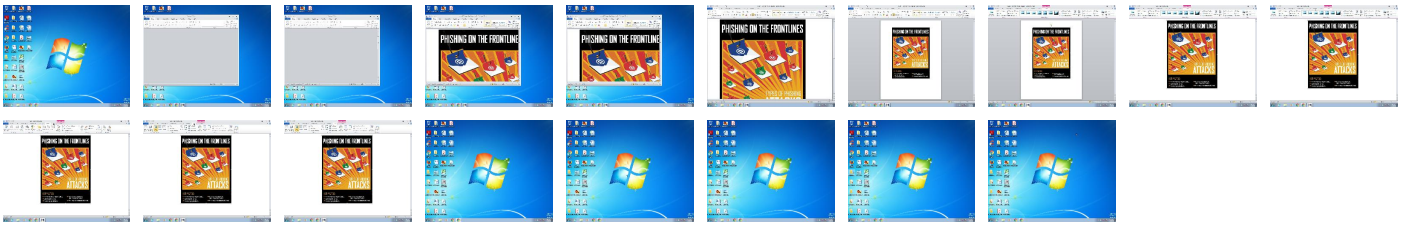
Copyright Joe Security LLC 2021

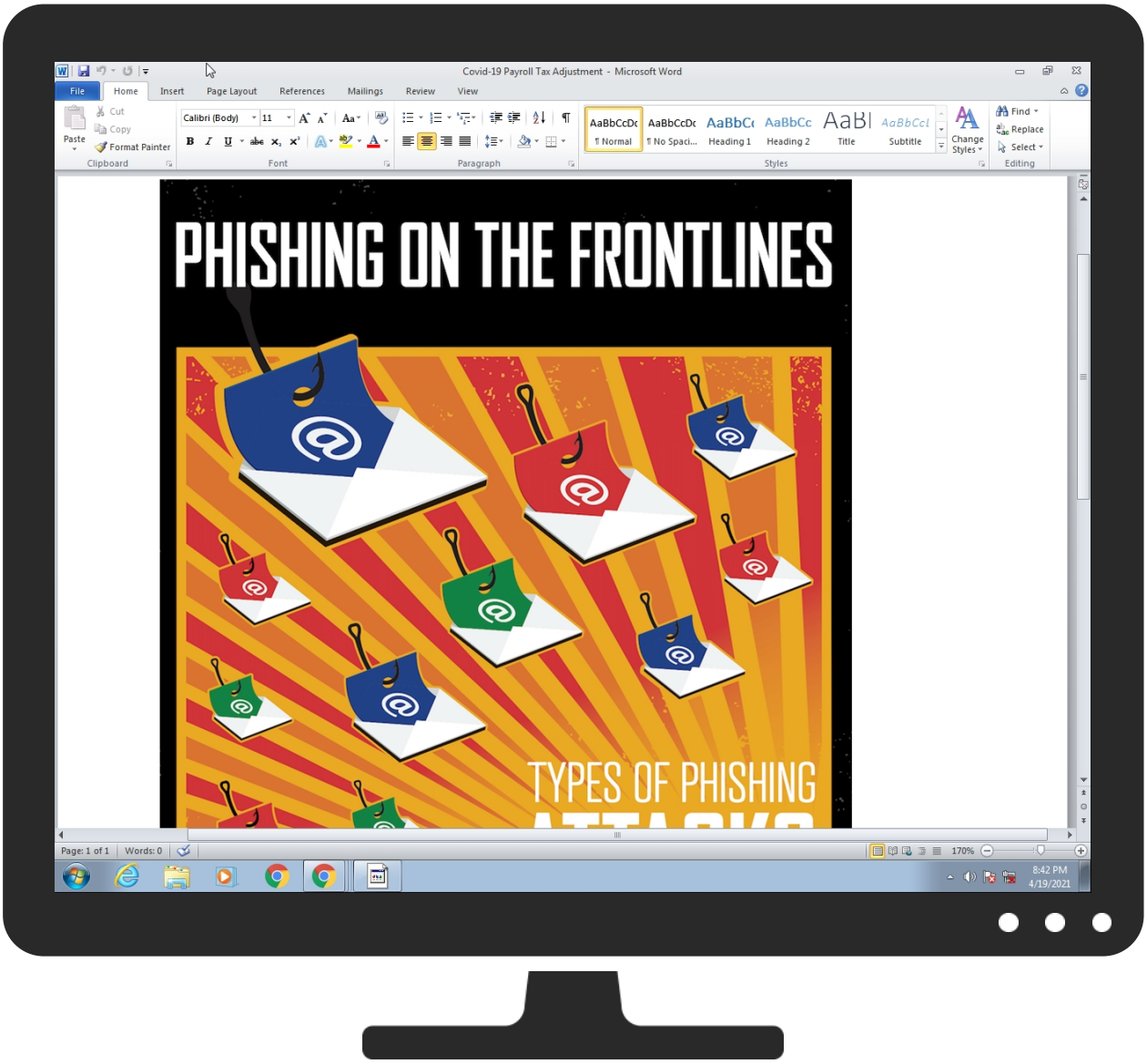


Screenshots

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

Source	Detection	Scanner	Label	Link
admin.phishproof.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://admin.phishproof.com/af-Dbh8nMk.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
admin.phishproof.com	18.211.24.111	true	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://admin.phishproof.com/af-Dbh8nMk.png	~WRS{A70475F6-E366-40C3-B2E6-22C3DC55A9E1}.tmp.0.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.211.24.111	admin.phishproof.com	United States		14618	AMAZON-AESUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392737
Start date:	19.04.2021
Start time:	20:41:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Covid-19 Payroll Tax Adjustment.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs

Copyright Joe Security LLC 2021

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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.evad.winDOCX@1/16@1/1
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 • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 91.199.212.52, 13.107.4.50 • Excluded domains from analysis (whitelisted): au.au-msedge.net, crt.usertrust.com, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, Edge-Prod-FRA.env.au.au-msedge.net, au.c-0001.c-msedge.net, elasticShed.au.au-msedge.net, au-bg-shim.trafficmanager.net, afdap.au.au-msedge.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.211.24.111	annualreport.xlsx	Get hash	malicious	Browse	
	annualreport.xlsx	Get hash	malicious	Browse	
	action_items.xlsm	Get hash	malicious	Browse	
	action_items.xlsm	Get hash	malicious	Browse	
	action_items.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
admin.phishproof.com	annualreport.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	annualreport.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	action_items.xlsm	Get hash	malicious	Browse	• 18.211.24.111

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	action_items.xlsm	Get hash	malicious	Browse	• 18.211.24.111
	action_items.xlsm	Get hash	malicious	Browse	• 18.211.24.111
	Love_you_201.doc	Get hash	malicious	Browse	• 18.233.242.165
	Love_you_201.doc	Get hash	malicious	Browse	• 18.233.242.165
	Love_you_201.doc	Get hash	malicious	Browse	• 18.233.242.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	VoicePlayback (0195) for turnerrd pellamw .html	Get hash	malicious	Browse	• 50.16.177.212
	Monday, April 19th, 2021, 20210419111136.68B7C9F20 FAF4F3F@classactsautobody.com.htm	Get hash	malicious	Browse	• 50.16.177.212
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 52.71.133.130
	bxJIU2nFC5.exe	Get hash	malicious	Browse	• 54.243.121.36
	KoF2fbpF8X.exe	Get hash	malicious	Browse	• 23.21.48.44
	RFQ.xlsx	Get hash	malicious	Browse	• 52.5.157.71
	GE3hVNHtrK.exe	Get hash	malicious	Browse	• 3.232.116.190
	preggo.apk	Get hash	malicious	Browse	• 54.86.40.118
	preggo.apk	Get hash	malicious	Browse	• 54.208.246.209
	q7uNNDJUI2.exe	Get hash	malicious	Browse	• 23.23.85.1
	BQGxKexU78.exe	Get hash	malicious	Browse	• 23.21.74.8
	oddMyFn53m.exe	Get hash	malicious	Browse	• 54.225.155.255
	kBB0LJe6UO.exe	Get hash	malicious	Browse	• 54.235.175.90
	078y61cSKy.exe	Get hash	malicious	Browse	• 50.19.242.215
	svchost.exe	Get hash	malicious	Browse	• 54.225.144.221
	Ficker.exe	Get hash	malicious	Browse	• 54.225.222.160
	H7YgdxkWKW.exe	Get hash	malicious	Browse	• 107.22.233.72
	JSChk2v3o9.exe	Get hash	malicious	Browse	• 54.225.144.221
	K7is14GW1m.exe	Get hash	malicious	Browse	• 54.235.83.248

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	xEkyQl1Yn2.rtf	Get hash	malicious	Browse	• 18.211.24.111
	catalog-1763942449.xlsm	Get hash	malicious	Browse	• 18.211.24.111
	159789-04192021.xls	Get hash	malicious	Browse	• 18.211.24.111
	494328_04192021.xls	Get hash	malicious	Browse	• 18.211.24.111
	369290.xls	Get hash	malicious	Browse	• 18.211.24.111
	369290.xls	Get hash	malicious	Browse	• 18.211.24.111
	RFQ.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	catalog-232888535.xlsm	Get hash	malicious	Browse	• 18.211.24.111
	Fox04-09-15-47-23.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	PO_31403.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	Arrival Notice 1.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	catalog-1180297109.xlsm	Get hash	malicious	Browse	• 18.211.24.111
	IINVOICE AND CORRECT BANKING DETAILS FOR YOUR REFERENCE.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	APRemittanceAdvice.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	ChineseRussian_2.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	presupuesto.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	INVOICE AND CORRECT BANKING DETAILS FOR YOUR REFERENCE.xlsx	Get hash	malicious	Browse	• 18.211.24.111
	a.docx	Get hash	malicious	Browse	• 18.211.24.111
	catalog-1204608778.xlsm	Get hash	malicious	Browse	• 18.211.24.111
	Order Confirmation_SA-NQAW12,NC9W03.xlsx	Get hash	malicious	Browse	• 18.211.24.111

Dropped Files

No context

Created / dropped Files

Copyright Joe Security LLC 2021

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0968A1E3A40D2582E7FD463BAEB59CD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1413
Entropy (8bit):	7.480496427934893
Encrypted:	false
SSDEEP:	24:yYvJm3RW857Ij3kTteTuQRFjGgZLE5XBy9+JYSE19rVAVsGnyI3SKB7:PL854TTuQL/ZoXQ9+mrGVrb3R
MD5:	285EC909C4AB0D2D57F5086B225799AA
SHA1:	D89E3BD43D5D909B47A18977AA9D5CE36CEE184C
SHA-256:	68B9C761219A5B1F0131784474665DB61BBDB109E00F05CA9F74244EE5F5F52B
SHA-512:	4CF305B95F94C7A9504C53C7F2DC8068E647A326D95976B7F4D80433B2284506FC5E3BB9A80A4E9A9889540BBF92908DD39EE4EB25F2566FE9AB37B4DC9A7C0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0..i.....9rD:.".Q..I..15.0...*.H.....0{1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Comodo CA Limited1!0...U....AAA Certificate Services0...190312000000Z..281231235959Z0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0.."0...*.H.....0.....e.6.....W.v..'.L.P.a. M.-d.....=.....{7(.+G.9.:._..}..cB.v.;+...o.. ..>..t.....bd.....j."<.....{.....Q..gF.Q..T?.3.~l.....Q.5..f.rg.!f..x..P:.....L....5.WZ....=.,..T....:M.L..\... =.."4.~;hf.D..NFS.3`...S7.sC.2.S...tNi.k.`.....2..;Qx.g..=V...i....%&k3m.nG.sC.~..f.)|2.cU.....T0....}7..]:l5\.A...I.....b..f.%....?.9.....L.|.k..^...g.....[..L..[...s.#;-..5Ut.I.IX...6.Q...&}.M....C&.A_@.DD...W..P.WT.>.tc/.Pe..XB.C.L..%GY.....&FJP...x..g...W...c..b.._U..\.(..%9..+..L...?.R.../.....0..0...U.#..0.....#>.....)...0..0...U.....Sy.Z.+J.T.....f.0...U.....0...U.....0....0...U

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.116981173650867
Encrypted:	false
SSDEEP:	6:kKBcwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:5cwTJrkPlE99SNxAhUe0ht
MD5:	D2B4EF7A6D90C3C69AA1D3EB9C0B904B
SHA1:	2380579533EA63CD738EB72CF77E9DCA17773013
SHA-256:	2330AEA57BC61B62200381E07826FCF5DA353706DDCC025DBFFFF8C4357C448D
SHA-512:	0F63FF12DF1CA24EB02E6BDD6048D4E8D22DF0FAE525C73F18524E3F008BAF974547B80304077B78AC402B73FCABDBE363ACF8A921ECAF578DCF4DBFD45ADCE4
Malicious:	false
Reputation:	low
Preview:	p..... .....v5.5..(..... ....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0968A1E3A40D2582E7FD463BAEB59CD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	2.9333015258354003
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0968A1E3A40D2582E7FD463BAEB59CD	
SSDEEP:	3:kkFklNloQblXfllXlE/lQcjT18tlwiANjpU+plgh3VEkax3QbaLU15lqErtd9lyt:kK6IQAbjMulgokaWbLOW+n
MD5:	2B8FBBFB0FF5231B0D2F0FD6B1B35229
SHA1:	9531B9CCAEB59AC01D358AAD91EDCDA011776F3C
SHA-256:	B512A4C620916F6DF27976B8634F39C802CDB6C590A3A94C03A636F6B87B441E
SHA-512:	049F3D453FA465E598F11F3F00D05B15B78A13937278311AD7F9E00ED38B93A9D6760CB475967D1D1BE5F161DDD3F79C541975F5CCDBD0991C6A41C4C74FE2D
Malicious:	false
Reputation:	low
Preview:	p..... ....h.....35.5..(..... .....(.f...@8.....h.t.t.p.:././.c.r.t...u.s.e.r.t.r.u.s.t...c.o.m./.U.S.E.R.T.r.u.s.t.R.S.A.A.d.d.T.r.u.s.t.C.A...c.r.t... ".5.c.8.6.f.6.8.0.-.5.8.5."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\af-Dbh8nMk[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 848 x 1184, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	719675
Entropy (8bit):	**7.996898300210567**
Encrypted:	**true**
SSDEEP:	12288:khSdZ8li0/LgtMVUv+NjBl0Q5x56AMIRJqNSrna5eoC9hgO6oWb/N8kJCXgsE/:kMdmVzQMOvSBl0Q536fGJa5RC9+O6eF4
MD5:	167730B067E677A65BAAA3E1C317392B
SHA1:	29ABFFFB01422F8CF9679ACCC4DF31891B79CE3E
SHA-256:	0023C3DA70CDE56DBBADAD0C6A872A90D025A38B3AC1E66BC48120A1478B9008
SHA-512:	928D6336F7911D9022576AF3F5196DEC9FF2FB1FD70C59ABF9E3603F09EE637E6D0322E7637A94CE0DA592D41AE041A499D30CBB8C5E82F0477426620C69AAE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://admin.phishproof.com/af-Dbh8nMk.png
Preview:	.PNG.....IHDR...P.....KiCCPICC Profile..H..W.TSI.[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ.(v.(.....*.....3w.....;..N.O*.Eu.....#BX.R.X.N@...9.-._.e..E.(.....u.(.+.J.. ..._....|..8.3.r~.....K.RY>.D...../U.I...`..K.8K.K.8C.+U6....w.@..x.,.....U..<.7!v.....t....E<.....8d|../.!N./k..sQ.9T,...f.....a..M$..W...v3gZ... .d..B...;.@e.1J.)"....)_.5.L.]...(.M !....Dk....p..p....|n.f.".<,A.Y#...;.3e..fn.O..?..Ibk.o...A..E...u...@....6.LyNB....).qb.md.xe.6...%.!j~lJ.,<^c/...-...1.\./J.....T..A.,....y.....a..KBI.&_.C.....R.....bSyA.f.....%.. .3.yc..... .p@(`..l.`.....K=..x@.....h4.3RT#..L.E.o..@>4/D5*..P.iH.~..L.h.jF.x.q.....B5K2.-.<...w..0.\.c...P...(.yY:...0b(1..Nt.M.@.....`..q..w0./..G.v...5B...Tq..|X`....59g|.3n.Y=.. <..Cn.....|4....oO..h"Wf.-..r....;.+.....S.....9.....R.1TW....9_UZ...o-.E.>.4v.;.....;.5c...J<....V..xU<9.G..?....r.z.n..|a.r...i.2q.(..;....G.`.....WL...a...+..C...../....._p/

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\af-Dbh8nMk[1].png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 848 x 1184, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	719675
Entropy (8bit):	**7.996898300210567**
Encrypted:	**true**
SSDEEP:	12288:khSdZ8li0/LgtMVUv+NjBl0Q5x56AMIRJqNSrna5eoC9hgO6oWb/N8kJCXgsE/:kMdmVzQMOvSBl0Q536fGJa5RC9+O6eF4
MD5:	167730B067E677A65BAAA3E1C317392B
SHA1:	29ABFFFB01422F8CF9679ACCC4DF31891B79CE3E
SHA-256:	0023C3DA70CDE56DBBADAD0C6A872A90D025A38B3AC1E66BC48120A1478B9008
SHA-512:	928D6336F7911D9022576AF3F5196DEC9FF2FB1FD70C59ABF9E3603F09EE637E6D0322E7637A94CE0DA592D41AE041A499D30CBB8C5E82F0477426620C69AAE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...P.....KiCCPICC Profile..H..W.TSI.[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ.(v.(.....*.....3w.....;..N.O*.Eu.....#BX.R.X.N@...9.-._.e..E.(.....u.(.+.J.. ..._....|..8.3.r~.....K.RY>.D...../U.I...`..K.8K.K.8C.+U6....w.@..x.,.....U..<.7!v.....t....E<.....8d|../.!N./k..sQ.9T,...f.....a..M$..W...v3gZ... .d..B...;.@e.1J.)"....)_.5.L.]...(.M !....Dk....p..p....|n.f.".<,A.Y#...;.3e..fn.O..?..Ibk.o...A..E...u...@....6.LyNB....).qb.md.xe.6...%.!j~lJ.,<^c/...-...1.\./J.....T..A.,....y.....a..KBI.&_.C.....R.....bSyA.f.....%.. .3.yc..... .p@(`..l.`.....K=..x@.....h4.3RT#..L.E.o..@>4/D5*..P.iH.~..L.h.jF.x.q.....B5K2.-.<...w..0.\.c...P...(.yY:...0b(1..Nt.M.@.....`..q..w0./..G.v...5B...Tq..|X`....59g|.3n.Y=.. <..Cn.....|4....oO..h"Wf.-..r....;.+.....S.....9.....R.1TW....9_UZ...o-.E.>.4v.;.....;.5c...J<....V..xU<9.G..?....r.z.n..|a.r...i.2q.(..;....G.`.....WL...a...+..C...../....._p/

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\102272C3.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 848 x 1184, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	719675
Entropy (8bit):	**7.996898300210567**
Encrypted:	**true**
SSDEEP:	12288:khSdZ8li0/LgtMVUv+NjBl0Q5x56AMIRJqNSrna5eoC9hgO6oWb/N8kJCXgsE/:kMdmVzQMOvSBl0Q536fGJa5RC9+O6eF4
MD5:	167730B067E677A65BAAA3E1C317392B
SHA1:	29ABFFFB01422F8CF9679ACCC4DF31891B79CE3E
SHA-256:	0023C3DA70CDE56DBBADAD0C6A872A90D025A38B3AC1E66BC48120A1478B9008
SHA-512:	928D6336F7911D9022576AF3F5196DEC9FF2FB1FD70C59ABF9E3603F09EE637E6D0322E7637A94CE0DA592D41AE041A499D30CBB8C5E82F0477426620C69AAE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\102272C3.png	
Reputation:	low
Preview:	.PNG.....IHDR...P.....KiCCPICC Profile..H..W.TSI.[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ.(v.(.....*.....3w.....;..N.O*.Eu.....#BX.R.X.N@...9.-._.e..E.(.....u.(.+.J.. .._....|..8.3.r~.....K.RY>.D...../U.I..`..K.8K.K.8C.+U6....w.@..x.,.....U..<.7!v.....t....E<.....8d|../.!N./k..sQ.9T,...f.....a..M$..W...v3gZ... .d..B...;.@e.1J.)"....)_.5.L.]...(.M !....Dk....p..p....|n.f.".<,A.Y#...;.3e..fn.O..?..Ibk.o...A..E...u...@....6.LyNB....).qb.md.xe.6...%.!j~lJ.,<^c/...-...1.\./J.....T..A.,....y.....a..KBI.&_.C.....R.....bSyA.f.....%.. .3.yc..... .p@(`..l.`.....K=..x@.....h4.3RT#..L.E.o..@>4/D5*..P.iH.~..L.h.jF.x.q.....B5K2.-.<...w..0.\.c...P...(.yY:...0b(1..Nt.M.@.....`..q..w0./..G.v...5B...Tq..|X`....59g|.3n.Y=.. <..Cn.....|4....oO..h"Wf.-..r....;.+.....S.....9.....R.1TW....9_UZ...o-.E.>.4v.;.....;.5c...J<....V..xU<9.G..?....r.z.n..|a.r...i.2q.(..;....G.`..........WL...a...+..C...../.....p/

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BF840B3-025D-4403-9DBE-B492A11253DC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A70475F6-E366-40C3-B2E6-22C3DC55A9E1}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.2969066424008302
Encrypted:	false
SSDEEP:	3:glXMKYHILlP8EP3+KZfolYxRknr2gt95w7ggE7ZSMl6ljtll5l/HZllNPThv51lJ:glXMKYjUbKvRknqgHuMZlwjHltq7ZUtp
MD5:	99BCB4A045A3CEE7CC68A8B6C228438E
SHA1:	B28A208799EA7AFCB1E9DFAB671D55F3C290E1FE
SHA-256:	A26D31E0D9186E67792B2D59108F4603646084D60FB6B80FDFF882812F75E66D
SHA-512:	78420EC8A3A41AEBFD814FE56E9F0DC986A2C8D413038D257FE409423C8B408260B378B317614EE2E94EE998C2F48603CE401088942E1318B303F1B4764FAD07
Malicious:	false
Preview:	....".h.t.t.p.s.:././.a.d.m.i.n...p.h.i.s.h.p.r.o.o.f...c.o.m./.a.f.-.D.b.h.8.n.M.k...p.n.g.". .\.*. .M.E.R.G.E.F.O.R.M.A.T. .\.d.I.N.C.L.U.D.E.P.I.C.T.U.R.E. ....hfT.....j.....hfT..U....j.

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):	1536
Entropy (8bit):	0.19557280042116507
Encrypted:	false
SSDEEP:	3:lly/nnjM/n/lLClk:WjMvY+
MD5:	D3639E51845151C937FD5D3BBCF24993
SHA1:	40472D691864544B1B85BF33D7DD7B076DF1FF7B
SHA-256:	E95E1E45570B2FFB047C5D9CDBBCD054D00A42A6E27ECBD8B251F4F503C84918
SHA-512:	44CFC72178F39FED4C345F94D8F74DE3886E384BD2752B84A5911C73E2D2D522D2B030C45ACB3FA1212ECF56BF6D48BD42345B6997B7896B4ECBE14BEEFC936
Malicious:	false
Preview:	../..... ....

C:\Users\user\AppData\Local\Temp\CabCF8F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Temp\CabCF8F.tmp	
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarCF9F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D48 5A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Covid-19 Payroll Tax Adjustment.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=Tue Apr 20 02:42:34 2021, length=10480, window=hide
Category:	dropped
Size (bytes):	2248
Entropy (8bit):	4.608603007241245
Encrypted:	false
SSDEEP:	48:8ZuW/XT0jFsL9I1YQh2ZuW/XT0jFsL9I1YQ/:8Zr/XojFCsYQh2Zr/XojFCsYQ/
MD5:	A4D482F324A3ECE0C901F5F6B7F7CDFF
SHA1:	60A79C75A0A271616E6BA263FBAA7A7B5AEB103A
SHA-256:	FBE284E82BE740F3780396CE35B2F048C8C0F18D85ABEA8C4D2E8F06F0D076B9
SHA-512:	E2EE10BF0A32D3FF549C96B3776F73493547F8C7F37E6CC68881588DD8001C45C99470B38BBD347EAA47E2986470E5281EC74C408D83FC73322D9B901BDACFA
Malicious:	false
Preview:	L.....F.... ....{...{...{...{..<..2.5...(.....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..(...RR. .COVID-~1.DOC..v.....Q.y.Q.y*...8.....C.o.v.i.d.-.1.9. .P.a.y.r.o.l.l. .T.a.x. .A.d.j.u.s.t.m.e.n.t...d.o.c.x.....-...8...[.....?J.....C:\Us ers\..#.....\\562258\Users.user\Desktop\Covid-19 Payroll Tax Adjustment.docx.;.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.v.i.d.-.1.9. .P.a.y.r.o.l.l. .T.a.x. .A.d.j.u.s .t.m.e.n.t...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.

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):	133
Entropy (8bit):	5.025364841875384
Encrypted:	false
SSDEEP:	3:HtoUc8RLo4RU+x+Uc8RLo4RUmxWtoUc8RLo4RUv:Ht35zRPJ5zRi35zR2
MD5:	1F471215981641DD8581692FE5F525D6

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	460F7521D2B66EA12562ACABAC72968A4481941A
SHA-256:	7B35DF2136C5CC51ECED3CB1D00D4EDAAE45207E521AC223CC5AB5AC790A1837
SHA-512:	FE959CDCCC822149011B53FF66605460106EDCD65BB14D0C20B755B39FA6AB60D891AAA2FC9DEFAFCCE3B2E59EDAB599B2D36A26B1BA269D9D9BC205F12D8 0A6
Malicious:	false
Preview:	[misc]..Covid-19 Payroll Tax Adjustment.LNK=0..Covid-19 Payroll Tax Adjustment.LNK=0..[misc]..Covid-19 Payroll Tax Adjustment.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:vdsCkWtW2llID9l
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...

C:\Users\user\Desktop\~$vid-19 Payroll Tax Adjustment.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:vdsCkWtW2llID9l
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:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.778256600131332
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% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Covid-19 Payroll Tax Adjustment.docx
File size:	10480
MD5:	f78e1a17152954d2c56e3de7f889065f
SHA1:	9ad2cffb62540c6ad60eee087c97cc756949adfd
SHA256:	606e7c0165678adb36211ad727f8d128577a06584034ee 39402b9a931f457b06
SHA512:	05089c96e04be77867cdadafc57a1a0a5f511ebbcae0702 37bd71302ed84ebb6f0051155ab8692d0ccc3eb639af4cf b58d58fd3f8cd74c08174b5168d0311073
SSDEEP:	192:77t5Z7p6Enlo2QOFipslkaCkMo2rIoVk0ipVH8Lad8 NXPEhMHsQO:Vj7p6ElzQJA5yIoGVcLhJPqEnO

General

File Content Preview:	PK.....4..R.....docProps/PK.....4..R.;q.....docProps/app.xml.S.n.!..W.?....Q.U.&..U9..%o.....QY@0..~}..x.Nz*.7.....K....l._..l.*.&4..V...v.ET..7....8b.7..'.l!b"..b..WbO..Rf.....=..!u@....mk.....'y9._K|!..6.q.....@.+..S.....YO.

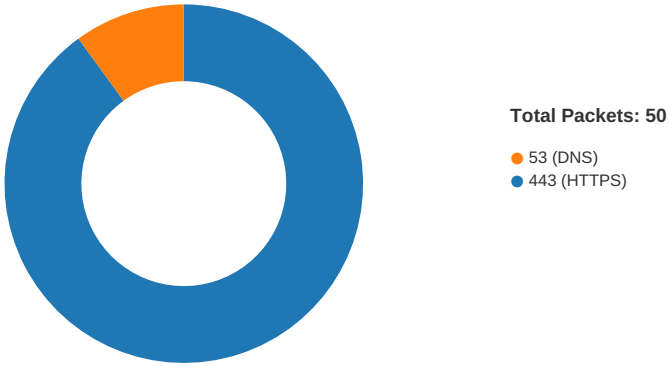
File Icon



Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 20:42:25.961451054 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.088267088 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.088479042 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.099739075 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.275042057 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.275063038 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.275078058 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.275085926 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.275105000 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.275250912 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.518917084 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.687149048 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.687175035 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.687361956 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.687403917 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.688298941 CEST	49167	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.690603018 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.814924955 CEST	443	49167	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.817434072 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.817639112 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.818710089 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:26.993246078 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.993275881 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.993288994 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.993297100 CEST	443	49168	18.211.24.111	192.168.2.22

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 20:42:26.993308067 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:26.993470907 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:27.250313997 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:27.414983034 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:27.415163994 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:28.784806967 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:28.973825932 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068414927 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068451881 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068476915 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068501949 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068526030 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068553925 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068578005 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068600893 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068608999 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068623066 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068624020 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068645954 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068646908 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068671942 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068691015 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068708897 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068711042 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068723917 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068733931 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.068736076 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068763018 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.068779945 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.070683956 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195308924 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195338964 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195367098 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195394039 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195446014 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195460081 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195465088 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195467949 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195488930 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195503950 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195518017 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195525885 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195545912 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195547104 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195578098 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195588112 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195610046 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195617914 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195638895 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195647001 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195667982 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195677996 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195698023 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195708990 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195725918 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195725918 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195755005 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195764065 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195784092 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195795059 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195812941 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195816994 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195847034 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195854902 CEST	49168	443	192.168.2.22	18.211.24.111

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 20:42:29.195874929 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195883989 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195903063 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195904016 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195933104 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195941925 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195961952 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.195971012 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.195991039 CEST	443	49168	18.211.24.111	192.168.2.22
Apr 19, 2021 20:42:29.196000099 CEST	49168	443	192.168.2.22	18.211.24.111
Apr 19, 2021 20:42:29.196019888 CEST	443	49168	18.211.24.111	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 20:42:25.887660980 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 19, 2021 20:42:25.952151060 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 19, 2021 20:42:27.745891094 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 19, 2021 20:42:27.795069933 CEST	53	53099	8.8.8.8	192.168.2.22
Apr 19, 2021 20:42:27.800374985 CEST	52838	53	192.168.2.22	8.8.8.8
Apr 19, 2021 20:42:27.852098942 CEST	53	52838	8.8.8.8	192.168.2.22
Apr 19, 2021 20:42:28.172858953 CEST	61200	53	192.168.2.22	8.8.8.8
Apr 19, 2021 20:42:28.231372118 CEST	53	61200	8.8.8.8	192.168.2.22
Apr 19, 2021 20:42:28.239871025 CEST	49548	53	192.168.2.22	8.8.8.8
Apr 19, 2021 20:42:28.292913914 CEST	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 19, 2021 20:42:25.887660980 CEST	192.168.2.22	8.8.8.8	0x15d4	Standard query (0)	admin.phishproof.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 19, 2021 20:42:25.952151060 CEST	8.8.8.8	192.168.2.22	0x15d4	No error (0)	admin.phishproof.com		18.211.24.111	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 19, 2021 20:42:26.275078058 CEST	18.211.24.111	443	192.168.2.22	49167	CN=*.phishproof.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Apr 07 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018	Fri Apr 08 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 19, 2021 20:42:26.993288994 CEST	18.211.24.111	443	192.168.2.22	49168	CN=*.phishproof.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Tue Apr 07 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018	Fri Apr 08 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2436 Parent PID: 584

General

Start time:	20:42:34
Start date:	19/04/2021
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:	0x13f0d0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A70475F6-E366-40C3-B2E6-22C3DC55A9E1}.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\~$vid-19 Payroll Tax Adjustment.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.Word\~WRS{A70475F6-E366-40C3-B2E6-22C3DC55A9E1}.tmp	unknown	1024	08 00 15 00 20 00 20 00 13 00 22 00 68 00 74 00 74 00 70 00 73 00 3a 00 2f 00 2f 00 61 00 64 00 6d 00 69 00 6e 00 2e 00 70 00 68 00 69 00 73 00 68 00 70 00 72 00 6f 00 6f 00 66 00 2e 00 63 00 6f 00 6d 00 2f 00 61 00 66 00 2d 00 44 00 62 00 68 00 38 00 6e 00 4d 00 6b 00 2e 00 70 00 6e 00 67 00 22 00 20 00 5c 00 2a 00 20 00 4d 00 45 00 52 00 47 00 45 00 46 00 4f 00 52 00 4d 00 41 00 54 00 20 00 5c 00 64 00 49 00 4e 00 43 00 4c 00 55 00 44 00 45 00 50 00 49 00 43 00 54 00 55 00 52 00 45 00 20 00 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....".h.t.t.p.s.:././.a. d.m.i.n...p.h.i.s.h.p.r.o.o.f. ..c.o.m./.a.f.- .D.b.h.8.n.M.k...p.n.g.". .\.*. .M.E.R.G.E.F.O.R.M.A.T. .\.d.I.N.C.L.U.D.E. P.I.C.T.U.R.E.	success or wait	1	7FEE90A9AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Covid-19 Payroll Tax Adjustment.docx	8494	288	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\F4E4F	success or wait	1	7FEE90A9AC0	unknown

Copyright Joe Security LLC 2021

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	binary	02 0B 06 04 03 05 04 04 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E4F	F4E4F	binary	04 00 00 00 84 09 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 62 68 CB 48 97 35 D7 01 4F 4E 0F 00 4F 4E 0F 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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 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	1385365550	1385365551	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1385365551	1385365552	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4E4F	F4E4F	binary	04 00 00 00 84 09 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 62 68 CB 48 97 35 D7 01 4F 4E 0F 00 4F 4E 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	04 00 00 00 84 09 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 4F 4E 0F 00 4F 4E 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	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				

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 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 FF FF FF FF				

Disassembly