ID: 429225
Sample Name: shorefront.eps
Cookbook: default.jbs
Time: 18:04:14
Date: 03/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

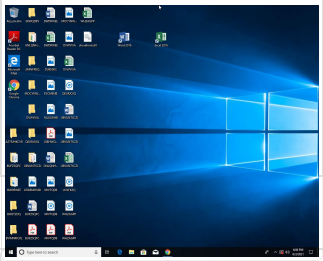
Analysis Report shorefront.eps

Overview

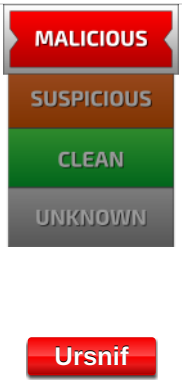
General Information

Sample Name:	shorefront.eps (renamed file extension from eps to dll)
Analysis ID:	429225
MD5:	b3526bc3c4a61f9..
SHA1:	d92ac3fa9cca4ed..
SHA256:	f4a464c2e5f14cd..
Tags:	dll Gozi
Infos:	

Most interesting Screenshot:



Detection



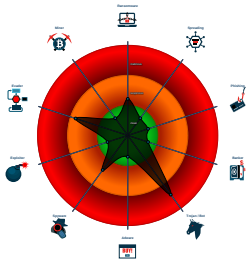
Ursnif

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Yara detected Ursnif
- Machine Learning detection for samp…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to detect virtu…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6604 cmdline: loaddll32.exe 'C:\Users\user\Desktop\shorefront.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6612 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\shorefront.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6640 cmdline: rundll32.exe 'C:\Users\user\Desktop\shorefront.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6628 cmdline: rundll32.exe C:\Users\user\Desktop\shorefront.dll,Child MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6700 cmdline: rundll32.exe C:\Users\user\Desktop\shorefront.dll,Forcearea MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6720 cmdline: rundll32.exe C:\Users\user\Desktop\shorefront.dll,Stationmeat MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 816 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6476 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:816 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4136 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:816 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"YO4ItoAHj27nQHcek0ajLmmby9wzIPBRe+hTTGA+vdmBx9WHGSmH+27G6fUvU8FIdumcsGzdR3nVucsR89Hrym0hEi/6912U3fz8nLZTmfMNITP1haHrjk4931u8AJbwFobO2OROdhnUSaxTMA4bUUhDQ512s4Mw9dwF+RVgzByOOXZj
Tb/8c7RAb5TF3S9udlcSUcG0UgRjjerDAkFDNoGfvrRUbQdmhzdTQTVlAQndB1/gGmNmYRjiDY3ZPIgGCxRg+L7+cRtLwnqkaPMhiWWYFszaBPeJgqFJ28z3OWmw84N+FITvVekj/sQLKPQHnW1Axm22vEhQb3UNvpyJEVFYrda06XMVS
Gm1E2H2wkQ=",
  "c2_domain": [
    "app.buboleinov.com",
    "chat.veminiare.com",
    "chat.billionady.com",
    "app3.maintorna.com"
  ],
  "botnet": "4500",
  "server": "580",
  "serpent_key": "46uoXhSnsCfVUpSs",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.827452979.0000000000530000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000003.874866712.0000000002FE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.876330514.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.874909818.0000000002FE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.874494648.0000000002FE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 20 entries				

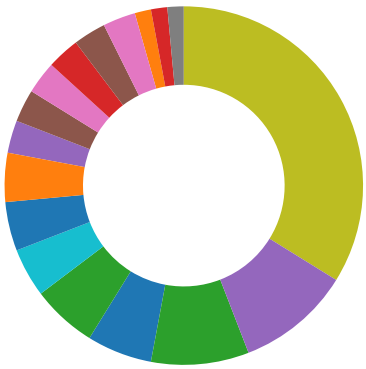
Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.rundll32.exe.3218d26.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.6c500000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.loaddll32.exe.538d26.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
6.3.rundll32.exe.30e8d26.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.2228d26.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- 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

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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 or reads registry keys via WMI

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

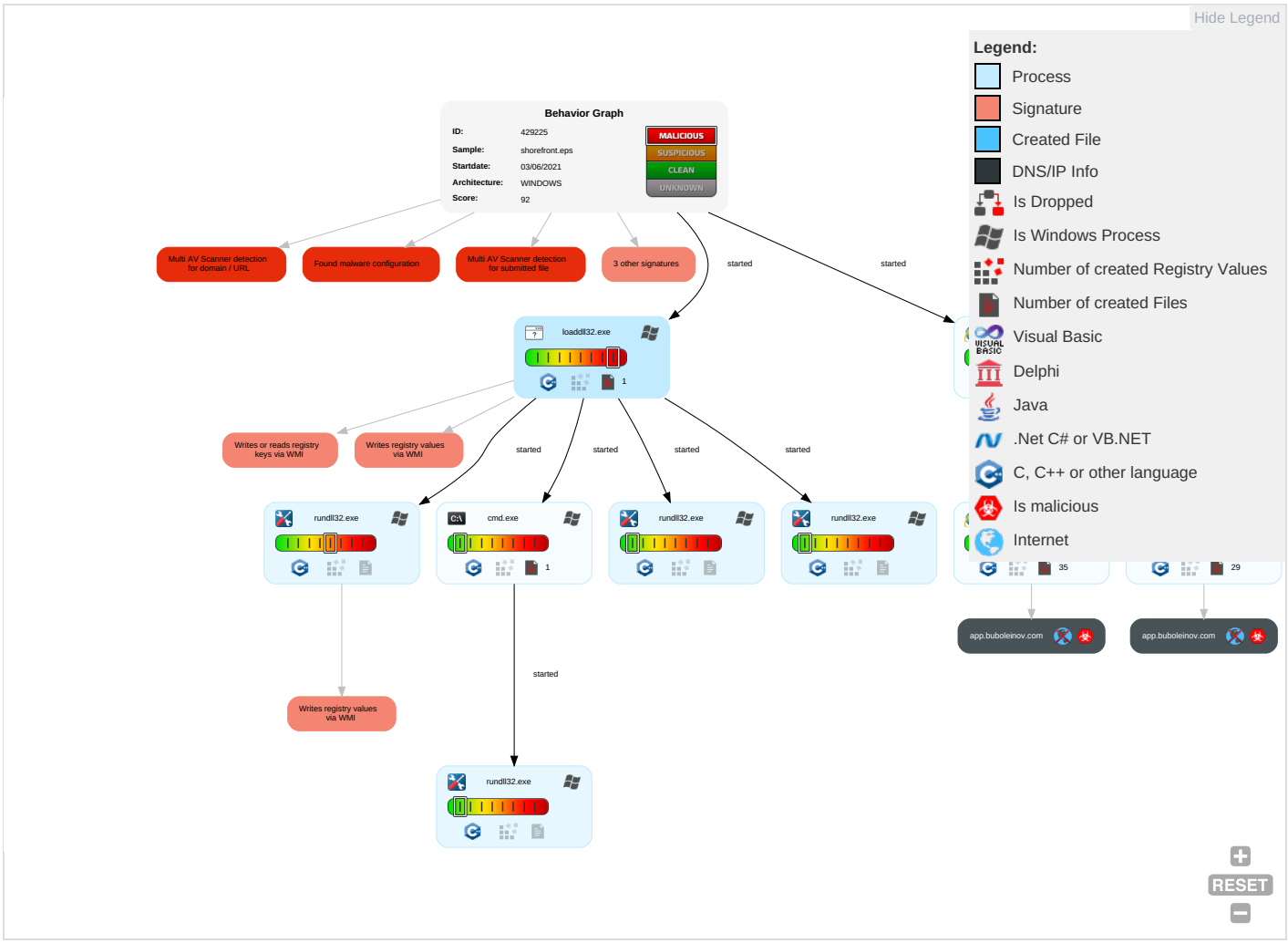
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdr Insecure Network Commur
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

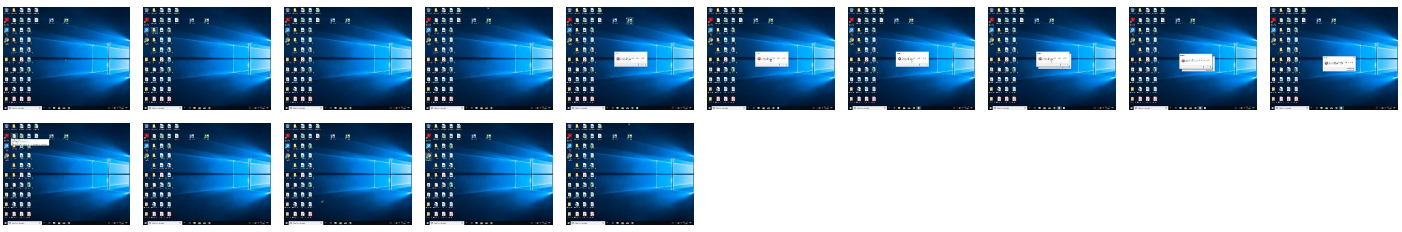
Behavior Graph



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
shorefront.dll	46%	Virustotal		Browse
shorefront.dll	54%	ReversingLabs	Win32.Trojan.Sdum	
shorefront.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.4770000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.500000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.3180000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
app.buboleinov.com	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://app.buboleinov.com/7dGVcD7hOw3lYt5/1yqoO_2BT5cAFQCvp3/7fGu2bPOM/Y70HlHuovLn2gp_2B2GH/4_2FYxaP	0%	Avira URL Cloud	safe	
http://app.buboleinov.com/BHxjQVeA3bCRL3A0U_2Bhx/6Mf2XW6xM9nlO/OBBDiHLG/gVHcEz5iH6i5Er6PkMAnMWX/IOi2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
app.buboleinov.com	unknown	unknown	true	• 7%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://app.buboleinov.com/7dGVcD7hOw3lYt5/1yqoO_2BT5cAFQCvp3/7fGu2bPOM/Y70HlHuovLn2gp_2B2GH/4_2FYxaP	~DF762A57E90D6A65CD.TMP.12.dr, {B147A470-C485-11EB-90EB-ECF4BBEA1588}.dat.12.dr	true	• Avira URL Cloud: safe	unknown
http://app.buboleinov.com/BHxjQVeA3bCRL3A0U_2Bhx/6Mf2XW6xM9nlO/OBBDiHLG/gVHcEz5iH6i5Er6PkMAnMWX/IOi2	{B147A472-C485-11EB-90EB-ECF4BBEA1588}.dat.12.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	429225
Start date:	03.06.2021
Start time:	18:04:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shorefront.eps (renamed file extension from eps to 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:	15
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:	mal92.troj.winDLL@16/17@6/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.6% (good quality ratio 15.8%) • Quality average: 79.5% • Quality standard deviation: 28.7%

HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.107.5.88, 13.107.42.23, 168.61.161.212, 184.30.25.218, 92.122.145.220, 104.42.151.234, 2.20.142.210, 2.20.142.209, 40.126.31.139, 40.126.31.6, 40.126.31.141, 40.126.31.137, 20.190.159.138, 40.126.31.143, 40.126.31.1, 40.126.31.4, 20.82.209.183, 40.88.32.150, 104.43.193.48, 88.221.62.148, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, config.edge.skype.com, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, afdo-tas-offload.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, l-0014.l-msedge.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Not all processes where analyzed, report is missing behavior information • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:06:28	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.{B147A46E-C485-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	1.9993845315328929
Encrypted:	false
SSDEEP:	192:r7ZYZdg2QjW0StiifcBPzMgHB+HDMKzcIwpSuM62pSbKpif8qpitkwNkimRwxkES:rN4FdxL900tk+dY1
MD5:	7978357DDA034C05E56F55DA35366205
SHA1:	48E4CABD925132F6A720DBF850A937DFCCC69152
SHA-256:	6B8EEF1FA301C04940AA30E7958CFA1C07D64E11423141A358089F78E59A2F6A
SHA-512:	1EEDC44DAFC7B64B1D1A1F26CBC74940EE74451114AA089D2C2B5C6B130A3C52E86B6137B4723D74066F57A50A1F2714C28AC7FAFD6AFF32A4D1FCDE53C8A 41
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\{B147A470-C485-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27588
Entropy (8bit):	1.9124316644431674
Encrypted:	false
SSDEEP:	192:rIZvQf6hkOjt2lWeMGVwmJ06ibFVwmJ06ixmmA:rIoSSIk83qhIbhIwx
MD5:	2E09A548EF11126190EFD8E8398EFBB9
SHA1:	17B8746C47A049ACAA52C304C607FC7E2F192F2B
SHA-256:	80ABDEBCCF9BCFC80CAE6DB09CB39304A8338B6927C70E988258FCE27FB8D74D
SHA-512:	C827881750C667D70195CD98D9279DC92C4EDFEC76925A4CF12969F00DBA76B63B5B89BF6ECF88A2D803B3351C46ED78DE8BC2D1BE5E12CB8884376A63BDE 62
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\{B147A472-C485-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B147A472-C485-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	28156
Entropy (8bit):	1.922108016741325
Encrypted:	false
SSDEEP:	96:roZvQr69BS/jl2FW1MpdphCuQbKolpIK9hCuQeOA:roZvQr69k/jl2FW1Mpdpw9lpfwnA
MD5:	99B43810D1B0B8FB2D4795325EBFF699
SHA1:	2BEA2EB826754881F2135787DE63991849271614
SHA-256:	891910C972C0E0B618F60AE4B2ACDE679390016D197D089D3DAD579BBB31EB46
SHA-512:	B17DFCDE50DACF718C2CC975DE6F5725FD4E64ED73402D04512318F5F4D6EFA092E80E58ADEFC5BFA58695969AF98BB7A286E715F35BD5BD5C437FC6211AB7D2
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\NewErrorPageTemplate[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):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\down[1]	
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
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\9026IKNJ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
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\Microsoft\Windows\INetCache\IE\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..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\CS6IXJW6\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
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
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9003
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
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 conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\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):	4.457498499025032
Encrypted:	false
SSDEEP:	3:oVXUbVCE9Ts4T48JOGXnEbVCE9Ts4uk+n:o9Urn4qErq
MD5:	330A46A120DAA4AA27765FF48C17CFA2
SHA1:	D64846D9E5996A84A50FE3522DF95B8D995D187C
SHA-256:	4C01D98C1E31356C9F8DDB63A2320560DF77C8A37B6215E8C51E4440AFFECC12
SHA-512:	3DD1DED3DDE41C97ED2C1D32E9065F58D9FC8272D403D0BD7B2DFEEEE064A924AE80049DEF6917EFF2861F795F741AA7FCBE281E7D17EF49B0A26F0CD50C5 45
Malicious:	false
Preview:	[2021/06/03 18:06:46.920] Latest deploy version: ..[2021/06/03 18:06:46.920] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF2325E3FA7AA39907.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40185
Entropy (8bit):	0.6775647831808976
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+EiIZCPphCuQbKephCuQbKZphCuQbK6:kBqoxKAuqR+EiIZCPpwVpwOpwT
MD5:	69940C57E758F61ED876E80B30613A47
SHA1:	643EE6264C9C8B4B54B84A83B7FCFF57B07F3B94
SHA-256:	85E2C831082051617156184594 50AEA91475F42DE1B577CE9E2BA86B0FE1BB8F
SHA-512:	4353AFCF37B8DBD3E0B99D737F385125D3BF072A8ACB1FE27A57D08E239162AED77D2C6184297D553D61ACE72C2A1F1299E006BAAE9F65AC3E9FDC50808C27 1
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF762A57E90D6A65CD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40073
Entropy (8bit):	0.6558580738443309
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+tzxQTWwmJ06iRwmJ06iqwmJ06if:kBqoxKAuqR+tzxQTWhIRhIqhIf
MD5:	BED294CA39E721D92EE7C908AFAA80A9

C:\Users\user\AppData\Local\Temp\~DF762A57E90D6A65CD.TMP	
SHA1:	E3B390F086560AF18F1C96F3633448B5B431C6D3
SHA-256:	52A5530CAFACE2F1C8A1D6D9B4E4B7A315236B316C6EF2C491278A9719F0B599
SHA-512:	740F9AE6B38ECC70861E1D4B746238D970EA40EA84B17276897ABCBA19D90D93DFFFDEF811D5F0D053EACEBD4A0B400E2B70BB3BCC41539DA707E44DF4A8981
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF896FBAE33087E32E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5972692611662705
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loJ9lop9lWnxTV929:kBqoIysrG
MD5:	E96BA0BC747494236BC0429356C61A71
SHA1:	50C56F2FB54ACF0D56C65C1F92B43894B8247773
SHA-256:	0FCB065D36956D9134F1DEAFE195677B90F3143C534147A4E91FB53DBFE1A301
SHA-512:	139FF4AB662834360F7D752A01ED0D14308FC85E782DEF0D10CCFBF0C2999DC1EBE105B5B1938BD5A34709D2A55C812D43D79F7DD3F0276F575BB2DF07A67A
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):	6.166903919730553
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:	shorefront.dll
File size:	393728
MD5:	b3526bc3c4a61f9f09ac31ee9a5fc8a5
SHA1:	d92ac3fa9cca4ed8273111f767e24d8f53896787
SHA256:	f4a464c2e5f14cd4c391a9b5ba60deca36ccaa6c1503a097eeb0c5070945d1fb
SHA512:	0583e811619ea1ce40c430436e91b8b216fc509e7c75ed7132fdccc9f52f1828f50dbca6cd4b973090962fe6e8b76e298b0fe43b56ea2485810d4dc52e033fdb
SSDEEP:	6144:hC5FUWwNmY036ua+71w5uJEr+AitTdyh+a6R+/ZQWdB:0FBwNuKu4umqAinyh+7+h1H
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....pS.....!.....$.....W.....K.....@.....m..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x1045798
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x53700FF7 [Mon May 12 00:04:07 2014 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	f97da13a5df33dbcb72f17527b1d6819

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F6174C5A777h
call 00007F6174C64340h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F6174C5A77Ch
add esp, 0Ch
pop ebp
retn 000Ch
push 0000000Ch
push 0105B7D8h
call 00007F6174C602DEh
xor eax, eax
inc eax
mov esi, dword ptr [ebp+0Ch]
test esi, esi
jne 00007F6174C5A77Eh
cmp dword ptr [020691B4h], esi
je 00007F6174C5A85Ah
and dword ptr [ebp-04h], 00000000h
cmp esi, 01h
je 00007F6174C5A777h
cmp esi, 02h
jne 00007F6174C5A7A7h
mov ecx, dword ptr [010137A0h]
test ecx, ecx
je 00007F6174C5A77Eh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call ecx
mov dword ptr [ebp-1Ch], eax
test eax, eax
je 00007F6174C5A827h
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007F6174C5A586h
mov dword ptr [ebp-1Ch], eax
test eax, eax

Instruction
je 00007F6174C5A810h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007F6174C52768h
mov edi, eax
mov dword ptr [ebp-1Ch], edi
cmp esi, 01h
jne 00007F6174C5A79Ah
test edi, edi
jne 00007F6174C5A796h
push ebx
push eax
push dword ptr [ebp+08h]
call 00007F6174C52750h
push ebx
push edi
push dword ptr [ebp+08h]
call 00007F6174C5A54Ch
mov eax, dword ptr [010137A0h]
test eax, eax
je 00007F6174C5A779h
push ebx
push edi
push dword ptr [ebp+08h]
call eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x5bdf0	0x6d	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x106c200	0x64	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x106d000	0x2334	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1080	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x18b68	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x106c000	0x200	.idata
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	0x5ae5d	0x5b000	False	0.629630623283	data	6.14182941666	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x5c000	0x100f10c	0x1c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x106c000	0xc34	0xe00	False	0.399832589286	data	5.23220949273	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x106d000	0x2334	0x2400	False	0.759331597222	data	6.62458632125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import

DLL	Import
KERNEL32.dll	SetStdHandle, WriteConsoleW, ReadConsoleW, CreateFileW, SetSystemPowerState, CreateFileA, GetWindowsDirectoryA, GetCommandLineA, CreateSemaphoreA, FormatMessageA, GetLocalTime, GetSystemTimeAsFileTime, HeapWalk, HeapCompact, HeapFree, HeapAlloc, VirtualProtectEx, OutputDebugStringW, LoadLibraryExW, SetFilePointerEx, ReadFile, GetConsoleMode, GetConsoleCP, FlushFileBuffers, CloseHandle, HeapReAlloc, GetModuleFileNameW, WriteFile, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCurrentProcessId, QueryPerformanceCounter, GetModuleFileNameA, GetFileType, GetStdHandle, WideCharToMultiByte, MultiByteToWideChar, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, EncodePointer, DecodePointer, GetLastError, RaiseException, RtlUnwind, GetCurrentThreadId, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, SetLastError, InitializeCriticalSectionAndSpinCount, Sleep, GetCurrentProcess, TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW, GetModuleHandleW, GetProcAddress, IsProcessorFeaturePresent, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, ExitProcess, GetModuleHandleExW, HeapSize, GetProcessHeap, IsDebuggerPresent, IsValidCodePage, GetACP, GetOEMCP
ole32.dll	OleUninitialize, OleInitialize, OleSetContainedObject
ADVAPI32.dll	AllocateAndInitializeSid, SetEntriesInAclA, StartServiceCtrlDispatcherW, SetServiceStatus, RegisterServiceCtrlHandlerA, QueryServiceStatus, OpenServiceA, OpenSCManagerA, DeleteService, RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, RegOpenKeyA, RegEnumKeyA, RegDeleteKeyA, RegCreateKeyExA, RegCloseKey, LookupPrivilegeValueA, OpenProcessToken, OpenThreadToken, GetTokenInformation, FreeSid, InitializeSecurityDescriptor, SetSecurityDescriptorDacl
hlink.dll	

Exports

Name	Ordinal	Address
Child	1	0x103dbb0
Forcearea	2	0x103dc60
Stationmeat	3	0x103d3d0

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2021 18:04:57.835787058 CEST	50579	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:57.877228022 CEST	53	50579	8.8.8.8	192.168.2.4
Jun 3, 2021 18:04:58.193685055 CEST	51703	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:58.194834948 CEST	65248	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:58.195405006 CEST	53723	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:58.235152006 CEST	53	51703	8.8.8.8	192.168.2.4
Jun 3, 2021 18:04:58.236143112 CEST	53	65248	8.8.8.8	192.168.2.4
Jun 3, 2021 18:04:58.236301899 CEST	53	53723	8.8.8.8	192.168.2.4
Jun 3, 2021 18:04:58.640815020 CEST	64646	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:58.690197945 CEST	53	64646	8.8.8.8	192.168.2.4
Jun 3, 2021 18:04:59.577861071 CEST	65298	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:59.626797915 CEST	53	65298	8.8.8.8	192.168.2.4
Jun 3, 2021 18:04:59.664598942 CEST	59123	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:04:59.737924099 CEST	53	59123	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:00.287354946 CEST	54531	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:00.341882944 CEST	53	54531	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:00.524528980 CEST	49714	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:00.574057102 CEST	53	49714	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:01.698822021 CEST	58028	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:01.747279882 CEST	53	58028	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:03.097371101 CEST	53097	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:03.139079094 CEST	53	53097	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:04.113044977 CEST	49257	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:04.161500931 CEST	53	49257	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:05.240236998 CEST	62389	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:05.283468008 CEST	53	62389	8.8.8.8	192.168.2.4
Jun 3, 2021 18:05:54.963553905 CEST	49910	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:05:55.027280092 CEST	53	49910	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:26.936666965 CEST	55854	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:26.978046894 CEST	53	55854	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:28.175432920 CEST	64549	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:28.218729019 CEST	53	64549	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:29.277987003 CEST	63153	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 3, 2021 18:06:29.328186989 CEST	53	63153	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:29.367486954 CEST	52991	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:29.416198969 CEST	53	52991	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:30.062048912 CEST	53700	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:30.127419949 CEST	53	53700	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:30.666662931 CEST	51726	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:30.715130091 CEST	53	51726	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:31.485276937 CEST	56794	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:31.534965038 CEST	53	56794	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:33.046251059 CEST	56534	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:33.096560955 CEST	53	56534	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:37.884838104 CEST	56627	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:37.934593916 CEST	53	56627	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:39.378293037 CEST	56621	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:39.420027018 CEST	53	56621	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:40.316010952 CEST	63116	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:40.365956068 CEST	53	63116	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:41.262558937 CEST	64078	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:41.314126015 CEST	53	64078	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:43.233447075 CEST	64801	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:43.282026052 CEST	53	64801	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:46.981379986 CEST	61721	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:47.032116890 CEST	53	61721	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:48.251032114 CEST	51255	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:48.301836967 CEST	53	51255	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:48.314477921 CEST	61522	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:48.377386093 CEST	53	61522	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:48.390541077 CEST	52337	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:48.439580917 CEST	53	52337	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:49.089580059 CEST	55046	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:49.138902903 CEST	53	55046	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:49.145909071 CEST	49612	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:49.194487095 CEST	53	49612	8.8.8.8	192.168.2.4
Jun 3, 2021 18:06:49.201268911 CEST	49285	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:06:49.252738953 CEST	53	49285	8.8.8.8	192.168.2.4
Jun 3, 2021 18:07:10.306181908 CEST	50601	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:07:10.375230074 CEST	53	50601	8.8.8.8	192.168.2.4
Jun 3, 2021 18:07:14.013451099 CEST	60875	53	192.168.2.4	8.8.8.8
Jun 3, 2021 18:07:14.063872099 CEST	53	60875	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 3, 2021 18:06:48.251032114 CEST	192.168.2.4	8.8.8.8	0xd976	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:48.314477921 CEST	192.168.2.4	8.8.8.8	0x65f0	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:48.390541077 CEST	192.168.2.4	8.8.8.8	0xf05a	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:49.089580059 CEST	192.168.2.4	8.8.8.8	0x72bc	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:49.145909071 CEST	192.168.2.4	8.8.8.8	0x2930	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:49.201268911 CEST	192.168.2.4	8.8.8.8	0xd559	Standard query (0)	app.bubole inov.com	A (IP address)	IN (0x0001)

DNS Answers

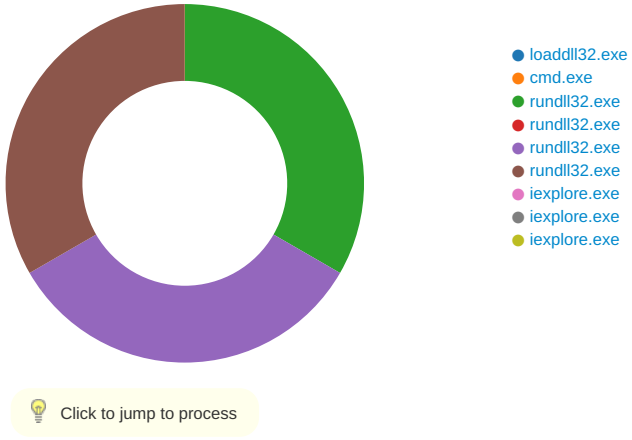
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 3, 2021 18:06:29.328186989 CEST	8.8.8.8	192.168.2.4	0xbf1e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jun 3, 2021 18:06:48.301836967 CEST	8.8.8.8	192.168.2.4	0xd976	Name error (3)	app.bubole inov.com	none	none	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:48.377386093 CEST	8.8.8.8	192.168.2.4	0x65f0	Name error (3)	app.bubole inov.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 3, 2021 18:06:48.439580917 CEST	8.8.8.8	192.168.2.4	0xf05a	Name error (3)	app.bubole inov.com	none	none	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:49.138902903 CEST	8.8.8.8	192.168.2.4	0x72bc	Name error (3)	app.bubole inov.com	none	none	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:49.194487095 CEST	8.8.8.8	192.168.2.4	0x2930	Name error (3)	app.bubole inov.com	none	none	A (IP address)	IN (0x0001)
Jun 3, 2021 18:06:49.252738953 CEST	8.8.8.8	192.168.2.4	0xd559	Name error (3)	app.bubole inov.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6604 Parent PID: 6040

General

Start time:	18:05:03
Start date:	03/06/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\shorefront.dll'
Imagebase:	0x960000
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: 00000000.00000003.827452979.0000000000530000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874866712.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874909818.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874494648.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874791903.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874837013.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874942139.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874588381.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.874885116.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.917892757.0000000002FE8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6612 Parent PID: 6604

General

Start time:	18:05:04
Start date:	03/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\shorefront.dll',#1
Imagebase:	0x11d0000
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: 6628 Parent PID: 6604

General

Start time:	18:05:04
Start date:	03/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\shorefront.dll,Child
Imagebase:	0x200000
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: 00000002.00000003.797710729.0000000002220000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1	31	1	invalid handle	20	6C5518B8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6640 Parent PID: 6612

General

Start time:	18:05:04
Start date:	03/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\shorefront.dll',#1
Imagebase:	0x200000
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: 00000003.00000003.876330514.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876188239.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.919920945.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876373518.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.794830642.00000000027F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876356161.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876088782.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876229416.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876297207.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.876268229.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6700 Parent PID: 6604

General

Start time:	18:05:08
Start date:	03/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\shorefront.dll,Forcearea
Imagebase:	0x200000
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: 00000005.00000003.813086420.0000000003210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1	31	1	invalid handle	20	6C5518B8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6720 Parent PID: 6604

General

Start time:	18:05:14
Start date:	03/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\shorefront.dll,Stationmeat
Imagebase:	0x200000
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: 00000006.00000003.821591213.00000000030E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1	31	1	invalid handle	20	6C5518B8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 816 Parent PID: 800

General

Start time:	18:06:45
Start date:	03/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff601e70000
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: 6476 Parent PID: 816

General

Start time:	18:06:46
Start date:	03/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:816 CREDAT:17410 /prefetch:2
Imagebase:	0x8a0000
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

Analysis Process: iexplore.exe PID: 4136 Parent PID: 816

General

Start time:	18:06:47
Start date:	03/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:816 CREDAT:17414 /prefetch:2
Imagebase:	0x8a0000
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