ID: 322904
Cookbook: browseurl.jbs
Time: 03:57:07
Date: 26/11/2020
Version: 31.0.0 Red Diamond

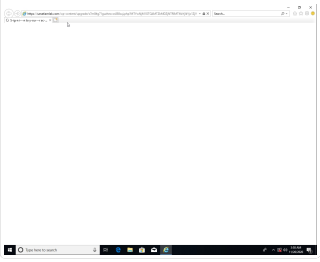
Table of Contents

Table of Contents 2
Analysis Report
http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==
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 6
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 15
No static file info 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 18
HTTP Packets 18
HTTPS Packets 18
Code Manipulations 18
Statistics 18
Behavior 18
System Behavior 19
Analysis Process: iexplore.exe PID: 6840 Parent PID: 800 19
General 19
File Activities 19
Registry Activities 19
Analysis Process: iexplore.exe PID: 6884 Parent PID: 6840 19
General 19
File Activities 20
Registry Activities 20
Disassembly 20

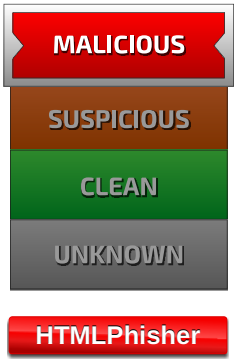
Analysis Report http://bihhwidigojbtkic.lfllavv.com/kam…

Overview

General Information

Sample URL:	http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==
Analysis ID:	322904
Most interesting Screenshot:	

Detection

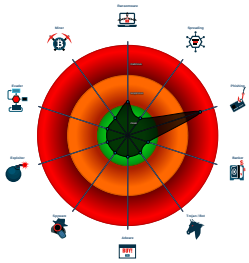


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid T&C link found

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6840 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6884 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6840 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

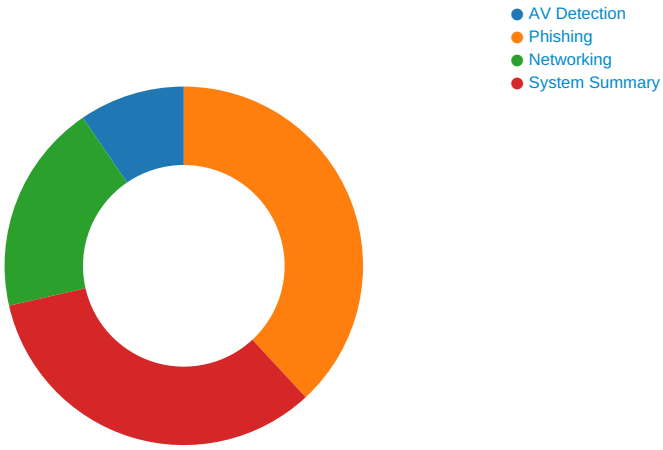
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\s7m8ltg71guzhecccs888xuj[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)

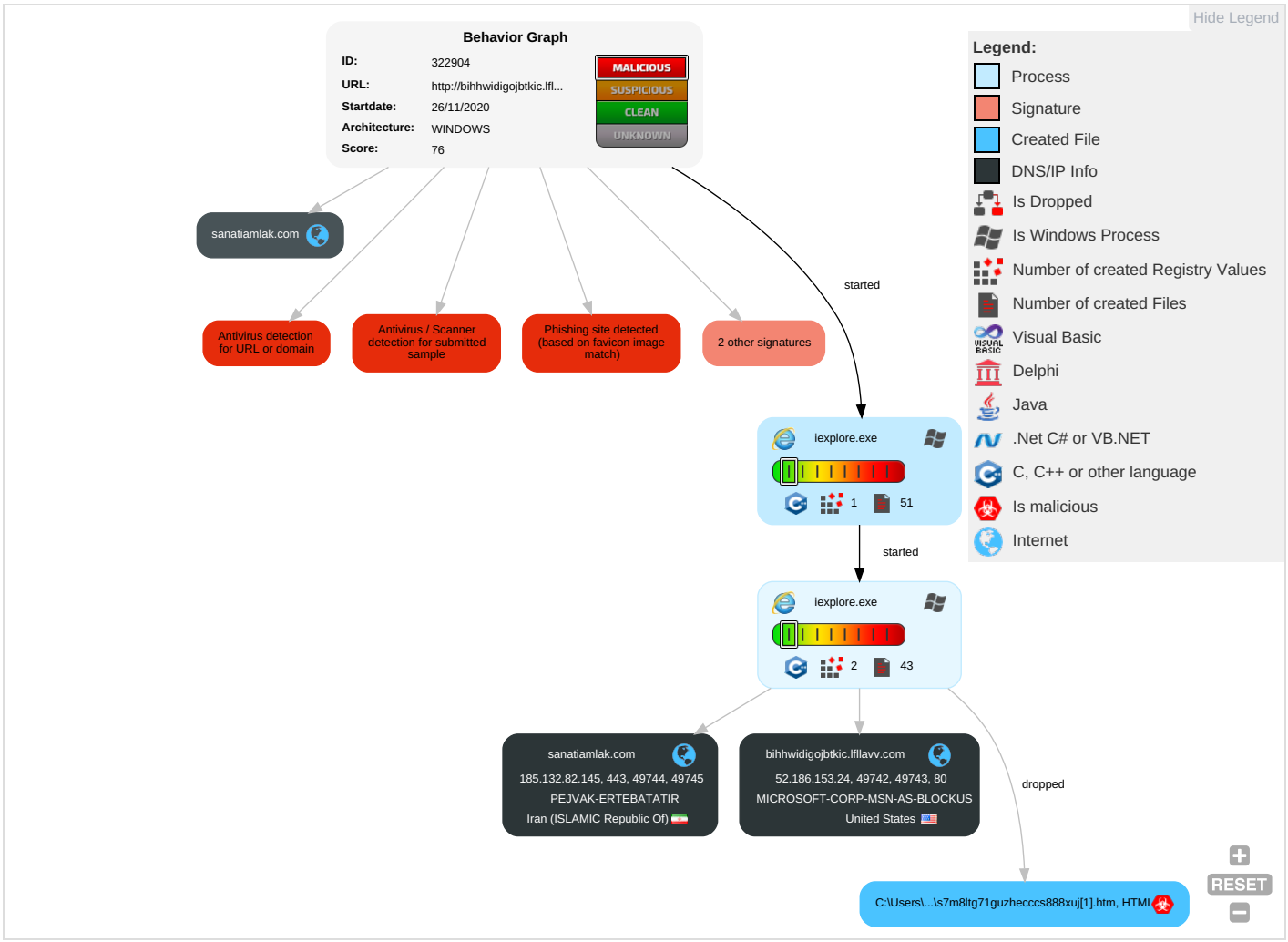
Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

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

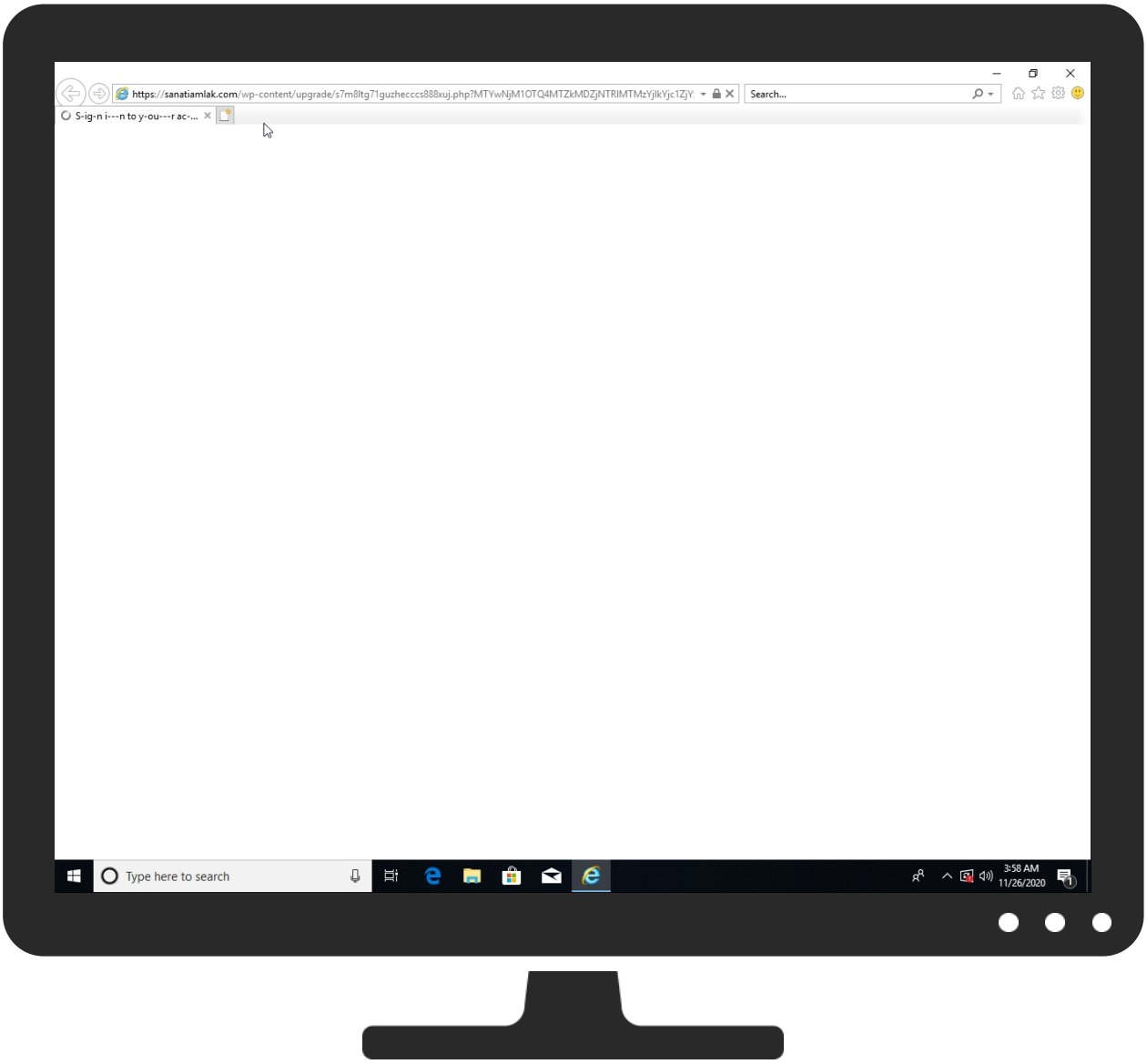
Behavior Graph



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://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==	0%	Avira URL Cloud	safe	
http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sanatiamlak.com/wp-content/upgrade/s7m8ltg71guzhecccs888xuj.php?MTYwNjM1OTQ4MTZkMDZjNTRlMTMzYjlkYjc1ZjYxZDhiY2U4OTBlZWU4OTcyNmFkYTE1MDk1MWM5OTc5YjQwYzJjMzgwNjE0YTk0OTZiYWE4Zg==&data=Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==Root	0%	Avira URL Cloud	safe	
http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://sanatiamlak.com/wp-content/upgrade/?corporate.actions.au2	0%	Avira URL Cloud	safe	
http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico~(	0%	Avira URL Cloud	safe	
http://https://sanatiamlak.com/wp-content/upgrade/s7m8ltg71guzhecccs888xuj.php?MTYwNjM1OTQ4MTZkMDZjNTRlMTMz	0%	Avira URL Cloud	safe	
http://https://sanatiamlak.coc.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==m/wp-content/upgra	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bihhwidigojbtkic.lfllavv.com	52.186.153.24	true	false		unknown
sanatiamlak.com	185.132.82.145	true	false		unknown

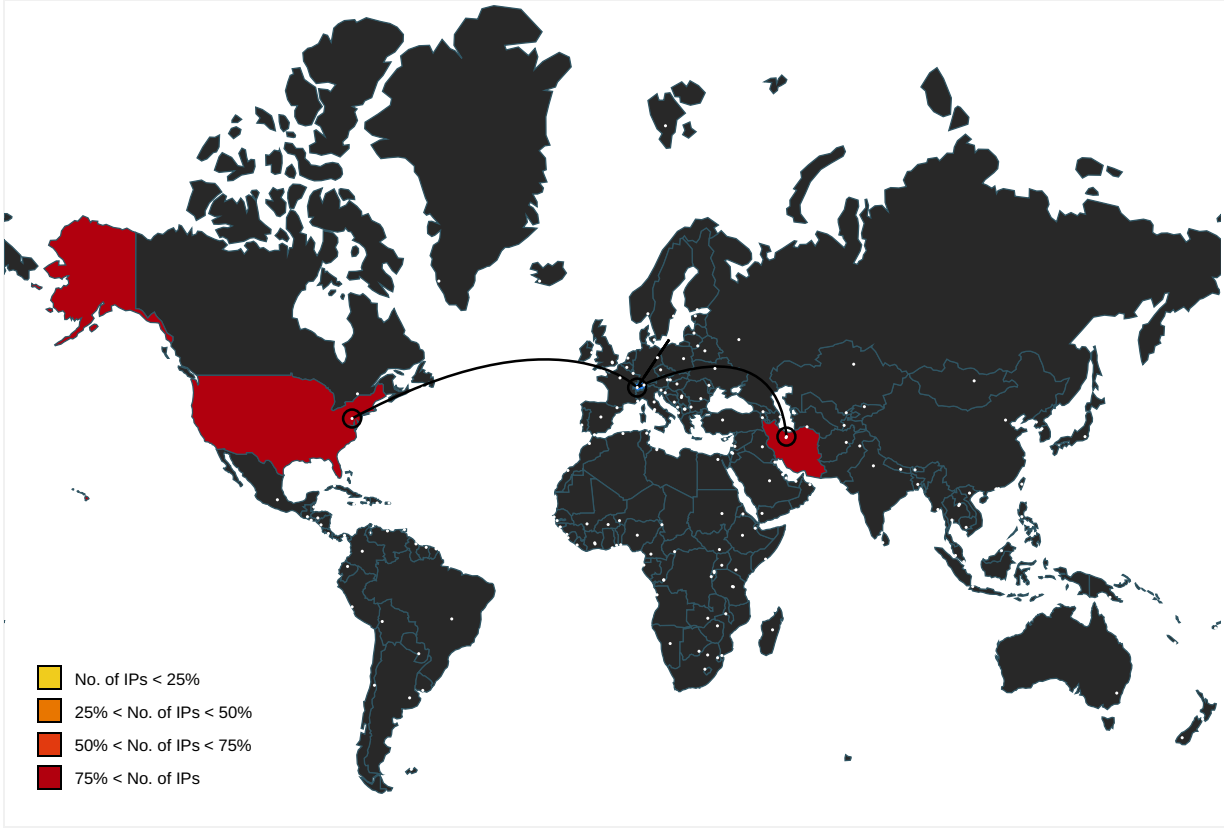
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://sanatiamlak.com/wp-content/upgrade/s7m8ltg71guzhecccs888xuj.php?MTYwNjM1OTQ4MTZkMDZjNTRlMTMzYjlkYjc1ZjYxZDhiY2U4OTBlZWU4OTcyNmFkYTE1MDk1MWM5OTc5YjQwYzJjMzgwNjE0YTk0OTZiYWE4Zg==&data=Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==Root	{2C0A73F0-2F93-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://sanatiamlak.com/wp-content/upgrade/?corporate.actions.au2	Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico~(	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://sanatiamlak.com/wp-content/upgrade/s7m8ltg71guzhecccs888xuj.php?MTYwNjM1OTQ4MTZkMDZjNTRlMTMz	~DF058445AA7ACBCBBD.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://sanatiamlak.coc.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==m/wp-content/upgra	{2C0A73F0-2F93-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.132.82.145	unknown	Iran (ISLAMIC Republic Of)		43212	PEJVAK-ERTEBATATIR	false
52.186.153.24	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322904
Start date:	26.11.2020
Start time:	03:57:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==
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:	9
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.phis.win@3/16@3/2

Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.83.120.32, 52.255.188.83, 52.147.198.201, 51.104.139.180 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, arc.msn.com.nsatc.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, arc.msn.com • VT rate limit hit for: http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==

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.{2C0A73EE-2F93-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8561428631936867
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2C0A73EE-2F93-11EB-90EB-ECF4BBEA1588}.dat	
SSDEEP:	192:rXZnZs2o9W0tMifBnJzMmhB9bDisf3nEjX:rJZboUghA0NxA
MD5:	B712895E973E62DE97F2CCEC75743DA1
SHA1:	38BD10678ED3228DE6DBA157DA840F2CB02BDF2B
SHA-256:	D84643D7FD7564F69DC05750E683BFC2EC5071F3D131AA6E2613ACAB20F35C5C
SHA-512:	CCEC65BE772496A966D09F3CB8CEF0C46B905C4A99B8F36F247882F29110BCD0A87F77EA2AC0371798917FEABD3313337F52BC605DD23583343EB3B443603278
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\{2C0A73F0-2F93-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	35370
Entropy (8bit):	2.18801284867805
Encrypted:	false
SSDEEP:	192:rsZzQI6mkmFjZ2kkWdMgYHV00Bsguk8lukmaqauhKuMu6ukhuF6dB:rs8TnmhoQugKVFs5NMVNDhzVjkIY
MD5:	DADDBA401E6D36277FEC0B6DE7E825CD
SHA1:	BA1572CFB689B6062AF2D67C80FD49B2D463695B
SHA-256:	83D735484425AB6BB42BAF73973614DD0605BA0034B1225367BD8D764E1267E6
SHA-512:	DCA5680CD2074884FA8B7628D6B5504BAC14DA542BA5973F4C6510FD508633250FE0BB2365F62B88C7EDB6E845602A284FC3DED473858FE8858838662D01B545
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\{35E4EA04-2F93-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5669699540556303
Encrypted:	false
SSDEEP:	48:Iw8WGcprBOGwpaf1G4pQ1nGrapbS8rGQpK4G7HpR7sTGIpG:rnZ8QP6hBS8FADT74A
MD5:	19E46E78E97E26111BFA3A4039EA8D71
SHA1:	78E9BD6726A70F1418AE13234358DFDC10A6E185
SHA-256:	439CADFA80C115FB6E243D3E9025A298E09CF2663645FB03D00EEE4915AD6BA0
SHA-512:	5650ADE2B062FD7F57BA5538CB507CF86D4E3EB2D8278298EC5898D47629064BBDC3FCD7DBEEEEAA578F5BD746905C02A5DC018DFD534A15D67B41CCF16197E
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	18176
Entropy (8bit):	3.0905696781372614
Encrypted:	false
SSDEEP:	48:9yyE/JmFyyE/GmFyyE/emFyyE/tgyyyyyyyyyyyyylmFyyE/DymFyyE/GQQQQQkW:EPmMImMQmMLmMomMsQQQQQkm/
MD5:	A19693B7CBEAC13D16ED8D1E68276B0B
SHA1:	736A58707C90FD6F5DE88FCC13A404934F019DC1
SHA-256:	EFD323B3279576BE6743CCDCA59755C3FAE3EAFED3CE5B53BF80C2D97C316E55
SHA-512:	015D5FA6D38276722AE3990321996723FD4954952216413EFABA11814AAB75D1A4D0316B9C4CDD3C8A79AAAE5878A5B708F6042F18606BFA82391E799175DA69
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat

Preview:	>.h.t.t.p.s.:././.s.a.n.a.t.i.a.m.l.a.k...c.o.m./.w.p.-.c.o.n.t.e.n.t./.u.p.g.r.a.d.e./.l.i.b./.i.m.g./.f.a.v.i.c.o.n...i.c.o.~(...............h(......(...................(...................................."P....... ....""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""" """""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333 333333333333333""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""""" """" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...3333333333333333333333333 33333""""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""""" ...333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	138
Entropy (8bit):	4.673581716398582
Encrypted:	false
SSDEEP:	3:gnkAqRAdu6/GY7voOkADFoHDSkMhKOZIbOlAQWbZJMDLJFyKyUYLn:7AqJm7+mmHLKIbOlA/JMDNFZyUYL
MD5:	BA1633F97C23DBF2D64FDCBD905B5B9D
SHA1:	E852874A3DEF0F9635DF3EC75BEF698EDE8CB3AC
SHA-256:	3A5BBC3E8447FC61CE241DD1B9F6458857218F33D686FE935353193D30410959
SHA-512:	433CFBCC97DCB0D0DF02CE9BC26F32B81C5A9758C8959116BA0AA8877FB12F390597269AEBA5EE160098FB10CBE71D517FD87FDB8BA373C097142F79CD30BC 6D
Malicious:	false
Reputation:	low
IE Cache URL:	http://bihhwidigojbtkic.lfllavv.com/kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ==
Preview:	<script type="text/javascript">window.location.href = "https://sanatiamlak.com/wp-content/upgrade/?corporate.actions.au2@ig.com"</script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\login[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	101788
Entropy (8bit):	5.304944776832708
Encrypted:	false
SSDEEP:	1536:QpHDglbuhw+ExmazA/PWrF7qvEAFiQcpmNtuhPyJRD:l74wyJZ
MD5:	4DB4A299AE7E73B3CB53351867416D0C
SHA1:	36C0DFF7A6742EAD3229E476F05C559069C3080F
SHA-256:	10C50B88EBF99FDF813A4CCE86BA218A6E2EA3D266146520529F1E1BDDC5EBD3
SHA-512:	8EB086FC241C314DDD4B15AC6F34DBD61B838E2D7C2B535A02AF2A83A92294AB1C79EB122EFCA8FF648346F4515B35EDEEB13DC5E79EBC2C7E9ACCC4AC5B AA76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sanatiamlak.com/wp-content/upgrade/lib/css/login.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.--- START OF THIRD PARTY NOTICE ---..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise.../-------------------------- --.twbs-bootstrap-sass (3.3.0).//---..The MIT License (MIT)..Copyright (c) 2013 Tw Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\white_ellipsis[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:	B9135D934B9EA50B51BB0316E383B114C8F24DFE75FEF11DCBD1C96170EA59202F6BAFE11AAF534CC2F4ED334A8EA4DBE96AF2504130896D6203BFD2DA6913 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sanatiamlak.com/wp-content/upgrade/lib/img/white_ellipsis.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\white_ellipsis[1].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-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.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-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\logo2[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://sanatiamlak.com/wp-content/upgrade/lib/img/logo2.svg
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\CS6IXJW6\arrow[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:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9 F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sanatiamlak.com/wp-content/upgrade/lib/img/arrow.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\OR0WKIO1\background[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2], progressive, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	31419
Entropy (8bit):	7.838593850267985
Encrypted:	false
SSDEEP:	768:B2CG6sPLHj1DDtLEHZwbz0yDEr+q5jc0T7KEE:4CG6sTDFRLKZwbzpDEr+Zc7e
MD5:	B204756661AE1F820ACDBF507B2C0FE7
SHA1:	8BCC62CD820991FE0C4D35C2E397E9D2E225D4A0
SHA-256:	A33593E9043EFEFBAF94D9CA220C885CE1C42DD2A7707F30ED072D7D71587DA5
SHA-512:	F115CD7216716F759575B0411028CFA56049150F54D2692CF8998E47D82959BA1521CB9462DF6E5496C51B08ED736FFC0CF4BB70C0328099143293CDDB4B570E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sanatiamlak.com/wp-content/upgrade/lib/img/background.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\background[1].jpg

Preview:	......JFIF.....`.`.....VExif..MM.*................>..........F.(...........................`.......`..! !,,;...! !,,;......8. ..."..&`...n.... .Z...&.P....UZ. .....%`....d.j...[@.....@.....C9kD...4..k@.Z36-jP..Y...2...f....4......b...*....uA..t..b.....3 .T....n....f... .+"KR..A.FC.`.d&..f. !t...@]P]P...b...g ....d.t...@.-.&..).".D.i.J.....2X@.H.HR.....T.`...0.D..0......3.....@..........hH....sL.. ...r[I.Am.U.]Pn.@..0.kL.&`.2.n.L....h.5..@bS[U.$-f@.1.ee5....".$...E......k L..w 9..........`h.......m..e..f.....$S9-&a...`.U..R....7B..... ....P.:.......V..Z..P.U.# .s...$.&...&.....Ahk@.....9].....V..B,u%R...h.7r.w6....,.a5-.....@."f..J..]...{.uCt..b...rD.4$I@........i2]....... ..%...&..a0.......h....7rkE.LCy.9...$.*..u@.oi..]Vd7B.T...3fE........"..].H.M..uQ.QjK.sg&....%.$...@n....5)M.eu@.U(....H..*`3.&a2hFi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\favicon[1].ico

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sanatiamlak.com/wp-content/upgrade/lib/img/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(...................(...................................."P.."""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\logo3[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 4-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1750
Entropy (8bit):	7.784821733371315
Encrypted:	false
SSDEEP:	24:W6Yai7i2Tz46sC7PbpHZMYYsOWFzyKgXW0n9/ND1LCgz7AXtew1pcv8m5PRlQXt+:9KtTzx/HxRF+KKWE/B1LCgYXtIZRlN
MD5:	533E293F0C8947ADA653B47C00E394E2
SHA1:	0F507BB89C42F937A290D0EEDA3F2E0DBFCAD5C1
SHA-256:	B5D587F6C48A9B22BBE97150249E0C0655AC1780BD273431480A22F8A5BFEF6C
SHA-512:	B91127D6C27E270F7AAB0A83054451FFF4719C587A425F36EC32F4E532CF4E4D74505AAC71ED3629769552924BC9A9C8CB7F73667B0D20EA5AAED587BCD3E17
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://sanatiamlak.com/wp-content/upgrade/lib/img/logo3.png
Preview:	.PNG........IHDR...V...H....._*......gAMA......a.....sRGB........0PLTEGpL..D>......tRNS.w.D...3f..".U...1;...)IDATh..ZMh\U...t&...L#..:I(.P..7..T$V ....1h....Eq!..Q.....q.....&Bq.Up.".B..$.L..Os...}..s...%3.w........=..s...a....T.9.i.......'...\.7X...~......c..........3.`.6.Z.T......m..U.YM*.....K-..Y..g...<..-.z...Bs.....uZ;.F.w...Y..m......m... ..jMYl..RkzQ.{]..V...i..i.R.V...e..yj....Mk..[g.y#h..,.u.].K.f..d......b.u..L.a..Kk...5r....Rk...v.\../..Ekz...........i..,.K..?F......).<..x...=o.k..}'g.0.o...n.......K.L..l..B...5......4..`.CD+...-1...E. ((.=k.....}.H.dqe.Q..b.%.C.\.e..=...m.\k.".4_......Y5.S......U....j.ZV.*wY;..^.X......&.1.!.*..;m.,..?..`.<t.Z....3@...../...j..rC>x>.e.,.=...F.....p..U...J...5d....>.~d._\.....o.....j...\.z8.8..a... <.MI8.]...3.V.Z.G....V.S..ta.c.m..Z."k.&y....a....p..Z.h..q..a.#......s>4O}.F.&9....R.$....\....>..0....F.."......8f.....i-X....".aX.1....j..#k.c.U.9).ta.#K..!..z..zXD...&8.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\s7m8ltg71guzhecccs888xuj[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	4879
Entropy (8bit):	3.503009133459594
Encrypted:	false
SSDEEP:	48:NIV53h2OBWmvAavqWRtpPkf0UGvIDiUzSGVv:NInUkl7LkMdSmGVv
MD5:	BFDF928CEB75ABE05314B55BBC59E38D
SHA1:	A4259DD254B0AF95F106189AA805ABED33E4B3EB
SHA-256:	1C53EA945C96009E1AB9064D06EAFE9A2C3AFCEE2BC0548DCCF1236D1E579C83
SHA-512:	B8622FF5A6BDA20812649C152E50E75649CC6D07AB06817DF992A13F3A3EB7806E279FF8721DE930A14C4708046C0ED346550B2A7F2DD25BD72CAD6068BDE22
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\s7m8ltg71guzhecccs888xuj[1].htm, Author: Joe Security
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\s7m8ltg71guzhecccs888xuj[1].htm

Preview:	<html dir=ltr lang=en>..<title>S.ig.n i...n to y.ou...r ac...cou.nt</title>..<link href=lib/img/favicon.ico rel="shortcut icon">..<link href=lib/css/login.css rel=stylesheet>..<div>..<div>..<div class="app background"> .. <div style=background-image:url(lib/img/background.jpg)></div> .. </div>.. </div>.. <div > </div>.. <form method=post action=process>.. <div class=outer>..<div class="app middle">..<div class=background-logo-holder>..<img src=lib/img/logo3.png class=background-logo>..</div>..<div class="app fade-in-lightbox inner">..<div class=lightbox-cover>..</div>..<div>..<img src=lib/img/logo2.svg class=logo>..</div>..<div>..<div>.. .. .. .. <div class="animate slide-in-next">.. <div>..<div class=identityBanner>......<img src=lib/img/arrow.svg>......<div cl

C:\Users\user\AppData\Local\Temp\~DF058445AA7ACBCBBD.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	46395
Entropy (8bit):	0.8193895554145566
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+RP98fsVqVjhuDluWuhKuMu6ukhuF:kBqoxKAuqR+RP98fsVqVjIDMPhzVjkI
MD5:	D793E61EC5F79EC6AC4A33FA03820235
SHA1:	4EE23FBCAFF95700602D92F205DED74E8B9D7B1B
SHA-256:	88EA3588A4ACC49113E830CA4121D64CA8F0CACF6C7F566C1F15CB19D3ECC5F6
SHA-512:	561988837869C87B3BC3C514A9F721E752E1E9C5CAD0BB717626D85732F497E32B80E8F0C8D77A7DC6F0E46EE6A1D03DF141079FCA41E222BAA3EA4AC7520A3E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF0C7E4045ADA69AC9.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3741423780685993
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAsncDuth4:kBqoxxJhHWSVSEab+bw
MD5:	B28C9B7BF08302CF7E564B67DC270CEB
SHA1:	9E8949D9C77A8479EBF09A51CA4FA4B61BD02144
SHA-256:	795E6FE13F9DA3405EAA82A8F370CEBEA7F9F38CF28B628CCFBD1930AA450E94
SHA-512:	D22303AD3032AE499794311186C9067C14FB1C87C246CFFD5DE2CCFBD06D92532EA10CAC00C930B38F90EA1DCF008729F4EBB163AE1A5D90874CA8266723D78
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFECEF3B821227381B.TMP

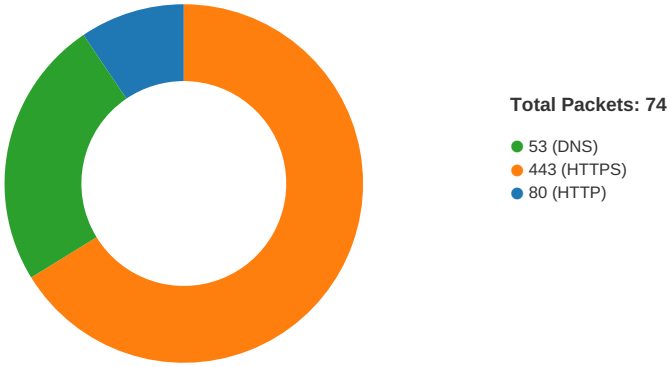
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4764564699045098
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9losi9losS9lWsQ4L5f:kBqoIm465f
MD5:	A88FEA16A348DFF8D8D39603073867AC
SHA1:	E2CE5ADF83ECAD87A9E28DD5EDAF5B6FB04C6FB6
SHA-256:	B3C804675108BDDD92DB485BDE5DA47A9B9F348AEC17BD167F6DEAA62E127886
SHA-512:	AA0C0C3D544E8F44FCF060C8093C742830E000814BF6492924BC6FFEF9456A4A8F718A706EEE7120BBD2E385A4106C5A093CE17300F29A5576E515EC46C8ED9D
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



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 03:57:53.773441076 CET	49742	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:57:53.774322987 CET	49743	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:57:53.873954058 CET	80	49742	52.186.153.24	192.168.2.4
Nov 26, 2020 03:57:53.874074936 CET	49742	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:57:53.875099897 CET	80	49743	52.186.153.24	192.168.2.4
Nov 26, 2020 03:57:53.875178099 CET	49742	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:57:53.875363111 CET	49743	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:57:54.022218943 CET	80	49742	52.186.153.24	192.168.2.4
Nov 26, 2020 03:57:54.382567883 CET	80	49742	52.186.153.24	192.168.2.4
Nov 26, 2020 03:57:54.382673979 CET	49742	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:57:54.761099100 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:54.761235952 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:54.896867037 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:54.897156954 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:54.900469065 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:54.900696039 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:54.905452013 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:54.905530930 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.041703939 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.043356895 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.045660973 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.045685053 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.045696020 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.045710087 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.045749903 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.045789957 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.046346903 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.046375036 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.046387911 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.046427011 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.046468973 CET	49745	443	192.168.2.4	185.132.82.145

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 03:57:55.047341108 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.047482014 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.087569952 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.095724106 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.107621908 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.222908974 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.223109007 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.246413946 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:55.246556997 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:55.269767046 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:57.455882072 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:57.456187963 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:57.465881109 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:57.466150045 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:57.470889091 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:57:57.604825020 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:57:59.892482996 CET	80	49742	52.186.153.24	192.168.2.4
Nov 26, 2020 03:57:59.892601967 CET	49742	80	192.168.2.4	52.186.153.24
Nov 26, 2020 03:58:02.848877907 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:02.849015951 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:02.864798069 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:02.864959002 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:02.869220018 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:03.002850056 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.758017063 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.758050919 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.758188009 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.758248091 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.767951965 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.768114090 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.815947056 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.816534996 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.816596031 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.817563057 CET	49756	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.818805933 CET	49757	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.819803953 CET	49758	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.820734978 CET	49759	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.947655916 CET	443	49756	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.947828054 CET	49756	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.949368000 CET	49756	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.949953079 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.952665091 CET	443	49745	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.952761889 CET	49745	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.959686995 CET	443	49759	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.959836006 CET	49759	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.960494995 CET	49759	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.961143970 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.961180925 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.961342096 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.961383104 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.963570118 CET	49744	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.971949100 CET	443	49757	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.972124100 CET	49757	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.977087975 CET	443	49758	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:05.977209091 CET	49758	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.988023043 CET	49757	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:05.988097906 CET	49758	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:06.077620983 CET	443	49756	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:06.078577995 CET	443	49756	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:06.078679085 CET	49756	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:06.079349041 CET	49756	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:06.085462093 CET	49756	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:06.098725080 CET	443	49759	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:06.099703074 CET	443	49759	185.132.82.145	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 03:58:06.099783897 CET	49759	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:06.100337982 CET	49759	443	192.168.2.4	185.132.82.145
Nov 26, 2020 03:58:06.102144003 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:06.102185011 CET	443	49744	185.132.82.145	192.168.2.4
Nov 26, 2020 03:58:06.102226973 CET	443	49744	185.132.82.145	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 03:57:50.622629881 CET	51726	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:50.657886028 CET	53	51726	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:52.628283024 CET	56794	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:52.665568113 CET	53	56794	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:53.725411892 CET	56534	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:53.764386892 CET	53	56534	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:54.566170931 CET	56627	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:54.758038998 CET	53	56627	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:56.239062071 CET	56621	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:56.274701118 CET	53	56621	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:56.928513050 CET	63116	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:56.955637932 CET	53	63116	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:57.622745991 CET	64078	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:57.649894953 CET	53	64078	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:58.539633036 CET	64801	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:58.575023890 CET	53	64801	8.8.8.8	192.168.2.4
Nov 26, 2020 03:57:59.810678005 CET	61721	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:57:59.846384048 CET	53	61721	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:00.750513077 CET	51255	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:00.777806044 CET	53	51255	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:02.919147968 CET	61522	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:02.954592943 CET	53	61522	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:03.639828920 CET	52337	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:03.677198887 CET	53	52337	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:04.390418053 CET	55046	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:04.417942047 CET	53	55046	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:05.042419910 CET	49612	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:05.069506884 CET	53	49612	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:05.904109955 CET	49285	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:05.931648016 CET	53	49285	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:06.563687086 CET	50601	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:06.590711117 CET	53	50601	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:11.092849016 CET	60875	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:11.128585100 CET	53	60875	8.8.8.8	192.168.2.4
Nov 26, 2020 03:58:14.258075953 CET	56448	53	192.168.2.4	8.8.8.8
Nov 26, 2020 03:58:14.285235882 CET	53	56448	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 03:57:53.725411892 CET	192.168.2.4	8.8.8.8	0x1060	Standard query (0)	bihhwidigo jbtkic.lfllavv.com	A (IP address)	IN (0x0001)
Nov 26, 2020 03:57:54.566170931 CET	192.168.2.4	8.8.8.8	0x93d1	Standard query (0)	sanatiamlak.com	A (IP address)	IN (0x0001)
Nov 26, 2020 03:58:11.092849016 CET	192.168.2.4	8.8.8.8	0xe8ae	Standard query (0)	sanatiamlak.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 03:57:53.764386892 CET	8.8.8.8	192.168.2.4	0x1060	No error (0)	bihhwidigo jbtkic.lfllavv.com		52.186.153.24	A (IP address)	IN (0x0001)
Nov 26, 2020 03:57:54.758038998 CET	8.8.8.8	192.168.2.4	0x93d1	No error (0)	sanatiamlak.com		185.132.82.145	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 03:58:11.128585100 CET	8.8.8.8	192.168.2.4	0xe8ae	No error (0)	sanatiamlak.com		185.132.82.145	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bihhwidigojbtkic.lfllavv.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	52.186.153.24	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 03:57:53.875178099 CET	112	OUT	GET /kampo/Y29ycG9yYXRlLmFjdGlvbnMuYXUyQGlnLmNvbQ== 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: bihhwidigojbtkic.lfllavv.com Connection: Keep-Alive
Nov 26, 2020 03:57:54.382567883 CET	113	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 02:57:54 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.4.12 X-Powered-By: PHP/7.4.12 Content-Length: 138 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 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 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 73 3a 2f 2f 73 61 6e 61 74 69 61 6d 6c 61 6b 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 67 72 61 64 65 2f 3f 63 6f 72 70 6f 72 61 74 65 2e 61 63 74 69 6f 6e 73 2e 61 75 32 40 69 67 2e 63 6f 6d 22 3c 2f 73 63 72 69 70 74 3e 0a Data Ascii: <script type="text/javascript">window.location.href = "https://sanatiamlak.com/wp-content/upgrade/?corporate .actions.au2@ig.com"</script>

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
Nov 26, 2020 03:57:55.045710087 CET	185.132.82.145	443	192.168.2.4	49744	CN=mail.sanatiamlak.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 23 21:58:40 CEST 2020	Thu Jan 21 20:58:40 CET 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6840 Parent PID: 800

General

Start time:	03:57:51
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6307f0000
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	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: 6884 Parent PID: 6840

General

Start time:	03:57:52

Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6840 CREDAT:17410 /prefetch:2
Imagebase:	0x170000
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