ID: 404837
Sample Name: presentation.dll
Cookbook: default.jbs
Time: 12:50:17
Date: 05/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

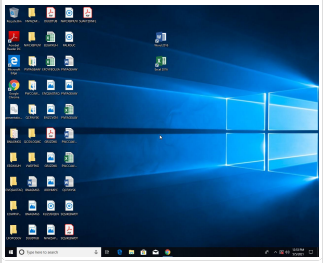
Analysis Report presentation.dll

Overview

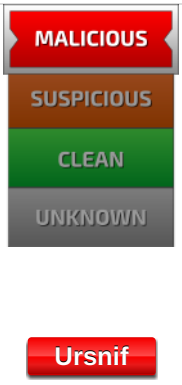
General Information

Sample Name:	presentation.dll
Analysis ID:	404837
MD5:	9debcd92976539..
SHA1:	d0c68d1d874a87..
SHA256:	9969cfd81612d1e.
Tags:	gozi
Infos:	

Most interesting Screenshot:



Detection

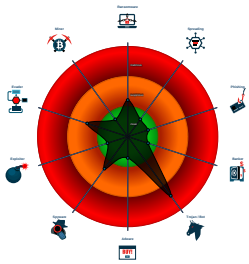


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Yara detected Ursnif
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Queries the installation date of Wind…
- Sample execution stops while proce…
- Sample file is different than original …
- Uses 32bit PE files

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5564 cmdline: loaddll32.exe 'C:\Users\user\Desktop\presentation.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5608 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\presentation.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1004 cmdline: rundll32.exe 'C:\Users\user\Desktop\presentation.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 204 cmdline: rundll32.exe C:\Users\user\Desktop\presentation.dll,Hadlaw MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4152 cmdline: rundll32.exe C:\Users\user\Desktop\presentation.dll,Might MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 4784 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5260 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4784 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"8oKmD0Ib40VYxHRgT7OnHwlxmK3U2F2Fl3GpR9KrKxvSCrIeiCLZWlQ2QCt+AnP+N5tCnTTv45/b0/D8Eb4xqxiXBnUy/ADWorQScIoNIPfBQqutzO+Ozy/mev4m2eZAuMivS2UNJVH4DVsYsAkGAC4GR+aszytDfGSZp3MklfgRJ6No
j034BrS4tQl5qmeWhJa+Of/CLdmkCwJurSEhMKu3NK7g4EVzni8lIJrDkWNCTaVL4CWXewbAOJFPwh8Y/20KkHTZmVKLmJJRcSj8yyH0avZDtWvJHRDxiI+JYUar2ia3phWwtqVzVhzYzz8aoUVzmlt840TF55o2e8TRUCEZNNmvmluqg
NZzQuNIj68=",
  "c2_domain": [
    "app.buboleinov.com",
    "chat.veminiare.com",
    "chat.billionady.com",
    "app3.maintorna.com"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "ZQktwkM8O9lYn9oX",
  "sleep_time": "10",
  "SetWaitableTimer_value": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.496778045.0000000005918000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.353723061.0000000004820000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000004.00000003.496874828.0000000005918000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.352567979.0000000002EE0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000001.00000003.363425153.00000000014C0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 8 entries				

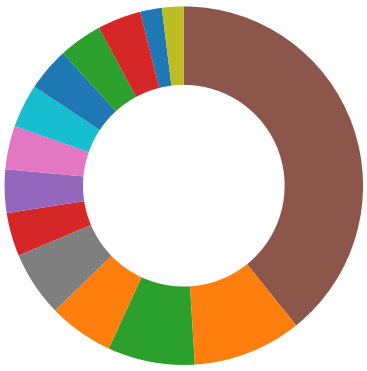
Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.rundll32.exe.3468d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.4828d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.6d640000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.loaddll32.exe.14c8d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.6d640000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Yara detected Ursnif

System Summary:

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Yara detected Ursnif

Remote Access Functionality:

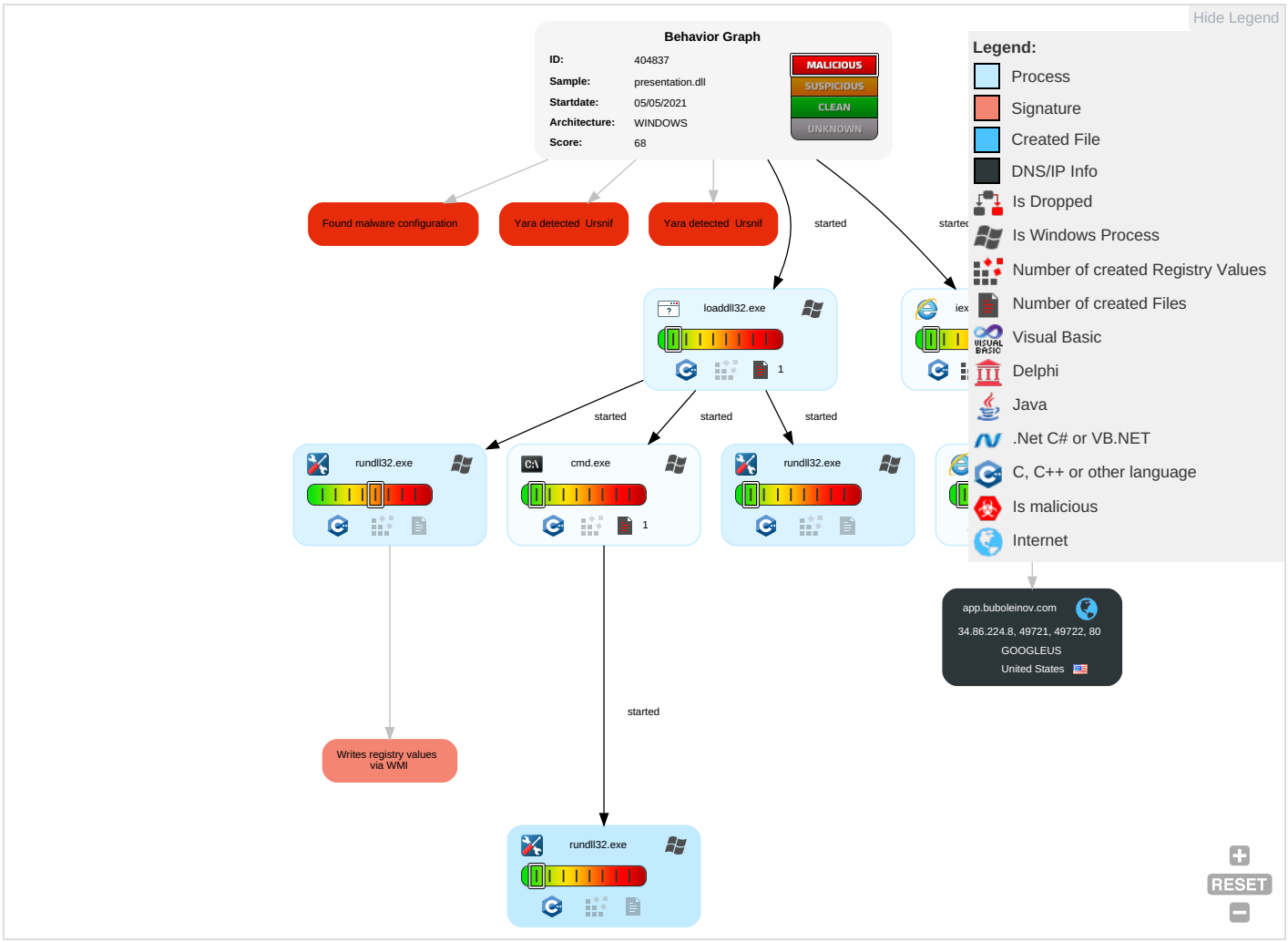
Yara detected Ursnif

Yara detected Ursnif

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
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Devi Without Authorizati
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	System Information Discovery 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	

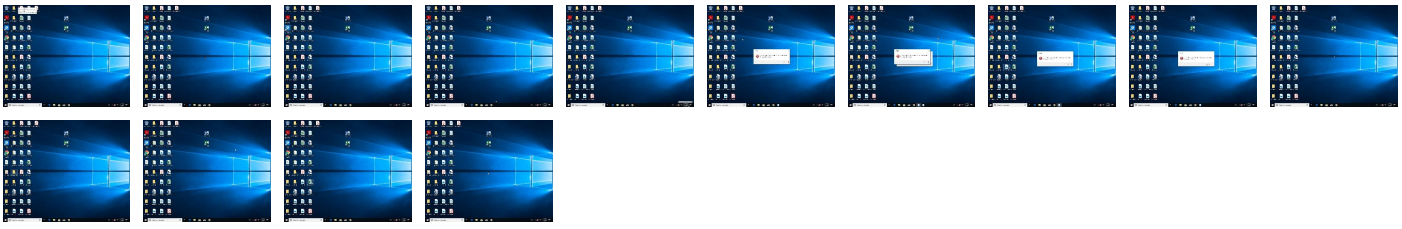
Behavior Graph



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
presentation.dll	4%	Virustotal		Browse
presentation.dll	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.2f30000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://app.buboleinov.com/bMm8AkF4K_2F_2FveRzR2f/nYi0xtk5xaARe/_2F_2Fyn/MhC_2BrW8ZBR5d6Ebe1q1AA/_2FU	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
app.buboleinov.com	34.86.224.8	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://app.buboleinov.com/bMm8AkF4K_2F_2FveRzR2f/nYi0xtk5xaARe/_2F_2Fyn/MhC_2BrW8ZBR5d6Ebe1q1AA/_2FU	{93F744B3-ADDB-11EB-90E6-ECF4BB82F7E0}.dat.21.dr, ~DF615A7858A33FDD4B.TMP.21.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.86.224.8	app.buboleinov.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404837
Start date:	05.05.2021
Start time:	12:50:17

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	presentation.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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:	mal68.troj.winDLL@12/13@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.7% (good quality ratio 4.5%) • Quality average: 79.9% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.193.48, 92.122.144.200, 2.20.142.209, 2.20.142.210, 13.64.90.137, 104.43.139.144, 92.122.145.220, 20.82.210.154, 88.221.62.148 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, go.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, go.microsoft.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:52:56	API Interceptor	1x Sleep call for process: rundll32.exe modified

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.{93F744B1-ADDB-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7728194424765753
Encrypted:	false
SSDEEP:	96:rLZuZ62DLWj1tj3Hifj+tHjHzMeQcH7HpH6THvHB7WHsHpB:rLZuZ623WRtzifKtTzM6b56jfBCspB
MD5:	49F6B7EC57B2D00C8D6EB883B89F469B
SHA1:	71678F63F6820A1052EF0508BB36CCF1751D6B44
SHA-256:	B46B55FABE8D834E48425FC723F5BBB14FBA93D05AE4882C33809D0087ED1E89
SHA-512:	3A4FC96E8E080EDA99C7D35FF3B0C00F479A6F2C8A13D283C32D3FB82FC16CFA5EFFFEFA6F3B72CF3DB972E679AFDDD07E60E8683F1D3B113F84871BBCE07FC
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\{93F744B3-ADDB-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	28140
Entropy (8bit):	1.914272415965734
Encrypted:	false
SSDEEP:	192:rBZwQs6ek7bjN2ASWiMLNHl/SlHlu/L4A:rHJ3/LEETBMEb
MD5:	18C6CB437E09C5DA3138CFE0C12FACF3
SHA1:	8EAA0C13469F0F244A0E65371025528D0E47BCF3
SHA-256:	57276398DCB4EA94A93ACCB8E744E7F170359BFA81EE6774282F41625AC03170
SHA-512:	065779A71327E7156022DF2724660E4BDF049F4812C59975E8BFE466D5B184C7503AFB95D4665059E14DE41670BFCB7C4B70E498A017941440653FE1AABE5D39
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG........IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG........IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t.,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\errorPageStrings[1]	
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB7
Malicious:	false
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Found</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.....}!$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\background_gradient[1]	
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5 A
Malicious:	false
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d......Ducky.......P......Adobe.d.. ....W...................................... ....Qa................................?......%.....x......s...Z.......j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.........p......A..........BP..qD.(.........ntH.@......h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\VAHFWDJC\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.440534734931472
Encrypted:	false
SSDEEP:	3:oVXUWQuXfmEqH8JOGXnEWQuXfmEZun:o9UXYehHqEXYed
MD5:	337C7ABD96ABBAE48D3334B09D918018
SHA1:	9D3673103FC0E9E29C10689E5D7A33EB8FE1292B
SHA-256:	7429818A07E321667F900E52C0A74B786E744F233F33F16E60BC091DC5C9E0F3
SHA-512:	881B5BFEAA4F21B4282797BBB2092681BF4D32F4EC6B602D12E3E327107570B452E9B847A3485E140291BF9197DFD8499B7A804CF644916ABF75691964646AF6
Malicious:	false
Preview:	[2021/05/05 12:53:37.917] Latest deploy version: ..[2021/05/05 12:53:37.917] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF615A7858A33FDD4B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40153
Entropy (8bit):	0.6680819612631073
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+ewe2esete2erUiFO48G3sxUiFO48G3syUiFO48G3sH:kBqoxKAuqR+Z3lUX6Hl/YHl/LHl/8
MD5:	F6A18585F58F28D0865FABEF22178F85
SHA1:	FCFAC439D675E64C4A8A654EF3DBBC25698E6927
SHA-256:	56DE1E56B45194300E42201A5AB96792E73EDD6D4C6867EC9608D3888489162C
SHA-512:	80320E170D9F102DB253196823283FCCC3AD411ADEFC4DA073C7C0F96FAF1EEDF6E481414E437950D61981F01DE0D2946354257F3CFF8390048D486284C9A53E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

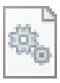
C:\Users\user\AppData\Local\Temp\~DFE183529A9C549E1C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4098284740596134
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lok9lo09lW82DN2+/:kBqoIPZ8ANB/
MD5:	EDFD47AA0AB0E70499337009970D93AD
SHA1:	12E92A6960D3FEAF2379B3EF2FE12834F3B5A339
SHA-256:	581389B2E758E1D3D9A77D3605813C07E389F81C817DA00AB922E94CA29653BC
SHA-512:	4C477F2731E4F4CBF73CEF1C77C46A85125520E3A9FF65CFD6618A4891231B4EB1714BE211FEA1FD2BE8E612582779C1042A5C9A8DA906AF4D96E82F78957B8(
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.151629290740381
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	presentation.dll
File size:	317952
MD5:	9debcd929765390555ca123c0076eea4
SHA1:	d0c68d1d874a877dbbbce1fea0bb164c6bdad642
SHA256:	9969cfd81612d1efbc5e983b57ff2fa2a69a3f6a6812c6da8382bf0c22014cf4
SHA512:	6c81556e2438ee04d5fae0e0b069d1558c2ab0fa2023915dad80203cca62b16f6dcf797bd58c854cfa5fdb113bf831cf2f7a040a287a66efa9637f64c35fd9ab
SSDEEP:	6144:ZUQrm4xMOQVFUy/kLYFnEaynGFa7ygc8eY:ZUelqO0REa2G0egJ
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......7. cs.N0s.N0s.N0m..0c.N0m..0:.N0z..0t.N0s.O0'.N0m..0Q.N0m..0r.N0m..0r.N0m..0r.N0Richs.N0...............PE..L....Ay`...........

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1033ecf
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x60794100 [Fri Apr 16 07:47:12 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	28e501612900311a5e5c7fed3dd79d00

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F79888EDA77h
call 00007F79888F088Ah
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F79888ED961h
pop ecx
pop ebp
retn 000Ch
mov edi, edi
push esi
push 00000001h
push 0104B110h
mov esi, ecx
call 00007F79888F0960h
mov dword ptr [esi], 01007B18h
mov eax, esi
pop esi
ret
mov dword ptr [ecx], 01007B18h
jmp 00007F79888F0A20h
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
mov dword ptr [esi], 01007B18h
call 00007F79888F0A0Dh
test byte ptr [ebp+08h], 00000001h
je 00007F79888EDA79h
push esi
call 00007F79888F0C37h
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F79888F0931h
mov dword ptr [esi], 01007B18h
mov eax, esi
pop esi
pop ebp

Instruction
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0Ch
jmp 00007F79888EDA7Fh
push dword ptr [ebp+08h]
call 00007F79888EF6DCh
pop ecx
test eax, eax
je 00007F79888EDA81h
push dword ptr [ebp+08h]
call 00007F79888ED69Ah
pop ecx
test eax, eax
je 00007F79888EDA58h
leave
ret
test byte ptr [01153F80h], 00000001h
mov esi, 01153F74h
jne 00007F79888EDA8Bh
or dword ptr [01153F80h], 01h

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [ASM] VS2008 build 21022 • [LNK] VS2008 build 21022 • [RES] VS2008 build 21022 • [EXP] VS2008 build 21022 • [IMP] VS2008 SP1 build 30729 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x4acc0	0x54	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4a4d4	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x155000	0x468	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x156000	0x1488	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1190	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xa048	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x15c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x49d14	0x49e00	False	0.632693527919	data	6.20599588203	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x4b000	0x109ba0	0x1000	False	0.249755859375	data	2.58806537383	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x155000	0x468	0x600	False	0.354166666667	data	2.94194825311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x156000	0x20d4	0x2200	False	0.5	data	4.90185749017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1550a0	0x330	data	English	United States
RT_MANIFEST	0x1553d0	0x91	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	OpenMutexW, VirtualProtectEx, CreateProcessW, GetCurrentDirectoryW, GetFileAttributesW, CompareStringW, CompareStringA, GetLastError, HeapFree, HeapAlloc, GetCurrentThreadId, GetCommandLineA, HeapCreate, HeapDestroy, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, VirtualAlloc, HeapReAlloc, GetModuleHandleW, Sleep, GetProcAddress, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, GetCurrentThread, SetHandleCount, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, RaiseException, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, InitializeCriticalSectionAndSpinCount, RtlUnwind, SetConsoleCtrlHandler, FreeLibrary, InterlockedExchange, LoadLibraryA, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapSize, GetLocaleInfoW, GetLocaleInfoA, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, GetStringTypeA, MultiByteToWideChar, GetStringTypeW, LCMapStringA, LCMapStringW, GetTimeZoneInformation, SetEnvironmentVariableA
ADVAPI32.dll	RegCloseKey, RegCreateKeyW, RegOpenKeyExW, RegQueryValueExA
XOLEHLP.dll	

Exports

Name	Ordinal	Address
Hadlaw	1	0x1033719
Might	2	0x103394e

Version Infos

Description	Data
LegalCopyright	Termwide Corporation. All rights reserved
InternalName	Go
FileVersion	2.3.6.358
CompanyName	Termwide Corporation
ProductName	Termwide Grass fire
ProductVersion	2.3.6.358
FileDescription	Termwide Grass fire Untilsuccess
OriginalFilename	Flower.dll
Translation	0x0409 0x04b0

Possible Origin

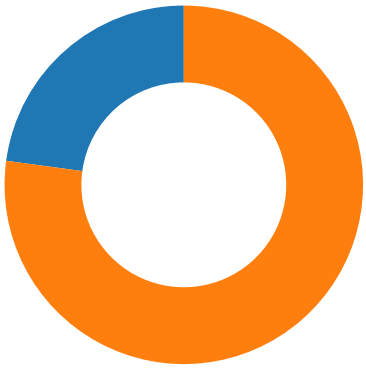
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 35

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 12:53:10.657921076 CEST	49722	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:10.657957077 CEST	49721	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:10.782052994 CEST	80	49722	34.86.224.8	192.168.2.7
May 5, 2021 12:53:10.782185078 CEST	49722	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:10.782567024 CEST	80	49721	34.86.224.8	192.168.2.7
May 5, 2021 12:53:10.782696962 CEST	49721	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:10.783261061 CEST	49722	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:10.949968100 CEST	80	49722	34.86.224.8	192.168.2.7
May 5, 2021 12:53:11.556493998 CEST	80	49722	34.86.224.8	192.168.2.7
May 5, 2021 12:53:11.556581020 CEST	49722	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:11.558764935 CEST	49722	80	192.168.2.7	34.86.224.8
May 5, 2021 12:53:11.683712959 CEST	80	49722	34.86.224.8	192.168.2.7
May 5, 2021 12:53:12.818595886 CEST	49721	80	192.168.2.7	34.86.224.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 12:51:07.527060986 CEST	50848	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:07.575766087 CEST	53	50848	8.8.8.8	192.168.2.7
May 5, 2021 12:51:08.701751947 CEST	61242	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:08.769575119 CEST	53	61242	8.8.8.8	192.168.2.7
May 5, 2021 12:51:10.040729046 CEST	58562	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:10.091387987 CEST	53	58562	8.8.8.8	192.168.2.7
May 5, 2021 12:51:10.935476065 CEST	56590	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:10.986607075 CEST	53	56590	8.8.8.8	192.168.2.7
May 5, 2021 12:51:12.011157990 CEST	60501	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:12.062582016 CEST	53	60501	8.8.8.8	192.168.2.7
May 5, 2021 12:51:13.227658987 CEST	53775	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:13.279352903 CEST	53	53775	8.8.8.8	192.168.2.7
May 5, 2021 12:51:14.198093891 CEST	51837	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:14.249691963 CEST	53	51837	8.8.8.8	192.168.2.7
May 5, 2021 12:51:15.168385029 CEST	55411	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:15.220807076 CEST	53	55411	8.8.8.8	192.168.2.7
May 5, 2021 12:51:37.306358099 CEST	63668	53	192.168.2.7	8.8.8.8
May 5, 2021 12:51:37.366440058 CEST	53	63668	8.8.8.8	192.168.2.7
May 5, 2021 12:52:03.938519955 CEST	54640	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:03.999603033 CEST	53	54640	8.8.8.8	192.168.2.7
May 5, 2021 12:52:11.432591915 CEST	58739	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:11.493288040 CEST	53	58739	8.8.8.8	192.168.2.7
May 5, 2021 12:52:12.722719908 CEST	60338	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:12.772093058 CEST	53	60338	8.8.8.8	192.168.2.7
May 5, 2021 12:52:14.136724949 CEST	58717	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:14.194367886 CEST	53	58717	8.8.8.8	192.168.2.7
May 5, 2021 12:52:16.115958929 CEST	59762	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:16.168989897 CEST	53	59762	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 12:52:17.303625107 CEST	54329	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:17.352282047 CEST	53	54329	8.8.8.8	192.168.2.7
May 5, 2021 12:52:18.407641888 CEST	58052	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:18.461596966 CEST	53	58052	8.8.8.8	192.168.2.7
May 5, 2021 12:52:19.618488073 CEST	54008	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:19.667156935 CEST	53	54008	8.8.8.8	192.168.2.7
May 5, 2021 12:52:21.217267036 CEST	59451	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:21.266094923 CEST	53	59451	8.8.8.8	192.168.2.7
May 5, 2021 12:52:23.682877064 CEST	52914	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:23.731807947 CEST	53	52914	8.8.8.8	192.168.2.7
May 5, 2021 12:52:24.504023075 CEST	64569	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:24.564321995 CEST	53	64569	8.8.8.8	192.168.2.7
May 5, 2021 12:52:24.746968985 CEST	52816	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:24.795684099 CEST	53	52816	8.8.8.8	192.168.2.7
May 5, 2021 12:52:25.702385902 CEST	50781	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:25.765597105 CEST	53	50781	8.8.8.8	192.168.2.7
May 5, 2021 12:52:26.864789009 CEST	54230	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:26.913532972 CEST	53	54230	8.8.8.8	192.168.2.7
May 5, 2021 12:52:27.795420885 CEST	54911	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:27.844294071 CEST	53	54911	8.8.8.8	192.168.2.7
May 5, 2021 12:52:50.267683029 CEST	49958	53	192.168.2.7	8.8.8.8
May 5, 2021 12:52:50.343266010 CEST	53	49958	8.8.8.8	192.168.2.7
May 5, 2021 12:53:08.797975063 CEST	50860	53	192.168.2.7	8.8.8.8
May 5, 2021 12:53:08.856270075 CEST	53	50860	8.8.8.8	192.168.2.7
May 5, 2021 12:53:10.286233902 CEST	50452	53	192.168.2.7	8.8.8.8
May 5, 2021 12:53:10.623338938 CEST	53	50452	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2021 12:53:10.286233902 CEST	192.168.2.7	8.8.8.8	0xd7c8	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2021 12:53:10.623338938 CEST	8.8.8.8	192.168.2.7	0xd7c8	No error (0)	app.bubole inov.com		34.86.224.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- app.buboleinov.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49722	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 5, 2021 12:53:10.783261061 CEST	1498	OUT	GET /bMm8AkF4K_2F_2FveRzR2f/nYi0xtk5xaARe/_2F_2Fyn/MhC_2BrW8ZBR5d6Ebe1q1AA/_2FUVq6FVw/212_2Fmya7wvf6qm5/W9P25GOkXEp_/2B7li5Reomx/DNGUxpOts5V_2F/m1ZCLgb0yZELhr1HDh2za/sK1pwrtT_2FYeJvy/UKI9xt8zwa55YYh/KZ8_2FX9rMmmJgeD_2/F8QbTyDtN/gF0rE8FYow3_2Fnp33aS/fsqd8_2FyHPS0_2Bp5_/2FbtiZGb31ZO5pN2ppiKul/1QXBqN9S9lxCl/vSq83RG3/yyRImlzN5vRP_2Bwx60Qoqa/1yNTVkSL_2Bp8is/j0c4aw 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: app.buboleinov.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 5, 2021 12:53:11.556493998 CEST	1498	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 05 May 2021 10:53:11 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5564 Parent PID: 5768

General

Start time:	12:51:43
Start date:	05/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\presentation.dll'
Imagebase:	0x1c0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.363425153.00000000014C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5608 Parent PID: 5564

General

Start time:	12:51:43
Start date:	05/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\presentation.dll',#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: rundll32.exe PID: 204 Parent PID: 5564

General

Start time:	12:51:43
Start date:	05/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\presentation.dll,Hadlaw
Imagebase:	0xa40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.353723061.0000000004820000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1004 Parent PID: 5608

General

Start time:	12:51:43
Start date:	05/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\presentation.dll',#1
Imagebase:	0xa40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496778045.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496874828.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.352567979.0000000002EE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496855209.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496831807.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496666566.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496741796.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496893630.0000000005918000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.496622014.0000000005918000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 4152 Parent PID: 5564

General

Start time:	12:51:46
Start date:	05/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\presentation.dll,Might
Imagebase:	0xa40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.362002402.0000000003460000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4784 Parent PID: 792

General

Start time:	12:53:36
Start date:	05/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff699dd0000
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	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: 5260 Parent PID: 4784

General

Start time:	12:53:37
Start date:	05/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4784 CREDAT:17410 /prefetch:2
Imagebase:	0xd50000
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

Code Analysis