ID: 321434
Sample Name: sc.com
Cookbook:
defaultwindowshtmlcookbook.jbs
Time: 05:03:32
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

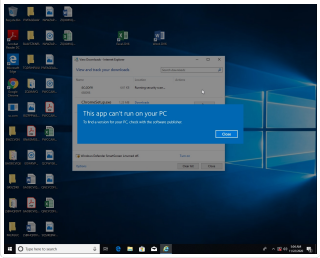
Analysis Report sc.com

Overview

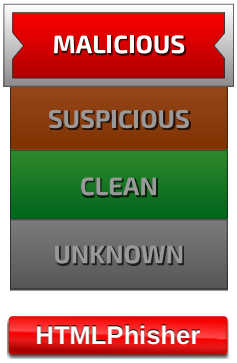
General Information

Sample Name:	sc.com
Analysis ID:	321434
MD5:	a2f3a68db7863f4..
SHA1:	fe611bbce708b77.
SHA256:	5411a2337cd4c6..

Most interesting Screenshot:



Detection

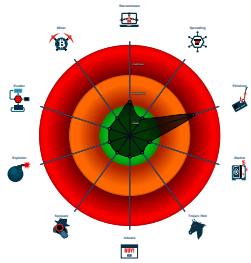


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected HtmlPhish_10

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5624 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1720 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5624 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

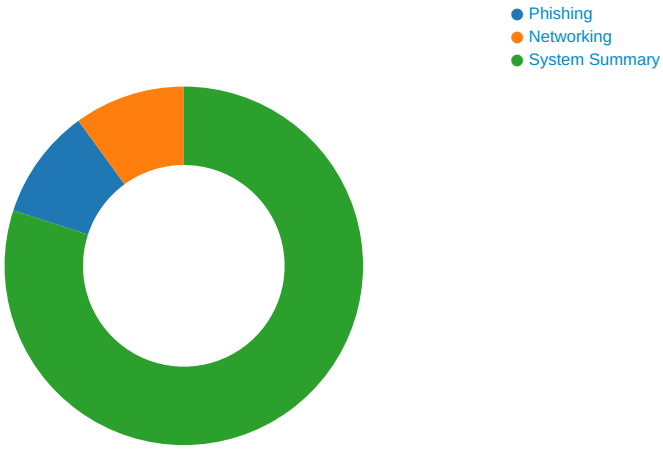
Initial Sample

Source	Rule	Description	Author	Strings
sc.com	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

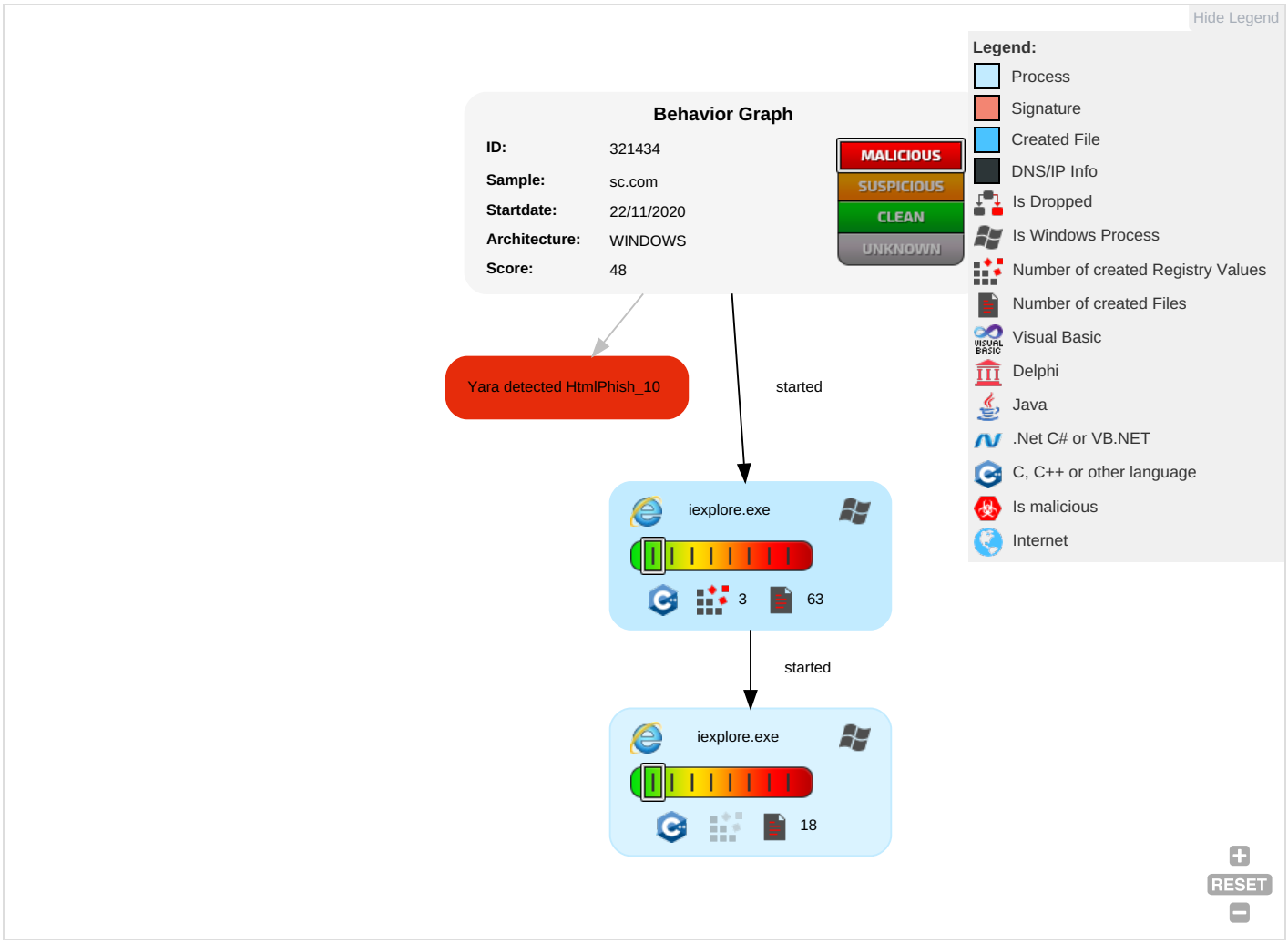
Phishing:

Yara detected HtmlPhish_10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

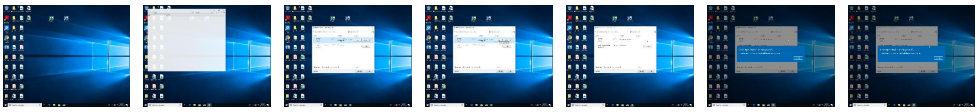
Behavior Graph

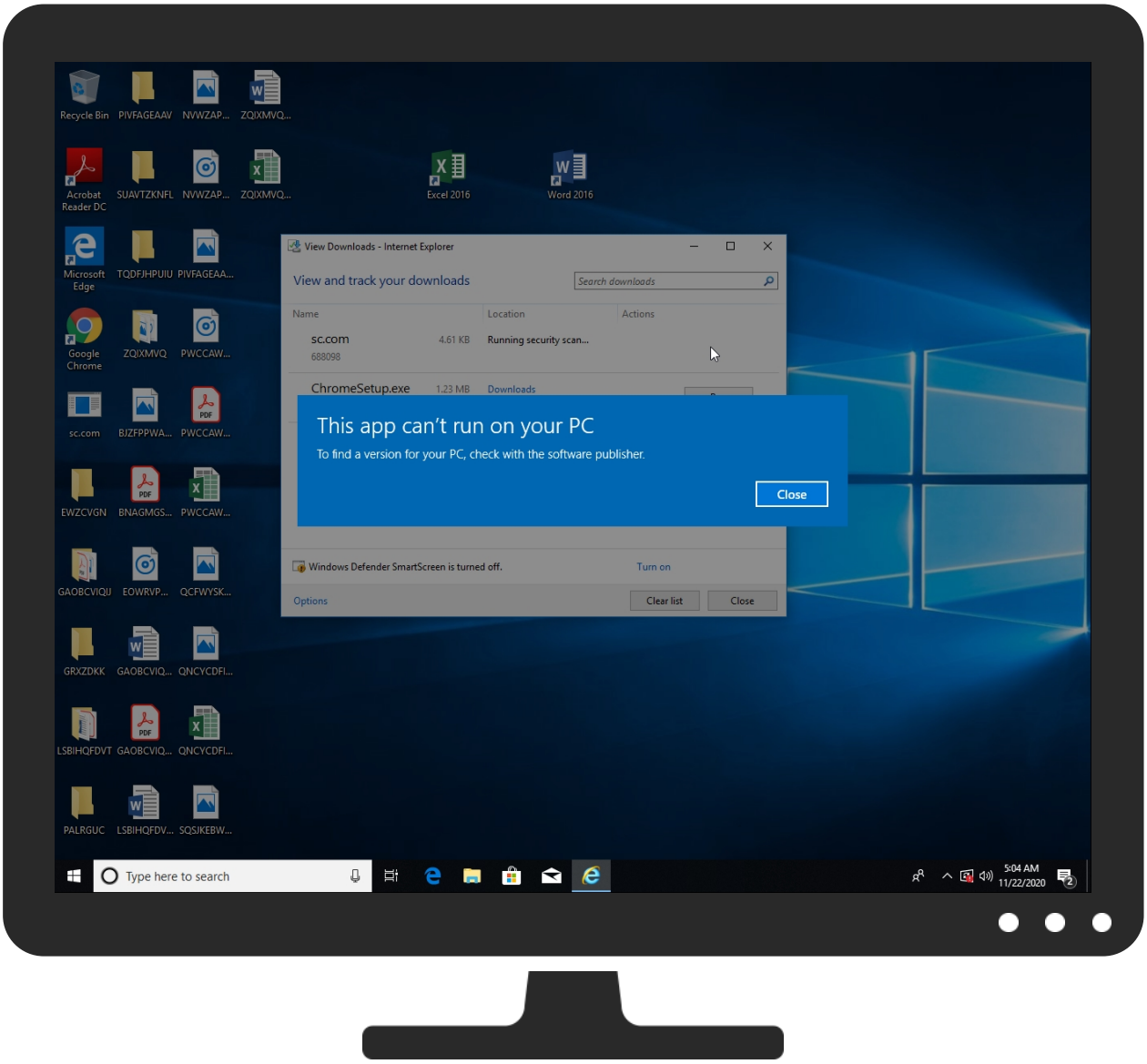


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
0	1%	Virustotal		Browse
http://https://pikap.kz/wp-admin/wed/server5.php	0%	Virustotal		Browse
http://https://pikap.kz/wp-admin/wed/server5.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
0	true	• 1%, Virustotal, Browse	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i.ibb.co/gtKmtC9/officebg.png	sc.com	false		high
http://https://i.ibb.co/F3yr74z/forgotpass.png	sc.com	false		high
http://https://i.ibb.co/7CKgHCt/ep.png	sc.com	false		high
http://https://i.ibb.co/9qFGmjh/miciconlogo.png	sc.com	false		high
http://https://passwordreset.microsoftonline.com/	sc.com	false		high
http://https://pikap.kz/wp-admin/wed/server5.php	sc.com	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://i.ibb.co/r5zjhmN/officebg2.png	sc.com	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321434
Start date:	22.11.2020
Start time:	05:03:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sc.com
Cookbook file name:	defaultwindowshtmlcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.winCOM@4/5@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .com

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.83.120.32, 52.255.188.83, 204.79.197.200, 13.107.21.200, 52.147.198.201, 51.104.146.109, 152.199.19.161, 2.20.84.85, 20.54.26.129, 205.185.216.42, 205.185.216.10, 51.11.168.160, 92.122.213.247, 92.122.213.194, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.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.{39FD2C44-2CC3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.7956995869487435
Encrypted:	false
SSDEEP:	96:r1/ZGZ92n9W0jt0Bmf0Mf5M09/0ZrCW7p/2:rJZGZ92n9W6tFfjxMiknx2
MD5:	4907CE853EF4E98EC4DC45391D8DE412
SHA1:	F71E80E1977CA41ECD18437DCF74E7B1980B0FE8
SHA-256:	5DFDCD1F151D479B9D9F7AAB499D798495AC2CFAEC68AB99713F8E714A3C79AE
SHA-512:	49AFE853B3046AE1016A1523CAE3B3FD964982259EC4F264693993808B1DB860577B305B59CD3F16659747D6325EF79DBE5F4CFE711703EC859D9FE4E43E54AC
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\{39FD2C46-2CC3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5994825180714751
Encrypted:	false
SSDEEP:	48:IwuZGcpr7GwpavZG4pQtGrapbStrGQpBuGHHpc0sTGUpQdeGcpm:ru/ZVQv76NBStFj920k64g
MD5:	B5F7FB94BAD916EAC8AEEC5EAA5E6EF8
SHA1:	FF28D3CC2480CEFF59C5F1F6A7A1BBD74876E066
SHA-256:	457E8276346628D18FD4E8F5B4ABC94819A17F4ACC3F4CBDC91DB9DEAD67C9FF
SHA-512:	FD061127E25232A73C8FEA98500A21580FF2DF86F4DB93121C94A7B2572D49C692AFFF60C75AB296426A37811EB7570A336790F926281616EBF498AB64DE5969
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.44290456303799
Encrypted:	false
SSDEEP:	3:oVXVP7KVf7W8JOGXnFP7KV6UCn:o9xKliqBKo
MD5:	2BC7190F8B2A23B4141C9A5902E75A2B
SHA1:	2069ECD2D922B238804EAD83EBB509000BA66DFC
SHA-256:	A693ED9EDE98E568A55BC69EC59EBE73C34044854877020ED94AF78FC4855255
SHA-512:	A667464DD5503E59E04ABF87D6D050A333E19A1747A8B4032305587951BDD24E023592C841C2C5F0F85EA3DB01A1BDABD79487C17D503EACFF38E5ADB508D11B
Malicious:	false
Reputation:	low
Preview:	[2020/11/22 05:04:18.682] Latest deploy version: ..[2020/11/22 05:04:18.697] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF94625A1E314DF9D3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.3307972330823734
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwz9lwz9l29/9l2F9lak:kBqoxKAuvScS+Mq9+cdy

C:\Users\user\AppData\Local\Temp\~DF94625A1E314DF9D3.TMP	
MD5:	2FF2BF692E4C77EC54170E6D352C36D1
SHA1:	36D490BA77703B911538F1A3DF5B5C8B379506EF
SHA-256:	47DABF286F8AC370AFA2870F60F9D4919DF200CF2EB96B62746EEBF59A4A0538
SHA-512:	E9EBC75CA07B117786E8CF232905C988B0B0C3BAD58CA989B3DC5586170152653A7C94A9190CC9232F72CC78DAE26FD2C5FC07C57EA502B82981F5C0EF3E924
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF37C87F1E61570B4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981
Entropy (8bit):	0.44419176970341645
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lojF9lop9lWUJmE9:kBqoIysUsE9
MD5:	E9D86FBFAFF79C4C0E992EEF7C920487
SHA1:	38D458E11137BA3523D5A510310D89F4A5AE687C
SHA-256:	8FE5D7274A37E71FC871EFE848EB12E879A4518EFCA4D1F35074F85FAED4EC0F
SHA-512:	FB406E2F0AA4656FD031DB8467CDE39CBFCE035E5F2DC36B366AD21069DA4CAF7100B548E7227F1D5AC388FC91CCD6C546B1BB731B39F5656FBE5285E68109E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PHP script, ASCII text, with CRLF line terminators
Entropy (8bit):	5.433898732889625
TrID:	• HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (12001/1) 20.69% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11501/1) 19.83% • HyperText Markup Language (11001/1) 18.97%
File name:	sc.com
File size:	4725
MD5:	a2f3a68db7863f4da11cf0255a4969e4
SHA1:	fe611bbce708b77bab1b9c31eb3dd30c4a7b763a
SHA256:	5411a2337cd4c63d1b0740ca513bc5c958b37777f10de80f96217368a3191b89
SHA512:	3f1bb71a5e2f6aa6482125ec887f5b8895516b41a402518179c46437b222e88aed5a24378c2aacf299f8d411cb0b7c4d3e8f36f7ae8add8ec2d2565247f7c9c2
SSDEEP:	96:b80F7Mb5M1eFSm4i0PKgdZpYUGBAxXrgsxo:b80F7Mb5M1zm10PKgtvGBA9Zo
File Content Preview:	<?php..function getloginIDFromlogin($email)..{..$find = '@';..$pos = strpos($email, $find);..$loginID = substr($email, 0, $pos);..return $loginID;..}..function getDomainFromEmail($email)..{..// Get the data after the @ sign..$domain = substr(strrchr($emai

Network Behavior

UDP Packets

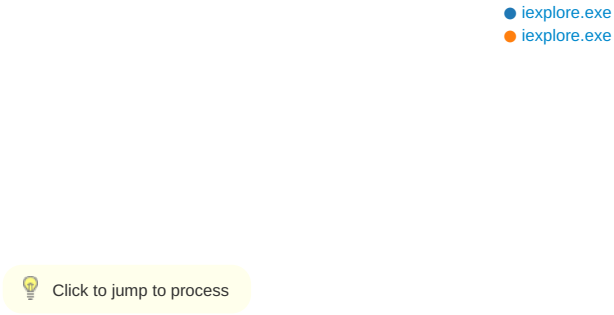
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 05:04:18.505337954 CET	60152	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:18.551997900 CET	53	60152	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:19.515686035 CET	57544	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:19.551600933 CET	53	57544	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:20.072047949 CET	55984	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:20.118105888 CET	53	55984	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:21.648971081 CET	64185	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:21.676378965 CET	53	64185	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:22.407416105 CET	65110	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:22.434619904 CET	53	65110	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:23.092139006 CET	58361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:23.119343996 CET	53	58361	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:23.729373932 CET	63492	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:23.764771938 CET	53	63492	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:24.356817007 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:24.384241104 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:24.993370056 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:25.029124022 CET	53	60100	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:25.870409966 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:25.906217098 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:26.597121954 CET	50141	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:26.624509096 CET	53	50141	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:27.246165037 CET	53023	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:27.273411989 CET	53	53023	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:27.958231926 CET	49563	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:27.993649006 CET	53	49563	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:28.718867064 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:28.754568100 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:29.618155003 CET	59349	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:29.654743910 CET	53	59349	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:30.313848972 CET	57084	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:30.349673033 CET	53	57084	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:31.138428926 CET	58823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:31.165664911 CET	53	58823	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:31.801748991 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:31.837255001 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:33.224858046 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:33.251946926 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:35.792715073 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:35.819859982 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:36.537048101 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:36.564412117 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:40.754169941 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:40.781481981 CET	53	57762	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:48.513592005 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:48.531310081 CET	50713	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:48.552469015 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:48.571352959 CET	53	50713	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:49.505681992 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:49.545350075 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:50.518254042 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:50.556442976 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:52.533986092 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:52.571835041 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:53.138783932 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:53.189985037 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 05:04:56.534576893 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:04:56.570269108 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 05:05:04.232932091 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:05:04.260068893 CET	53	58987	8.8.8.8	192.168.2.3
Nov 22, 2020 05:05:15.767765999 CET	56579	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:05:15.803425074 CET	53	56579	8.8.8.8	192.168.2.3
Nov 22, 2020 05:05:18.788387060 CET	60633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:05:18.825659037 CET	53	60633	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 05:05:50.209261894 CET	61292	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:05:50.236398935 CET	53	61292	8.8.8.8	192.168.2.3
Nov 22, 2020 05:05:51.595794916 CET	63619	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:05:51.631422043 CET	53	63619	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5624 Parent PID: 792

General

Start time:	05:04:17
Start date:	22/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7175e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1720 Parent PID: 5624

General

Start time:	05:04:18
Start date:	22/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5624 CREDAT:17410 /prefetch:2
Imagebase:	0xaa0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly