JoeSandbox Cloud BASIC

**ID:** 886219
**Sample Name:**
HkObDPju6Z.exe
**Cookbook:** default.jbs
**Time:** 21:31:34
**Date:** 12/06/2023
**Version:** 37.1.0 Beryl

# Table of Contents

Copyright Joe Security LLC 2023

Copyright Joe Security LLC 2023

Copyright Joe Security LLC 2023

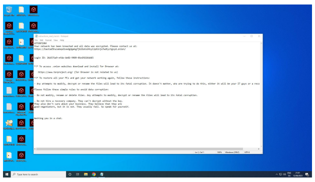
# Windows Analysis Report

## HkObDPju6Z.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | HkObDPju6Z.exe |
| Analysis ID: | 886219 |
| MD5: | 6441d7260944.. |
| SHA1: | 462579828404.. |
| SHA256: | 723d1cf3d74fb… |
| Infos: | |



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

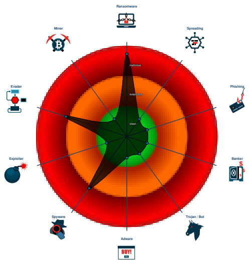
BlackBasta

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

### Signatures

- Multi AV Scanner detection for subm…
- Yara detected BlackBasta ransomw…
- Found ransom note / readme
- Found Tor onion address
- Machine Learning detection for sam…
- Contains functionality to modify clip…
- May disable shadow drive data (use…
- Writes a notice file (html or txt) to de…
- Deletes shadow drive data (may be …
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…

### Classification



## Process Tree

- **System is w10x64native**
- HkObDPju6Z.exe (PID: 332 cmdline: C:\Users\user\Desktop\HkObDPju6Z.exe MD5: 6441D7260944BCEDC5958C5C8A05D16D)
  - cmd.exe (PID: 312 cmdline: C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 2280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - vssadmin.exe (PID: 8948 cmdline: C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: B58073DB8892B67A672906C9358020EC)
  - cmd.exe (PID: 3944 cmdline: cmd.exe /c start /MAX notepad.exe c:\instructions_read_me.txt MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 7328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - notepad.exe (PID: 1352 cmdline: notepad.exe c:\instructions_read_me.txt MD5: E92D3A824A0578A50D2DD81B5060145F)
- HkObDPju6Z.exe (PID: 1508 cmdline: "C:\Users\user\Desktop\HkObDPju6Z.exe" MD5: 6441D7260944BCEDC5958C5C8A05D16D)
  - cmd.exe (PID: 3292 cmdline: C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 2452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - vssadmin.exe (PID: 4644 cmdline: C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: B58073DB8892B67A672906C9358020EC)
- HkObDPju6Z.exe (PID: 5560 cmdline: "C:\Users\user\Desktop\HkObDPju6Z.exe" MD5: 6441D7260944BCEDC5958C5C8A05D16D)
  - cmd.exe (PID: 1808 cmdline: C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 4152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - vssadmin.exe (PID: 8264 cmdline: C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet MD5: B58073DB8892B67A672906C9358020EC)
- **cleanup**

## Malware Threat Intel

Provided by malpedia

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|

Copyright Joe Security LLC 2023

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|
| **Black Basta** | "Black Basta" is a new ransomware strain discovered during April 2022 - looks in dev since at least early February 2022 - and due to their ability to quickly amass new victims and the style of their negotiations, this is likely not a new operation but rather a rebrand of a previous top-tier ransomware gang that brought along their affiliates. | No Attribution | http:// https://assets.sentinelone.com/sentinellabs22/sentinellabs-blackbastahttps://gbhackers.com/black-basta-ransomware/https://mandiant.widen.net/s/pkffwrbjlz/m-trends-2023https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdfhttps://quadrantsec.com/resource/technical-analysis/black-basta-malware-overview | http:// https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbasta |

## Malware Configuration

**No configs have been found**

## Yara Signatures

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000A.00000003.22756871962.00000000028F0000.00000004.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 0000001E.00000002.27586886931.0000000003343000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 00000003.00000003.22575159083.0000000002F20000.00000004.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 0000000E.00000003.22839485707.0000000002980000.00000004.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 0000000E.00000002.22856927512.0000000002A90000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |

Click to see the 5 entries

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 10.3.HkObDPju6Z.exe.28f0000.0.raw.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 14.3.HkObDPju6Z.exe.2980000.0.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 14.2.HkObDPju6Z.exe.2a90000.1.raw.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 10.2.HkObDPju6Z.exe.2a40000.1.raw.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |
| 3.3.HkObDPju6Z.exe.2f20000.0.raw.unpack | JoeSecurity_BlackBasta | Yara detected BlackBasta ransomware | Joe Security | |

Click to see the 5 entries

## Sigma Signatures

⊘ **No Sigma rule has matched**

## Snort Signatures

⊘ **No Snort rule has matched**

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Networking

Found Tor onion address

### Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to modify clipboard data

### Spam, unwanted Advertisements and Ransom Demands

Yara detected BlackBasta ransomware

Found ransom note / readme

May disable shadow drive data (uses vssadmin)

Writes a notice file (html or txt) to demand a ransom

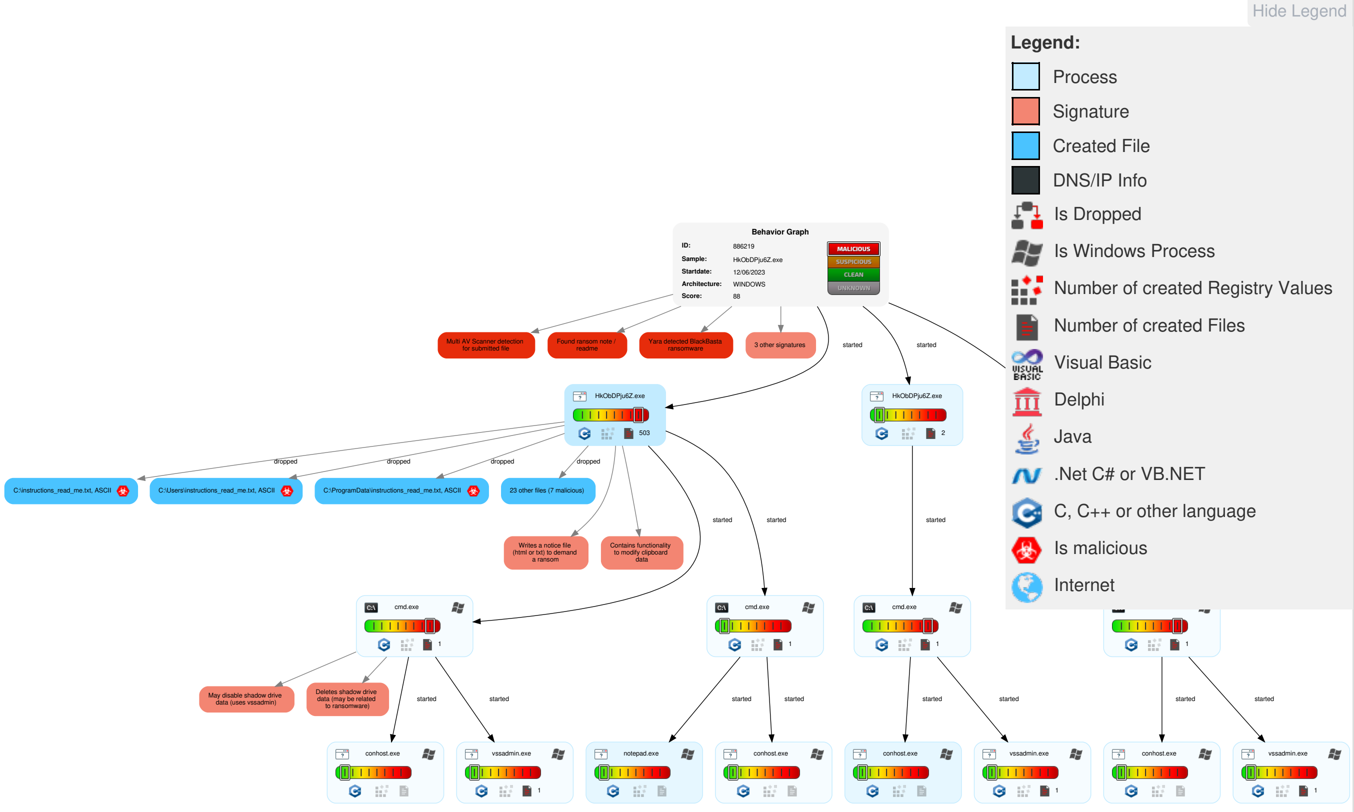
Deletes shadow drive data (may be related to ransomware)

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | 2 Command and Scripting Interpreter | 1 DLL Side-Loading | 1 2 Process Injection | 3 Masquerading | 1 1 Input Capture | 2 System Time Discovery | Remote Services | 1 1 Input Capture | Exfiltration Over Other Network Medium | 2 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 Data Encrypted for Impact |
| Default Accounts | 1 Native API | Boot or Logon Initialization Scripts | 1 DLL Side-Loading | 1 2 Process Injection | LSASS Memory | 3 1 Security Software Discovery | Remote Desktop Protocol | 1 Archive Collected Data | Exfiltration Over Bluetooth | 1 Proxy | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 1 Deobfuscate/Decode Files or Information | Security Account Manager | 1 Process Discovery | SMB/Windows Admin Shares | 1 1 Clipboard Data | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 3 Obfuscated Files or Information | NTDS | 1 Application Window Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 1<br>Software Packing | LSA Secrets | 1<br>File and Directory Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication |  | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 1<br>DLL Side-Loading | Cached Domain Credentials | 3 5<br>System Information Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |  | Abuse Accessibility Features |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | 1<br>File Deletion | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points |  | Data Encrypted for Impact |

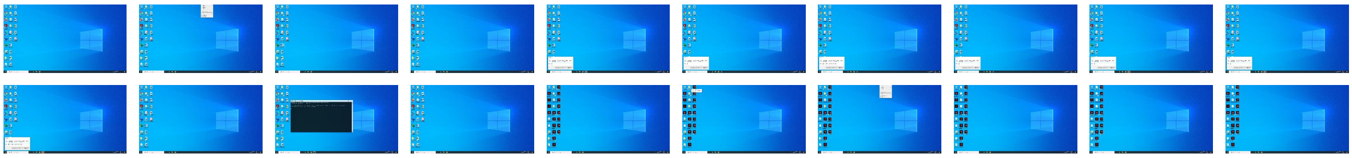
## Behavior Graph

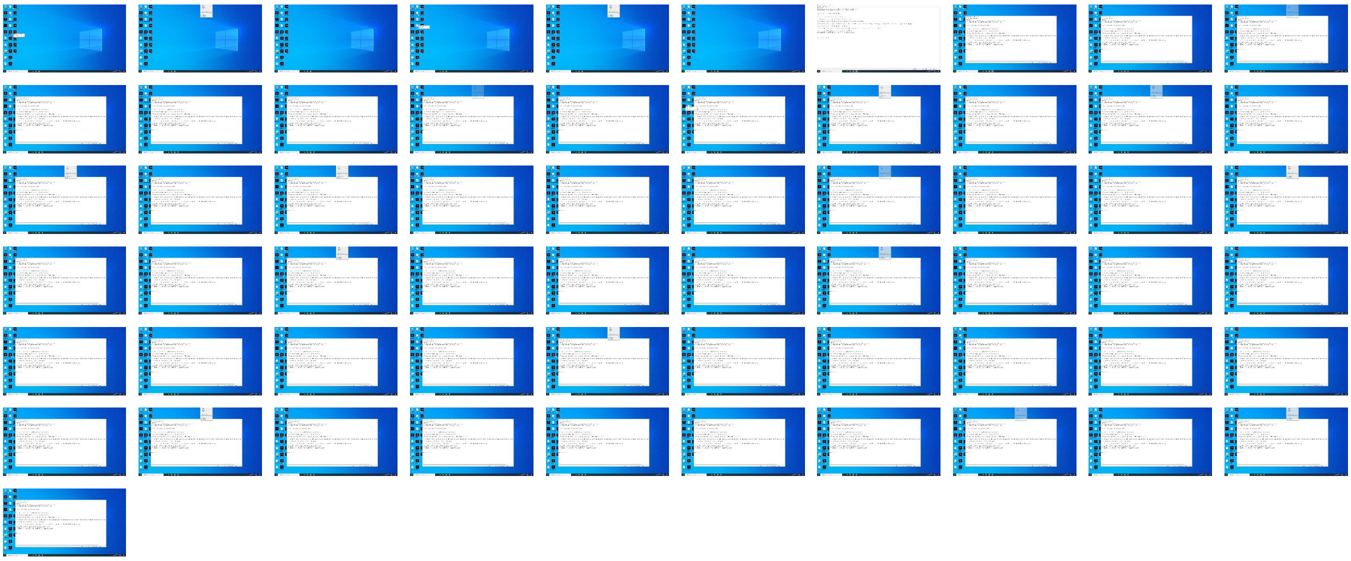


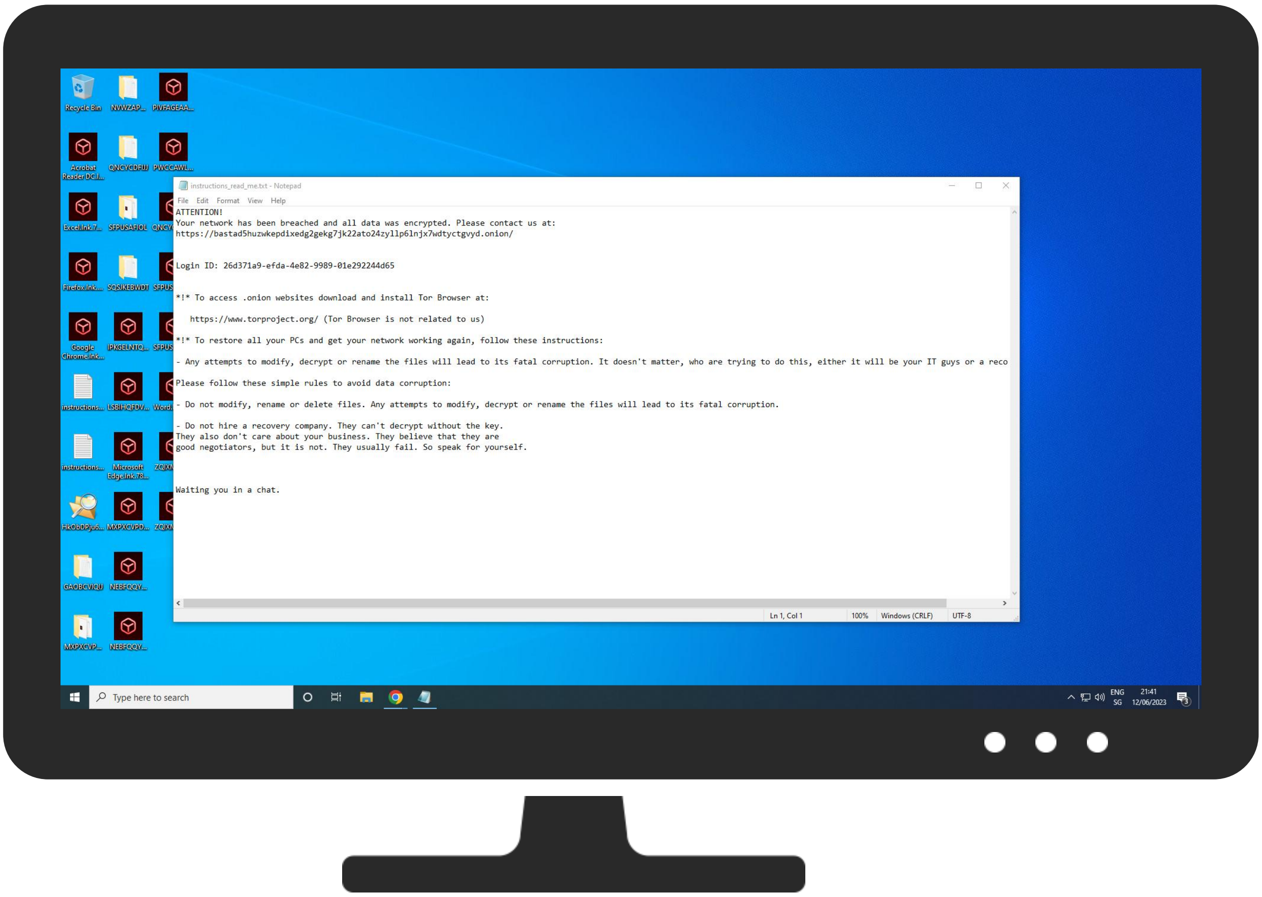
## Screenshots

### Thumbnails

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







```
ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/


Login ID: 26d371a9-efda-4e82-9989-01e292244d65


*!* To access .onion websites download and install Tor Browser at:

   https://www.torproject.org/ (Tor Browser is not related to us)

*!* To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a reco

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.



Waiting you in a chat.
```

## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| HkObDPju6Z.exe | 59% | ReversingLabs | Win32.Ransomware.Basta | |
| HkObDPju6Z.exe | 69% | Virustotal | | Browse |
| HkObDPju6Z.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

⊘ **No Antivirus matches**

### Unpacked PE Files

⊘ **No Antivirus matches**

### Domains

⊘ **No Antivirus matches**

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://crl.mi) | 0% | Avira URL Cloud | safe | |
| http://www.w3.L | 0% | Avira URL Cloud | safe | |
| http://https://licensing.micro. | 0% | Avira URL Cloud | safe | |
| http://www.w3.orRR | 0% | Avira URL Cloud | safe | |
| http://https://www.flos-freeware.chopenmailto:florian.balmer | 0% | Avira URL Cloud | safe | |
| http://www.microsoft.co | 0% | Avira URL Cloud | safe | |
| http://www.microsoft.co | 1% | Virustotal | | Browse |
| http://https://odc.officeapps.l= | 0% | Avira URL Cloud | safe | |
| http://https://login.windows.localPath | 0% | Avira URL Cloud | safe | |
| http://www.w3.oro | 0% | Avira URL Cloud | safe | |
| http://https://login.mi7 | 0% | Avira URL Cloud | safe | |
| http://www.w3.o | 0% | Avira URL Cloud | safe | |
| http://www.w3.od9( | 0% | Avira URL Cloud | safe | |
| http://www.microsoft.c | 0% | Avira URL Cloud | safe | |
| http://www.w3.i | 0% | Avira URL Cloud | safe | |
| http://https://docs.live-tst.net/skydocsservice.svc | 0% | Avira URL Cloud | safe | |
| http://https://go.mJ | 0% | Avira URL Cloud | safe | |
| http://https://graph.microsoft.uslogin.microsoftonline.ushttps://microsoftgraph.chinacloudapi.cnlogin.us3 | 0% | Avira URL Cloud | safe | |
| http://https://go.microsoft.c | 0% | Avira URL Cloud | safe | |
| http://https://go.mic | 0% | Avira URL Cloud | safe | |
| http://https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ | 0% | Avira URL Cloud | safe | |
| http://www.w3.orqq5 | 0% | Avira URL Cloud | safe | |
| http://crl.mic | 0% | Avira URL Cloud | safe | |
| http://crl.miy | 0% | Avira URL Cloud | safe | |
| http://www.w3.or | 0% | Avira URL Cloud | safe | |
| http://www.microsoft. | 0% | Avira URL Cloud | safe | |
| http://https://go.micd1t | 0% | Avira URL Cloud | safe | |
| http://https://licensing.microsoft.c | 0% | Avira URL Cloud | safe | |
| http://www.w3.5( | 0% | Avira URL Cloud | safe | |
| http://www.microsoft.cog | 0% | Avira URL Cloud | safe | |
| http://https://go.microso | 0% | Avira URL Cloud | safe | |
| http://https://graph.microsoft.us | 0% | Avira URL Cloud | safe | |
| http://https://go.mi | 0% | Avira URL Cloud | safe | |
| http://crl.micro | 0% | Avira URL Cloud | safe | |
| http://crl.micrpNi | 0% | Avira URL Cloud | safe | |
| http://https://licensing.microso | 0% | Avira URL Cloud | safe | |
| http://https://licensing.microsoft | 0% | Avira URL Cloud | safe | |
| http://crl.mic& | 0% | Avira URL Cloud | safe | |
| http://www.w3.orQZ | 0% | Avira URL Cloud | safe | |
| http://https://licensing.mic | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

⊘ **No contacted domains info**

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://crl.mi) | ChakraCore.Debugger.dll.3.dr | false | - Avira URL Cloud: safe | low |
| http://https://licensing.micro. | SkypeforBusiness2019R_Trial-ppd.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://www.w3.orRR | Standard2019R_Grace-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://www.microsoft.co | ProjectProCO365R_Subscription-pl.xrm-ms.3.dr, Access2021VL_MAK_AE-pl.xrm-ms.3.dr, Publisher2021R_Retail2-pl.xrm-ms.3.dr | false | - 1%, Virustotal, Browse<br>- Avira URL Cloud: safe | unknown |
| http://https://www.flos-freeware.chopenmailto:florian.balmer | HkObDPju6Z.exe | false | - Avira URL Cloud: safe | low |
| http://https://microsoftgraph.chinacloudapi.cn | inventory.dll.3.dr | false | | high |
| http://www.w3.L | ProjectProCO365R_SubTest-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://www.torproject.org/ | HkObDPju6Z.exe, HkObDPju6Z.exe, 0000000A.00000003.22756871962.00000000028F0000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000A.00000002.22781985168.0000000002A40000.00000040.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000E.00000003.22839485707.0000000002980000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000E.00000002.22856927512.0000000002A90000.00000040.00001000.00020000.00000000.sdmp, notepad.exe, 0000001E.00000002.27586886931.0000000003343000.00000004.00000020.00020000.00000000.sdmp, instructions_read_me.txt46.3.dr, instructions_read_me.txt51.3.dr, instructions_read_me.txt79.3.dr, instructions_read_me.txt78.3.dr, instructions_read_me.txt39.3.dr, instructions_read_me.txt13.3.dr, instructions_read_me.txt21.3.dr, instructions_read_me.txt38.3.dr, instructions_read_me.txt40.3.dr, instructions_read_me.txt15.3.dr, instructions_read_me.txt57.3.dr, instructions_read_me.txt71.3.dr, instructions_read_me.txt6.3.dr, instructions_read_me.txt69.3.dr, instructions_read_me.txt30.3.dr | false | | high |
| http://https://odc.officeapps.l= | inventory.dll.3.dr | false | - Avira URL Cloud: safe | low |
| http://https://substrate.office.com/profile/v1.0/me/profileaccountspassportMemberNamephonesphoneNumbername | inventory.dll.3.dr | false | | high |
| http://https://www.flos-freeware.ch | HkObDPju6Z.exe | false | | high |
| http://www.w3. | ProjectPro2021VL_MAK_AE1-ul-oob.xrm-ms.3.dr | false | | high |
| http://https://login.windows.localPath | inventory.dll.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://profile.live.com/home | inventory.dll.3.dr | false | | high |
| http://www.videolan.org/x264.html | StartMenu_Win8.mp4.3.dr, StartMenu_Win10_RTL.mp4.3.dr | false | | high |
| http://www.w3.oro | Standard2021R_Grace-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://login.mi7 | inventory.dll.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://www.w3.o | O365HomePremR_SubTrial4-ul-oob.xrm-ms.3.dr, Publisher2021R_Trial-ul-oob.xrm-ms.3.dr, Standard2021R_Retail-ul-oob.xrm-ms.3.dr, Access2021R_Retail-pl.xrm-ms.3.dr, ProPlusVL_KMS_Client-ul.xrm-ms.3.dr, Standard2019VL_MAK_AE-ul-phn.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://www.w3.od9( | O365HomePremR_SubTrial5-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | low |
| http://www.microsoft.c | HkObDPju6Z.exe, 00000003.00000003.22622038049.0000000001070000.00000004.00000020.00020000.00000000.sdmp, C2RINTL.ru-ru.dll.3.dr, AccessR_Grace-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://www.w3.i | Standard2021MSDNR_Retail-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://docs.live-tst.net/skydocsservice.svc | inventory.dll.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://login.microsoftonline.com/commonSetAuthorityAttempted | inventory.dll.3.dr | false | | high |
| http://https://go.mJ | ProjectProCO365R_SubTest-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://graph.microsoft.uslogin.microsoftonline.ushttps://microsoftgraph.chinacloudapi.cnlogin.us3 | inventory.dll.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://go.microsoft.c | Publisher2021R_Trial-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |
| http://https://go.mic | O365HomePremR_SubTrial4-ul-oob.xrm-ms.3.dr | false | - Avira URL Cloud: safe | unknown |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ | HkObDPju6Z.exe, HkObDPju6Z.exe, 0000000A.00000003.22756871962.0000000028F0000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000A.00000002.22779639838.000000000D20000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000A.00000002.22781985168.0000000002A40000.00000040.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000E.00000002.22855902907.0000000002900000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000E.00000003.22839485707.0000000002980000.00000004.00001000.00020000.00000000.sdmp, HkObDPju6Z.exe, 0000000E.00000002.22856927512.0000000002A90000.00000040.00001000.00020000.00000000.sdmp, notepad.exe, 0000001E.00000002.27586886931.0000000003343000.00000004.00000020.00020000.00000000.sdmp, instructions_read_me.txt46.3.dr, instructions_read_me.txt51.3.dr, instructions_read_me.txt79.3.dr, instructions_read_me.txt78.3.dr, instructions_read_me.txt39.3.dr, instructions_read_me.txt13.3.dr, instructions_read_me.txt21.3.dr, instructions_read_me.txt38.3.dr, instructions_read_me.txt40.3.dr, instructions_read_me.txt15.3.dr, instructions_read_me.txt57.3.dr, instructions_read_me.txt71.3.dr, instructions_read_me.txt6.3.dr | true | • Avira URL Cloud: safe | unknown |
| http://https://clients.config.office.net/collec | inventory.dll.3.dr | false | | high |
| http://www.w3.orqq5 | O365HomePremR_SubTrial5-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://crl.mic | C2RINTL.vi-vn.dll.3.dr, Interceptor.dll.3.dr, MSBARCODE.DLL.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://crl.miy | MAPISHELL.DLL.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://www.w3.or | O365HomePremR_SubTrial4-ul-oob.xrm-ms.3.dr, Access2021VL_MAK_AE-ul-oob.xrm-ms.3.dr, Standard2021R_Trial-ul-oob.xrm-ms.3.dr, Access2019VL_MAK_AE-ul-oob.xrm-ms.3.dr, ProfesionalR_Trial-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://www.microsoft. | ProjectPro2019VL_MAK_AE-pl.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://go.micd1t | O365HomePremR_SubTrial5-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://www.rizonesoft.com | HkObDPju6Z.exe | false | | high |
| http://https://login.microsoftonline.de/common | inventory.dll.3.dr | false | | high |
| http://https://licensing.microsoft.c | Access2019VL_KMS_Client_AE-ul-oob.xrm-ms.3.dr, ProjectPro2019DemoR_BypassTrial180-ppd.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://substrate.office.com/profile/v1.0/me/profile | inventory.dll.3.dr | false | | high |
| http://www.w3.5( | Publisher2019R_Retail-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | low |
| http://www.microsoft.cog | O365EduCloudEDUR_Subscription-pl.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://go.microso | Standard2021MSDNR_Retail-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://graph.microsoft.us | inventory.dll.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://go.mi | ProjectPro2021VL_MAK_AE1-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://crl.micro | api-ms-win-crt-stdio-l1-1-0.dll.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://crl.micrpNi | api-ms-win-core-xstate-l2-1-0.dll.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://licensing.microso | Standard2019VL_KMS_Client_AE-ul-oob.xrm-ms.3.dr, O365ProPlusEDUR_Subscription-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://licensing.microsoft | O365HomePremR_Subscription5-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://crl.mic& | inventory.dll.3.dr | false | • Avira URL Cloud: safe | low |
| http://www.w3.orQZ | VisioPro2019R_Grace-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://licensing.mic | ProjectPro2021VL_KMS_Client_AE-ul-oob.xrm-ms.3.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://login.microsoftonline.de/commonmicrosoftonline.demicrosoftonline.mil3 | inventory.dll.3.dr | false | | high |
| http://https://login.microsoftonline.com/common | inventory.dll.3.dr | false | | high |

## World Map of Contacted IPs

⊘ **No contacted IP infos**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 37.1.0 Beryl |
| Analysis ID: | 886219 |
| Start date and time: | 2023-06-12 21:31:34 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 20m 5s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301 |
| Number of analysed new started processes analysed: | 36 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Sample file name: | HkObDPju6Z.exe |
| Detection: | MAL |
| Classification: | mal88.rans.spyw.evad.winEXE@21/1025@0/0 |
| EGA Information: | • Successful, ratio: 50% |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 79%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe<br>• Sleeps bigger than 100000000ms are automatically reduced to 1000ms |

### Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, VSSVC.exe, svchost.exe, TextInputHost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 40.126.32.74, 40.126.32.68, 20.190.160.17, 40.126.32.72, 40.126.32.76, 20.190.160.14, 40.126.32.136, 40.126.32.138
- Excluded domains from analysis (whitelisted): www.bing.com, spclient.wg.spotify.com, wdcpalt.microsoft.com, prdv4a.aadg.msidentity.com, login.live.com, www.tm.v4.a.prd.aadg.akadns.net, tile-service.weather.microsoft.com, wdcp.microsoft.com, array804.prod.do.dsp.mp.microsoft.com, login.msa.msidentity.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Execution Graph export aborted for target HkObDPju6Z.exe, PID 332 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior information.
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

## Simulations

### Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 21:33:39 | Autostart | Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Skype C:\Users\user\Desktop\HkObDPju6Z.exe |
| 21:33:47 | Autostart | Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Skype C:\Users\user\Desktop\HkObDPju6Z.exe |

## Joe Sandbox View / Context

### IPs

⊘ **No context**

## Domains

⊘ **No context**

## ASNs

⊘ **No context**

## JA3 Fingerprints

⊘ **No context**

## Dropped Files

⊘ **No context**

# Created / dropped Files

### C:\$WinREAgent\Scratch\instructions_read_me.txt ☣

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | 24:F6SGOzWKJa3XWOCYj1C1PpiyE/xVHpmjxNkX0lOhA5:VGOzW6CwRNsxV0jVOK5 |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | **true** |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ ......Login ID: 26d371a9-efda-4e82-9989-01e292244d65......*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

### C:\$WinREAgent\instructions_read_me.txt ☣

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | 24:F6SGOzWKJa3XWOCYj1C1PpiyE/xVHpmjxNkX0lOhA5:VGOzW6CwRNsxV0jVOK5 |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | **true** |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ ......Login ID: 26d371a9-efda-4e82-9989-01e292244d65......*!* To access .onion websites download and install Tor Browser at:.... https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

### C:\Intel\instructions_read_me.txt ☣

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | 24:F6SGOzWKJa3XWOCYj1C1PpiyE/xVHpmjxNkX0lOhA5:VGOzW6CwRNsxV0jVOK5 |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | **true** |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ ......Login ID: 26d371a9-efda-4e82-9989-01e292244d65......*!* To access .onion websites download and install Tor Browser at:....   https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

### C:\PerfLogs\instructions_read_me.txt ☣

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1091 |
| Entropy (8bit): | 4.804750185554599 |
| Encrypted: | false |
| SSDEEP: | 24:F6SGOzWKJa3XWOCYj1C1PpiyE/xVHpmjxNkX0lOhA5:VGOzW6CwRNsxV0jVOK5 |
| MD5: | BA21D49977850F54961EDE73B7E9E480 |
| SHA1: | BD630B3DBE9D7139527C1FFDBB2161E7A9067AE0 |
| SHA-256: | 34757273C5E041F07B0352C51CFAB2998AB676F3A39BC0F16A1B4D68F3FAC4F8 |
| SHA-512: | 4BF9BE5F41F7258357E838BA94F0AA2B7F17D8FE3266174AAF123156B422C4FB72E4D3FD36DB7B2E3E9D13202202D2A6B0ECCA06EE2A2A043CE6AD27FFD751E2 |
| Malicious: | **true** |
| Preview: | ATTENTION!..Your network has been breached and all data was encrypted. Please contact us at:..https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/ ......Login ID: 26d371a9-efda-4e82-9989-01e292244d65......*!* To access .onion websites download and install Tor Browser at:....   https://www.torproject.org/ (Tor Browser is not related to us)....*!* To restore all your PCs and get your network working again, follow these instructions:....- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.....Please follow these simple rules to avoid data corruption:....- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. ....- Do not hire a recovery company. They can't decrypt without the key. ..They also don't care about your business. They believe that they are ..good negotiator |

### C:\Program Files (x86)\AutoIt3\Include\AVIConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1897 |
| Entropy (8bit): | 7.545967015081844 |
| Encrypted: | false |
| SSDEEP: | 24:X7Ph1mw7QOvf7bphjL7qyp4ROso9hMJZrU2Kiybn5SVa/+aE8Nn7zq:X7p1b7P7thzqyEoArrH+jbNHq |
| MD5: | A3376EFC13EA76E8418AFFAE4C10AF46 |
| SHA1: | 37349D2AE75E1A6A0E9CB3A70E05A71BE7DED35F |
| SHA-256: | F362FC1A1AA0B22B8C29315A16FB6A02917B804755BBC9DE777D1394ECEDD72A |
| SHA-512: | 422D73FC6254C40CC8E92657C269989FCD5AB631C3D4D93FC773DFDA4711EF9D792563AFA7356DE4FF5FAA0348079E8F0947AEAF3CF954BFE5AECBAEBD810D1 |
| Malicious: | false |
| Preview: | Y..+<..?.../.YV.Hh>...8....F...9.paj..A.......<..R.1...a......E.G.um.Lg...q.ia..n#..A....F...9.paj..A.......<..R.1...a......E.G.um.Lg...q.ia..n...(..[.l.*.cry..\...n..r........\|o..d.X....!?.Q`.....eh.w^.........b.*.cry..9..X......+....A,Z....V.@..'>..;...l.;..~2>........T.2_a^)5/..)...H../....M...bi...N......h..8z... .'`.#m0..\....j\-.cry..F...]......R.1...a......E.G.um.Lg...q.ia..n#..A....F...9.paj..A.......<..R.1...a......E.G.um.Lg...q.ia..n#..A....F...9.paj..A.......<..e......a..l.,.Y.um.Lg...q.ia..n#..A....F...9.paj..A.......<..R.1...a......E.G.um.Lg...q.ia..n#..A....F...9.paj..A.......<..R.1.."g...A...p..'2..z...?.tx...A...(....[.O%C\">6..?..E...B..;.M..x.\|.....X.w..$?..6...". \|...M...(..."...0=G.;......^...!..,.S..e.\|.....r....)<.25...l......Q...=...)..{$.mma..q...r..s..O.i..]0Z..T...w..$?..6...". \|...W...#......pEf.\|j..=...e..R..=.B.."Q$...H......EZ..5...l.;2.6s:...*...(..aPo.....9.......1..e.`..I0...^.X.;.....4...l......]...(...,..zWu.\|\|..L. |

### C:\Program Files (x86)\AutoIt3\Include\BorderConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Public Key |
| Category: | dropped |
| Size (bytes): | 2434 |
| Entropy (8bit): | 7.71491997429176 |
| Encrypted: | false |
| SSDEEP: | 48:+/wYjw7iB3/oJywiXwY9Yi+3FnAwbS5xT+0:TyEiN/jDw8Y5eOl0 |
| MD5: | 030067596892F75F1329EA9A4E9D3DB4 |
| SHA1: | ACC83016AA4313BE72475A38EF75ED7E1BA3A70B |
| SHA-256: | E004B6CD78DC3F90A7A96ACC6B7A22223C04B5A2AD1E6A3469F3BAE86C316CEF |
| SHA-512: | 9B9DA9C51F61F627D9C711C9A4DA0526093BFD8DDAAB992EF841505D109F5A653C5EDE892D4083EC527ADDAAD55BB467F1DF01E56FAF0A2B1F2311B74D1C1D7 |
| Malicious: | false |
| Preview: | .wn",..............rds..m...3.....-%.0.k.oWh.V&P.SWS.G`...+3.D...#=\|}.H...}...$...l..w.....3.....-%.0.k.oWh.V&P.SWS.G`...+3.D...#=\|}.H...}...$...[....A.. .....>6.7..\ .0.4X...........6O..S..>V$2.....z...7...d 7q.y.V{..V..>6.#.l...2..h..dQN....Bfz..R..0.{`.....!........zT$.e..u\|..v..u0.#.\.r+ ..t...CN.Ts...6I..E..lo24....}...$...l..w.....3.....-%.0.k.oWh.V&P.SWS.G`...+3.D...#=\|}.H...}...$...l..w.....3.....-%.0.k.oWh.V&P.SWS.G`...+3.D...#=\|}.H..M...Z....ls......3.....-%.0.k.oWh.V&P.SWS.G`...+3.D...#=\|}.H...}...$...l..w.....3.....-%.0.k.oWh.V&P.SWS.G`...+3.D...#=\|}.H...}...^...0A...[...*..a..QQ.H..}./..V;].Zgd..2.G6M..O.:B...'........\...q.E{.?.^l.....~k.-..w.5..%P(.'$ .(}...n6.s{..\|a-`.....`...F....hs..a..3..K..._.b.7_r):..oM.+.).%..{63.;U..L(e..'.........L...}....g.d@..}..^].$.\t>.7..;......^..nIK.:t..>=a......d....J....cr..p...*..a..QQ.H..}./..f.*.....Z..Xb..<x..AR...0..`....K....b..\|.uA..v..0<.I..a.#../R#.+8G.p..Iwb.:S..j e..2........9..8Yr....cQ..}..^W.Y.. |

### C:\Program Files (x86)\AutoIt3\Include\ButtonConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4765 |
| Entropy (8bit): | 7.846326583221281 |
| Encrypted: | false |
| SSDEEP: | 96:unExTCnvyC+VnXTdxXqYD2LoPKk2STyZFtCc9WXBGbUFp:TC+VnXTdcYDNPH2fZYxp |
| MD5: | 8D552000303D05D36186C1B8725F53FC |
| SHA1: | C7549EC912A06FE4E3134EF8EF6F9CAAB42479CC |
| SHA-256: | 9A8B31F9F7ECD46A618E8FF329442A09021BA3B18AA6EF310055BBACA287DE7C |
| SHA-512: | F7037F1B966B625A95B3A685C248847AC215CCEE07BD869B832D0182479E0A34C8DA1E796C153DDF2CF69E83C96BCA6CB54B0C25FF9B29DF9AC090069FA6252 |
| Malicious: | false |
| Preview: | ..{......0c. ..zJp.*9...&zzjq./8.""V....w(.Zb....-.-..#..=.w.\|..%.....c=....MLm.^Jm..8gzjq./8.""V....w(.Zb....-.-..#..=.w.\|..%.....c=....ML].XW...i?gyb.<+.11E...>a......]d..d....A.>.....}....V.d ....AE~.n}k.d4 "-.w%.11E.....{..6...$+..u..l..t.%.a.."....K.?n.^...p..W8..cgeyb.su.zq.....\..&....x..3..j..n.t.....w....T..u.Y..P.$...#..ddg6".2B.pj.....\|.K....M{..h.....A.>.....1.....d.L...\|Z.CJm..8gzjq./8.""V....w(.Zb....-.-..#..=.w.\|..%.....c=....MLm.^Jm..8gzjq./8.""V....w(.Zb....-.-..#..=.w.\|..%.....c=....MLm.n}]..%y....FD.KLH....w(.Zb....-.-..#..=.w.\|..%.....c=....MLm.^Jm..8gzjq./8.""V....w(.Zb....-.-..#..=.w.\|..%.....c=....MLm.^Jm...P\|w..}p...,....&5..1....R..W..K..O.j.a...(...5.e .X....].$.?..iz.8".f%.]L4....X.Z..... ....q..l.../...<....}..E....@.`.SG]..i5%6 .Qj.lkK....P.7....{D..^..>..0.z.L...w....{.0s....#...%#p..5"wf\|....sp....%{......q]..D..W.. .j.9..(...W.?l.n....p.!$...V...../%.g/[....y..>..A~..0..M..U.......%....n..j....<..>..%~....[B.K?V... |

### C:\Program Files (x86)\AutoIt3\Include\CUIAutomation2.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 47975 |
| Entropy (8bit): | 6.777862266680883 |
| Encrypted: | false |
| SSDEEP: | 768:FUkNoN3MqRLh0MbIJDpLnNbSOSzrS8aR1OAXx:7ePlnGpLnNbRayeGx |
| MD5: | 01BFF50A243D43963A0A5DD015C5B12F |
| SHA1: | D41B8C4E1D426239E67F6A2DA0F2E4F7C48AEA71 |
| SHA-256: | B13033695A59ACA2BECDF3F9EEABB3A9CB0A478377B9F63444EF12575C6D4B55 |
| SHA-512: | 5CE511ABAE4AE78D256C3660C3066FBBAC750C07A26C2EB0F60D9F0999C5DE5B10B561D006DFE62E7B65D7A15A00B9ED8CAE863F59CF1200512D992487A80E9E |
| Malicious: | false |
| Preview: | ...1..o.'d.......+>....._z..@.,.u.-.H-........q*r..O..).X..083-8FB8-45CF-BCB7-C477ACB2F897}"....;CoClasses..Global Const $sCLSID_CUIAutomation = "{FF48DBA4-60EF-4201-AA87-54103EEF594E}".....(..7.X.o`+....6....D8...O;..^{@.}.........`!t.....0.\..0..Global Const $UIA_SelectionPatternId = 10001..Global Const $UIA_ValuePatternId = 10002..Global Const $UIA_RangeValuePatternId...t..Ot.k.lu3.$!.4.2j....c8..K/..R....O.....NA.....0....t $UIA_ExpandCollapsePatternId = 10005..Global Const $UIA_GridPatternId = 10006..Global Const $UIA_GridItemPatternId = 10007..Gl.......1.i#.GU....>;..u..N-...x1..c?D...r..t....u(&.....0.9.._WindowPatternId = 10009..Global Const $UIA_SelectionItemPatternId = 10010..Global Const $UIA_DockPatternId = 10011..Global Cons........#.%b.o`+....6..0.K.k..K8..K7D..R1....7....v(c.....q....nId = 10013..Global Const $UIA_TextPatternId = 10014..Global Const $UIA_TogglePatternId = 10015..Global Const $UIA_TransformPatt...d..sNy6.......+>....._z..M.6.X4.. |

### C:\Program Files (x86)\AutoIt3\Include\Clipboard.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |

| | |
|---|---|
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 19296 |
| Entropy (8bit): | 6.30998218992441 |
| Encrypted: | false |
| SSDEEP: | 384:q+ic5mRjnEBW2YdtEUGFpkrf7+Sx2hhcX5JuB0SOshWhX0X7PAowXoyt:qrRjEBW20ukHx2h6SVhWCPoXt |
| MD5: | A2687C7932D0F979F3F9BFB38F3F2A3A |
| SHA1: | DDC5D9035099304D450E6645D1D3A9C31F205041 |
| SHA-256: | 7B79095721B0CD692507CB9200F5DE378DDB63D09F5C763EA008385A5D2E46A1 |
| SHA-512: | 0D77E12983774373393B12F6565395D9EDCB70905003E404210E8FBB01CF1F152BE8B22E3A5C3EA3041E65180F0EFB5C232111409A7ECA7FD541C08CA9FA1BCI |
| Malicious: | false |
| Preview: | ).$.z..Q4...9.Y.#w....k.J<.../.U.._jVW.....A-.k4.E.ik>.z.r....=============================================================================================================..; Title .........: I.#.t..F}..WNu. qIj.&.\|..p..s.....wAW."%w....N..K.zx-.}..NPMIsh..; Description ...: Functions that assist with Clipboard management...;                  The clipboard is a set of functions k..S{..Gx..N@.5j {...j..n...#.X..D*T..9qI....J.....5x..\|.o....            Because  all applications have access to the clipboard, data can be easily transferred..;                  between az.&.u..]v.LN[.t>ww.../..p...0.E..^0.4.....#..G.....tx-.i.u.g@Ul Campbell (PaulIA)..; ================================================================================================================7.wN+...$..QS..i#=#.M....`%........d.'y.$8.._Y..L..X.ik>.z.r....=========================================================================================..Global Const $CF_TEXT = 1 ; Text fox.+...Xv..Nw.:mt>.3.M.>S.}.......4. |

### C:\Program Files (x86)\AutoIt3\Include\Color.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 10272 |
| Entropy (8bit): | 6.307934892632479 |
| Encrypted: | false |
| SSDEEP: | 96:SpkKfY3Sr9SSCPTbVww2rxt+/va8WBLVURFIm2pRNb2iOrod0719DJO39fNrsw:SqKfY3qMnQ0Ha9EFIm2pRxYM417ODrD |
| MD5: | F978819F881AD42CB8C450C288356E58 |
| SHA1: | 7AC4B6BBD5F298B2FF0871740ED02ADCAF14BC9B |
| SHA-256: | 497201C1DACCEBE4FBB3626CB27239B22D36DB2536AD034958228117E9E84780 |
| SHA-512: | 320F5A35D1C983BE9E715B3A056DC643D86674992426455875507CD25BB30437E679D1842CBB772823D7F7F22847246527BDB101AB6CBD61127CEC32975A0084 |
| Malicious: | false |
| Preview: | ..2#............<X..C.@.. .h.%5.C....gV>...N..g.hz]......~.]D====================================================================================================================..; Title ...ErnH.BV....s.....C.........u..a..J...8.c.yF....4......p.ZYEnglish..; Description ...: Functions that assist with color management...; Author(s) .....: Ultima, Jon, Jpm..; ===============.Va}[.QQ..V..<....h.......\.!.Q\|..D...4.p.N@..P._\|@....c.]D==================================================....; #CONSTANTS# ==============================================================.Va}[.QQ..V..<....h.......\.!.Q\|..D...4.p.N@..P._\|@...2.#.nst $__COLORCONSTANTS_HSLMAX = 240..Global Const $__COLORCONSTANTS_RGBMAX = 255..; ============================================.Va}[.QQ..V..<....h.......\.!.Q\|..D...4.p.N@..P._\|@....c.]D==================....; #CURRENT# ==================================================================================================.Va}[.QQ..V..<....h..../..>.s..3.C...} |

### C:\Program Files (x86)\AutoIt3\Include\ColorConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2919 |
| Entropy (8bit): | 7.711975722239858 |
| Encrypted: | false |
| SSDEEP: | 48:YgERlwfyEuEgEVv4T2JFdAjLdESSGZTOjPoFtcJCGAer7FrgzSMK9x:OqfrXASJPG1ScSzMtc1rvEk9x |
| MD5: | A4A009944D14CC526874F4ACDE5EEB2B |
| SHA1: | AFA25CD4A266A476505AA729AB443D592AD59815 |
| SHA-256: | 4E9C3621FA86E1B1B9C3C6AC3BA314C1F5171DF6DECCB7F2FD8479A2DA6847C8 |
| SHA-512: | EAC32014AA9212782E788770BD2E1DCB2BDFCD1B7C8A5A35FBCDA5393BB09D89C0BAE40F6B0916B95EB6F36E030B54FC5910F09A1FE7F1AE5EC0118CBC22C<br>1D4 |
| Malicious: | false |
| Preview: | ;..I@.`;_...R.?0.(..+...E......d.aH..Be.......]l..v,..!..,;...%.....8+..b....5.oXvu..X......d.aH..Be.......]l..v,..!..,;...%.....8+..b......iE.!.........w.r[..<7\..VZ..m[...d..U6.Gc..Fw......68..R...~i.5.*/.K......y.2....0?..p...#..?x..<l.?<.@v..KB.%b_.....\Y^}.7.k!...k.WP..\|....;@..C...[q..?y..41.1(...6.``.asC...*.ANWz.r&2*..6..M..w6.;.._v..=...]l..v,..!..,;...%.....8+..b....5.oXvu..X......d.aH..Be.......]l..v,..!..,;...%.....8+..b....5.oXvu..X......d.aH..Be.......m[..hR..O.._R...%.....8+..b....5.oXvu..X......d.aH..Be.......]l..v,..!..,;...%.....8+..b....5.oXvu..X......d.aH..Be.......]l..A...<..}i...[..YX.qe......WB?..>.)).&..Y......:..>.g.....Pa...W..[..sg..lw..^...JZ......qq.5.b.{x..U.. .OP;.0U...+F.t{..2....T..<r.!6..i^.m@.dz....,...qG..7....$....G...7.rRu..UU..#>..?1.S..CY..lP..k...5nv.....?0ud.0.'h.......`p...*..>.....L..Xa..F...s .}&..Ak...o.JDo........8.bUsx..h..F.A^5......x...{{..,...k,..dr.W@.."...EN.%U_.....qu~G..(....+....[....C..u |

### C:\Program Files (x86)\AutoIt3\Include\ComboConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |

| | |
|---|---|
| Size (bytes): | 8085 |
| Entropy (8bit): | 6.820140356592481 |
| Encrypted: | false |
| SSDEEP: | 192:rll+Sm7gUz8DrxGKo8HQHPo2NnggxD1vCm5:rlsYU4PlbQg2NXvCm5 |
| MD5: | 557B75BA9C260B34E2915439A2BBC9A2 |
| SHA1: | 493C87167FF5F27B299514847F41353230FDD0E3 |
| SHA-256: | 08F2EFC5F2AB4701D58F7C832E39E9FF7C672F1455967FE50932016433212812 |
| SHA-512: | D8F2C56E843F3D5818429708A561D9F880334B86C88CB0C2BD717003557727FF6FB4D882132D9BF6EFF77A03B11AF1614E15E03C624E6015416F5F1D0CB8C0D3 |
| Malicious: | false |
| Preview: | .........\|.'Q..,....D.DPB"..l)P.M$.Y.=.&..%L]WX.......h4c}=======================================================================================..; Title .........: ComboBox_Constants..; Aut........G.?...r*.=...A...(..xS.6qM.^7.J.:.^..t...h......%}7/n ...: Constants for <a href="../appendix/GUIStyles.htm#Combo">GUI control Combo styles</a> and more...; Author(s) .....: Valik,.......A.....a$.1..q<..YPB"..l)P.M$.Y.=.&..%L]WX.......h4c}=================================================== ==============================....; #CONSTANTS# ====================================.........."...a$.1..q<..YPB"..l)P.M$.Y.=.&..%L]WX.......h4c }===================..; Error checking..Global Const $CB_ERR = -1..Global Const $CB_ERRATTRIBUTE = -3..Global Const $CB_ERRREQUIR.......$.p..A\|Z.b..hB ..!?-Lv..QM.P4.i/G.t..tQ#...H.....P~} 0....; States..Global Const $STATE_SYSTEM_INVISIBLE = 0x8000..Global Const $STATE_SYSTEM_PRESSED = 0x8....; ComboBox Styles..Gl.......]..;..~.X.X....S..(MB?..e$M.PX.. |

### C:\Program Files (x86)\AutoIt3\Include\Constants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4547 |
| Entropy (8bit): | 7.730739147698964 |
| Encrypted: | false |
| SSDEEP: | 96:b2CXT2i2nnrj6qRL+QpDI0KvyK/OpUG2J/:R4rj6qvFBT8OpX2J |
| MD5: | B83F64F5443EB0DE4DF4CD644A5FC1F6 |
| SHA1: | DC5428831F639A37A1401076759143527B9A770D |
| SHA-256: | C5C7C5F8D5A3443FDA383532A6FB87A7390927F0B0417EE19802D921D0A84EF5 |
| SHA-512: | C4B5AACB4E4722BA1C26522DE0171C5126D7135CDCDA3E5AE5B94ED1B8134F83BE9F62CA4E96D1EB1B7143E3E738E7239D8E4914C31FF7121A3DAED56EF06<br>0F3 |
| Malicious: | false |
| Preview: | ..i.....K.c...............<..a".m.....Z^...O..r...p~...);....i........u....1.....}...<..V,.j.\...V2.V,.n..'\.H);....s....).#...g.........A... ..L9.0.....~...\...~..wu.^......i...........~.........W...=..C#.m.....y5..Q!.. ...Qh.n.:....t_............\.3..........n...p.#.O...I......&.8'...Wi.N..:L.......=../.K.........n...p.#.O...I......&.8'...Wi.N..:L.......=...2.........}.....p......2....t...S...D.:.I...4_..... ...g...........=..K>...I..\ ..O6.u.+ ..B.'....'....M.c...v........M...s..>.l.....~...J6.i...%4...Dn.9...c......P.t...Q...........4...m.0.....I......&.8'...Wi.N..:L.......=../.K.........n...p.#.O...I......&.8'...Wi.N..:L.......=../.K...... ...n...p.#.O...~2..a.U...KN...Wi.N..:L.......=../.K.........n...p.#.O...I......&.8'...Wi.N..:L.......=../.K.........n...p.#.O...I..2H..H...%n...5.S..u.......s...\|........\..7..K5.r......V..LO..;..Do.. d......i....).....w........K...s..Gm..... |

### C:\Program Files (x86)\AutoIt3\Include\Crypt.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 27609 |
| Entropy (8bit): | 6.48513689704632 |
| Encrypted: | false |
| SSDEEP: | 384:BmyFQ4JH67/DiNwVE6U8vNYVUnZZP1DhBhvDloNfpR3UL8SoUN9aLZ:4yy0N+1YIuoXYLZ |
| MD5: | E0B573A4342B45F5D00084A0AFA7B60E |
| SHA1: | 9A95EACBBC42ADAB57EC3C0B1C8944CEE1F5D848 |
| SHA-256: | 42F174DA9ACC5D12E4C61DABF9BDC7726BE6201FE48DA5C34E13804DAD8F571D |
| SHA-512: | EDD9D70BE54B9767966EC8F98886E7C347A2891EC736157579A351E546C3037ECA65079D9919442C5EE9336B775C93C136A1077C5E0B7259FA89548B6E1A24DA |
| Malicious: | false |
| Preview: | . H\|..=.[.%...kJ.exU/+i..l%]F^p..7.{4EB.E.....5x..@Is.$$../rror.au3"....; #INDEX# ============================================================================ ======================================..s.-..-.......,hw.eh.d%e\|M.n0..#.. .\|....&{._.vB....J.pE..Y.14.5..; Language ......: English..; Description ...: Functions for encrypting and hashing data...; Author(s) .....: Andreas Kar..=D~.....[.Z.l>d..ai<@0k..lhm..-.Bw.&4...&j.f.e&...f..jX..W====================================================== ==============================================================================....;...~B...D......"*u...40.w6vo^=}#..>.Qd.5'...Z3..+Sk)...]V ..wX..W===================================================================..; _Crypt_DecryptData..; _Crypt_DecryptFile..; _Crypt_DeriveKey..u.O..`.\|. [.mx1h....jT. .p4Al^`..).L{PV?m5..U./d....V.:.i..e..; _Crypt_GenRandom..; _Crypt_HashData..; _Crypt_HashFile..; _Crypt_Shutdown..; _Crypt_Startup..; =============== =============..s.-..-......"*u...40.w6vo^=}#..>.Qd.5 |

### C:\Program Files (x86)\AutoIt3\Include\Date.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 83198 |
| Entropy (8bit): | 6.49010464492589 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 768:qMGsIttPI2TQmjmPvu7EgprwQTbR+duUxxMlfcc3hKUbweHcm58HSpM4xm:qMGsIfo2WJ+TTb0qT9r5Kg9Y |
| MD5: | FFF4EB24DDD2237676FD0FD10F61D48A |
| SHA1: | 3895C45A82F60A9CD282B851B4CE895269AB9A72 |
| SHA-256: | A0B845107949E34441F36C52930C51A6ED1241580F90EA3BEEA60307459E5F58 |
| SHA-512: | 24193BAE0C2BA60DFF516D01A8D12FDBB609C267B7109923C65E150DBF5BA7DAA306333C105F762BB37B638BF65CC753C076030282EEFFFC39065786F47F66A<br>A |
| Malicious: | false |
| Preview: | .:....t./<..'?..(f.6p......3.....Zv.....J/.}..K.\..s.:..+....ory.au3"..#include "Security.au3"..#include "StructureConstants.au3"..#include "WinAPIError.au3"..#include "WinAPIHObj.au3"..#in.?....F...$4fZ.gj.4i....:.gE..8..8.....<@5..{.B.-.r..6..^.=========================================================================================..; Title .........: Date..; AutoIt........zrGS....%:._'..P.. ....S..6.....Uh.`..}.;..s.&..b..C...: Functions that assist with Date/Time management...;                    There are five time formats: System, File, Local, MS-DO.s.....x.$=......bb.un...R..!......[k.....Ko](.+._..~.E..+.C.            one of these formats.  You can also use the time functions  to convert between time formats for ease of..;   .s...1.`rT]...f..'u...V..g......L......Mi.z..o.Q..>.u.o..O.jlandes, exodius, PaulIA, Tuape, SlimShady, GaryFrost, /dev/null, Marc..; ====================================================.n...,.}oI@....62.h!......z[...@..%.. |

### C:\Program Files (x86)\AutoIt3\Include\DateTimeConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7368 |
| Entropy (8bit): | 6.8152234061787995 |
| Encrypted: | false |
| SSDEEP: | 96:Wy3qguv8u1BhF3C9fVuX9dMo2dGdahgCkPkbVaFmsI1yEop2tv6Gj:WyaguEsBjeGahg38bUB32tyGj |
| MD5: | 38460A57330C341347B40150ACA93071 |
| SHA1: | 2CE1187A7264C22202A15F9B2BEAAEB392AC4BC1 |
| SHA-256: | 81B3D654E785C28BA7C8260C5321F7FFFAEA3959AA6B639839EFA3608C508DF0 |
| SHA-512: | D2223094D7E2056C177B523184C432229C943A50EB7331D07581FA3CB2A62F3D20A67609B72E05C70AABAFA69CB25AAA59129279769DE7E82BFD5896F3BB3CB<br>A |
| Malicious: | false |
| Preview: | .....E...v.5..}7..2.E...w.4.....x.J.m....../....>...4."{..3=====================================================================================..; Title .........: DateTime_Constants..; AutF..8U..v.v.#D...#."....t.h..QSX..k.Y.~...~.S~.....#.Y.j.v6..an ...: Constants for <a href="../appendix/GUIStyles.htm#Date">GUI control Date styles</a> and much more...; Author(s) .....: Val@..)Q._.9.wz0../.1....i.4.....x.J.m....../....>...4."{..3================================================================================....; #CONSTANTS# ==============================....S...$.k.>J.../.1....i.4.....x.J.m....../....>...4."{..3=====================..; Date..Global Const $DTS_SHORTDATEFORMAT = 0..Global Const $DTS_UPDOWN = 1..Global Const $DTS_SHOWNONE ....dw...x.v.l.I..6.X.....M..atp....W.p.0.\|.[p.....p6..M.L...CEFORMAT = 9..Global Const $DTS_RIGHTALIGN = 32..Global Const $DTS_SHORTDATECENTURYFORMAT = 0x0000000C ; The year is a four-digit.. ...T...u.4.oWy.Ra.,.....Y..e\|o....W.p |

### C:\Program Files (x86)\AutoIt3\Include\Debug.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 27200 |
| Entropy (8bit): | 6.546339284293852 |
| Encrypted: | false |
| SSDEEP: | 384:M6RRIoNJW59vkp1IhlbGKP5MhtwKmYgc1Q0Q2UYv4MF9ZjHiWGEo:HWnvk/Ih70bnQ0oI4uHSEo |
| MD5: | BE253E248BAB1C25C52679A6B1A7C234 |
| SHA1: | CD043FAB3DBA2AC2DB1D511053F03FDEBC9CFF22 |
| SHA-256: | AEE358A456BB081CA773C1CA6BE9C6783D18610A5FF4A52BE47918F3A3B5F024 |
| SHA-512: | 9A8839E521CDC849EB29812E6154FD6579AC122B197AF06F5A5C4EB0958CDF009AFBF8D5F26CEF0D1D3D3370F3432577A375937DAC1968EA9BC63889DF7F5F<br>1 |
| Malicious: | false |
| Preview: | [D...+;...[...x...\|.Y.F{G4M.#*..# $....[....L..i0....q...."AutoItConstants.au3"..#include "MsgBoxConstants.au3"..#include "SendMessage.au3"..#include "StringConstants.au3"..#include "Win9}....(5.Y.[...`@.^(x.Ey;{..gS....gTw..Z.........Y..S. ....==================================================================================..; Title .........: Debug..; AutoIt Version :X.....3Y.Q...t.....0B..Hw(\|..4....PRj....H..M.V..J..N.h...Uons to help script debugging...; Author(s) .....: Nutster, Jpm, Valik, guinness, water..; ======================================E.....;i.W.k.'.f]..-Q..[d;{..gS....gTw..Z.........Y..S. ....==========================....; #CONSTANTS# ================================================================================E.....;i.W.k.'.f]..-Q..[d;{..P)..z*%.......^.J...U..9.s...hext _Debug = "Debug Window hidden text"..; ================================================================================E.....;i.W.k.'.f]..-Q..[d;{..gS....gT |

### C:\Program Files (x86)\AutoIt3\Include\DirConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1409 |
| Entropy (8bit): | 7.412938556318461 |

Copyright Joe Security LLC 2023

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 24:z0frFQTAcfrFQ5lQsj0p+GAcfrFQTAcfrFvaAcfrFQTAcfrFQymEsLsw+ydvv84I:z0jFAFsSsuFAF0FAFNsLs9mvNUTbFAFA |
| MD5: | E0212FD91B1C515A5D3A212E0EC66E4D |
| SHA1: | FA0CC267099549EAA2547B160B7BFBF110008429 |
| SHA-256: | 9E18AD9A4A4EB9D06E211450DA2FCD7F782F40AB7ECA9116908CABF679B94DE1 |
| SHA-512: | 2B4789AA7F4AF64359BEAB1E818B2EA00C3FFD6B18A0A625DBA19CB34A1D0818858EA848F4E4BFA1E314CBF164B9E18028177EE9123306595876645558A075D4 |
| Malicious: | false |
| Preview: | .H...U...]....#...:Z\^.K.).L...ts.....*.h...U........3...81.................&..$./'...4.L...ts.....*.h...U........3...81.................&...(2N.g.l._...g`....S.'w.............XjE..l..U..............."3^{.t.h.....g`...y. 9A..e......~..Ck,.....e...E..@....L~..wp~o.v.)....i.....7.f..........{..Bb,..H.S...X.......on..va:i.3.'._..../.....P.'Q............81.................&..$./'...4.L...ts.....*.h...U........3...81.................&..$./'.. .4.L...ts.....*.h...U........3..&......h.............&..$./'...4.L...ts.....*.h...U........3...81.................&..$./'...4.L...ts.....*.h...U........3...81.0..I......@...jW.KPZS.V.4.AR..y~.......9G.........J ..hL^..n.................u\|p{.3.f..^.......A.....X............@jn.....H.....l..{H.\3/:.k.9.A...yC....v.uk...........J..b%1.B.........t...B;.w`f:.W.E.#o........'.e...X.......o..ojb....b...t..a...;..)#"*.#.9.{m. +/.....d.u...$............5<....+............&..$./'...4.L...ts.....* |

### C:\Program Files (x86)\AutoIt3\Include\EditConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5148 |
| Entropy (8bit): | 7.795800976286432 |
| Encrypted: | false |
| SSDEEP: | 96:s2p757Y+Ofr50Ja5WoZdJnBKPAWhI1ixLparc:p5e0JtML+AWa1iNparc |
| MD5: | 46B5AEC58E96123C171B1EAC98F58A31 |
| SHA1: | 3EEB3C6EF05CFDE02CFC52F7203363137B7B9C3D |
| SHA-256: | 2F53876C0D30A436EAE93C0F65AED0D6882F93F9ABC4043D7B39508CB2CB4985 |
| SHA-512: | 8B8F025CA96E2BD7E7BEE0E7C763D24B0C95C287744562F137DE064391BA82C2E92FE6AB5B3C0935E2B39178D767842421E9F2942BF6C48878E4E34EC678136E |
| Malicious: | false |
| Preview: | q.....+\.t....XZT...8...q.....GS......WMN>jB.A.......?.._.o.....sL.'..o\l...A...q.....GS......WMN>jB.A.......?.._.o.....sL.'..o\y...(...Ml....T@.......)..p#........v...........nK.)....\|Ty...0...]-...T @........~.l_.....D...m..L.\|....<..'...."..........a.........z....-%:#4.........v...'......+..5.....6A....\..Ml.........2.......q...\......T....~........i.....\|l~...A...q.....GS......WMN>jB.A.......?.._.o.....sL.'..o\l... A...q.....GS......WMN>jB.A.......?.._.o.....sL.'..o\l...q.........=......WMN>jB.A.......?.._.o.....sL.'..o\l...A...q.....GS......WMN>jB.A.......?.._.o.....sL.'..o\l...A.."w......c..S.....)..p#_.9...h. ..?..o..........i......"1.......A......N..Q.....9/!J.7.\... ..m..........".W....../1...H...D#..............:5!@.,.\... ..m..........".V.....21...M..o .............+# T.-.\.......n....r....j4.E....."&...\...A......N..Q... ..9/2V.0./...a.."..Z.X.....n2.t......>:...8..dl.....p)..]. |

### C:\Program Files (x86)\AutoIt3\Include\EventLog.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 32042 |
| Entropy (8bit): | 6.4708245454472735 |
| Encrypted: | false |
| SSDEEP: | 768:LBOZdCaSSjyLux5oSoubKy0HlJJLNItx98PHJfDADy:ozoSoxVP |
| MD5: | 61115B439949D2EF878B12BC7381CF89 |
| SHA1: | 1171CA530AE5076D8B0607EDB8F229929738B69E |
| SHA-256: | 217BE5838A8C2EBB1474EBBC634C3FF877520E7FD3E9508DB9B8F7B7C9121B86 |
| SHA-512: | 1E0913225A3F16AF3DEA25442B69D548847562340DF1B820D2402F39A20258730B9BDCE981CA5F96491BE3CB92C16D9AB41286A1C793C6322F819FD23449451F |
| Malicious: | false |
| Preview: | JQ....X.......B...K....BN+..W.p4..p"....9c9e;=.{..a..r.}.u8sj.include "StructureConstants.au3"..#include "WinAPIError.au3"..#include "WinAPIRes.au3"..#include "WinAPISys. au3"....; #INDEX# ==T..J.........u...H.B...S4.U..ch..o.....h+`=&".#.....6.!C{'C].=========================================================..; Title .........: Event _Log..; AutoIt Version : 3.3.14.5..; Language ...G..M..R.E...s....F....N.g.F..du.U<L.Q..ub5ao?.m..`..\.r.)m.@.ystem logs...; Description ...: When an error occurs, the system administrator or support technicians must determine what  cause........L....E...U._...N).H..~u..3[.]...ub2 iz.q..a.e.<.)i.@.ata, and prevent the error from recurring.  It is helpful if  applications,  the..;                  operating system, and othe......Y.....+....@......d..Q.?;..7Y.V...&c>h;~.>..d.n.s.?:...ditions or excessive..;                  attempts to access a disk.  Then the system administrator can  use  the  event  log  toI.......M....!...UR....-U).H..~u..r.... |

### C:\Program Files (x86)\AutoIt3\Include\Excel.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 57934 |
| Entropy (8bit): | 6.658019826464878 |
| Encrypted: | false |
| SSDEEP: | 1536:SxOzsXRNbSWXnq6KE26ZBLHg0uZrgek8eIfm8p5raFriJCxrj756qG1aBEbc2:S4q/ZXnq6KE26ZBLHFuZrgekLUm8p5eM |
| MD5: | D986FB866E4ADE032EBD83DA7659C938 |
| SHA1: | 2E73C8ACFCA3A5045D989B01EDFA9B16EC109FE2 |
| SHA-256: | 23FB275792FB6D9FD3C73127CDFA82BCDC0E6C06F33637FDD5239BA328680B38 |

| | |
|---|---|
| SHA-512: | 479BADA3DA0BBE321C8332EE0412050B4398F587D34F0D83282E38EEDCB86F9AF40AC6324C93BD61393BE91CAD1B7BC7BDB7EB7DEC1B0DFEF1B58D2BD8BE 9177 |
| Malicious: | false |
| Preview: | ...e.....oU.Y....o....QN.(.....Q6..u....p.....]4..q..@t..,.3"....Global $LastExcelCOMErroDesc = ""....; #INDEX# ================================================ ==========================..;.....=...90..<W.GO.S.TZQ....8..B..^.!......q>..W......q... Microsoft Excel Function Library..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: A collection of f...r....fT..en.r........G.....Qi....C.u......Qw..Q...f..,... Author(s) .....: SEO (Locodarwin), DaLiMan, Stanley Lim, MikeOsdx, MRDev, big_daddy, PsaltyDS, litlmike, water, spiff59, golfin..&....r^..C@..!+...Q..I......Hl..D....s......y.[..9;...b...============================================= ============================================================================....; #...T....=...90..<W.GO.S.TZQ....8..B..^.!.......j.H...=...b...======= =====================================================..; _Excel_Open..; _Excel_Close..; _Excel_BookAttach..; _Excel_Boo...i... d.Dgh.C...>]..dmW.... G`..=.. |

### C:\Program Files (x86)\AutoIt3\Include\ExcelConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 19931 |
| Entropy (8bit): | 6.594933766785971 |
| Encrypted: | false |
| SSDEEP: | 384:eucAmPzQh/Wsgwg52/8MA1g/L81Nye51txue/aLew:GAT05MA1gD8ae7BTw |
| MD5: | 37A6AE76D56E834A76AC0857466C3A73 |
| SHA1: | 9D8EFA50E69FA7056F69621A290A6A9C04AAB270 |
| SHA-256: | C916C1BB0F481C772A2BA762961D5DF820A44C7B6270BD1B1C980C6036CC77A4 |
| SHA-512: | 66E6BDC0BDCE148549EC8E6DAAB150BC9651565DDC6333A932464BC94FAABC4E5725DFEAA58C8F79D32152746B002939BBF314921A40833416D60B57D4C7D0 9 |
| Malicious: | false |
| Preview: | f.;..r~..[.bGU.x.,4...6.9.. ..9:=_[..R......s....T.d.......C:.=========================================================================================..; Title ...... ...: ExcelConstants..; AutoIt ..'..ht.../.v.A."..m.>..R..z.*).LH..O.S...C...u..:.....[\^)..: Constants to be included in an AutoIt script when using the Excel UDF...; Author(s) .....: water..; Resources .....: Excel 20t.u..rw..U.hM6.O..`.&.]..F..3..guo..D.A.Y..;..X..8.......F?.5(v=office.14).aspx..; ======================================== ==================================================================x.h..:'....<.e.H.*).k...l?.>..JTT#(v.L......s....T.d.......C:.====================== ====================================================================..; XlAutoFilterOperator Enumeration.e.%..n\|..G.uJ=...rf."^...Z..n.ph ..Q...@.... !...X..+...D^.b. by a filter...; See: http://msdn.microsoft.com/en-us/library/ff839625(v=office.14).aspx..Global Const $xlAnd = 1 ; Logical AND *.u..nn..].0.9...Tf."T.... .Z..fflB%M... |

### C:\Program Files (x86)\AutoIt3\Include\FTPEx.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 45916 |
| Entropy (8bit): | 6.631269137746139 |
| Encrypted: | false |
| SSDEEP: | 768:q3onrQN1zjxumu9IwI1waJY4/+T2hov+qLTai:qiQNduywIqaJY2+ahoGSTx |
| MD5: | 57C7534E363EE5CCFDB6AA1BDE2827A1 |
| SHA1: | 82D0ED9EA518797AFAB308D90BF54F483ACE2BA9 |
| SHA-256: | 9675455E9B4BC2DEF594517961C1D26A3C2552A6F1C4295972F4D7F0F2ED1714 |
| SHA-512: | 262289B852698DE8299F5727AC713DA1B0F56D438F4EFA4F2812EF15A0DDAC9B007E826C5123C6F25DCF608B968B9EB764F5A49D5A7DE0FF531B827A0D989E9 F |
| Malicious: | false |
| Preview: | ..H.-j....wpN...Y$.....z I..6C.F.... ..=.R..,..8.U..[.lK...q.O3"..#include "StructureConstants.au3"..#include "WinAPIConv.au3"..#include "WinAPIError.au3"....; #INDEX# == ====================....\|".L.V$..<..Gp.]..."=V............n....t...l...U..%...b..==================================..; Title .........: FTP..; AutoIt Version : 3.3.14.5..; Language ......: English..; Descriptio...o%.7P.zgBn...%....li...5O.O.p....h....!.."...F..6...*._r, Prog@ndy, jpm, Beege..; Notes .........: based on FTP_Ex.au3 16/02/2009 http://www.autoit.de/index.php?page=Thread&postID=483..+.z?.L.V$..<..Gp.]..."=V............n....t...l...U..%...b..============================================= ======================....; #VARIABLES# ===========================================....\|".L.V$..<..Gp.]..."=V............n....t...l...U..%...b..===== =====..Global $__g_hWinInet_FTP = -1..Global $__g_hCallback_FTP, $__g_bCallback_FTP = False..; ============================....\|".L.V$..<..Gp.]..."=V. ........... |

### C:\Program Files (x86)\AutoIt3\Include\File.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 44268 |
| Entropy (8bit): | 6.709693589202476 |
| Encrypted: | false |
| SSDEEP: | 768:mykPkjd7XIWliN+lgzD8Jhy73MPN0ZAZfTZmeIDdtp0Wz7:Osjd/iNMgUJw73IN0UmeIDbuWz7 |
| MD5: | 8131E0D17A70C1953C744CDDF40AF9E5 |
| SHA1: | 7FB7C515CD752A9EE5B19B233512FCAA11D8F31F |

| | |
|---|---|
| SHA-256: | DCFE586EF8530EDE2B833F45F52CB0C8D9BBEC84BA6D2EA381AF79D2F5931A6B |
| SHA-512: | 1C87B4DF51149C43F1F8969D985E322F16F07DC7818A1A043440BDB5FE6F08520ABFBDDF6D8E2E0A893FA0EF4731A326E62889464CE11BD5C9047E00D045841 |
| Malicious: | false |
| Preview: | 85....l.y.......+k.....1..F...x.1fn..y...Q......k..rQ<U.@.._u3"..#include "StringConstants.au3"....; #INDEX# ====================================================== ===========================&a..V..4.+..E....8.W...,.......$Z?y^...k.p..N... ..2.f.X..ZRe..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with files and directories..V..*.a.d..Q.....I?.(......Q...9*k'..\|A..G......g..oJd.([...JdeB, Jeremy Landes, MrCreatoR, cdkid, Valik, Erik Pilsits, Kurt, Dale, guinness, DXRW4E, Melba23..; ===========================&a..V..4.+..E....8.W...,.......$Z?y^..-\.........3..!.u._....=====================================....; #CURRENT# ==========================================================================&a..V..4.+..E....8.W...,.......$Z?y^..-l...G..{..PK&Q.9.. ._FileCreate..; _FileListToArray..; _FileListToArrayRec..; _FilePrint..; _FileReadToArray..; _FileWriteFromArray..; _FileWriteLog.V..4.e.A........`.`..A..\.....m9d<. |

### C:\Program Files (x86)\AutoIt3\Include\FileConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6995 |
| Entropy (8bit): | 6.8295069312709344 |
| Encrypted: | false |
| SSDEEP: | 96:KmGr0nRyRKqwRf4/UMB2OWj6Rf3PiV/t3wvoS6seYtUBH5qFv1oM8:Km3R0KqwRg/U82ODI1wvC5qFv1of |
| MD5: | 62E29CED03FC1DD443E7080B7B5C9083 |
| SHA1: | 1ABBA31436880E9CE51F00BA08AB06776F07BC5C |
| SHA-256: | 4939D7F9DF430C753402350D35B1467A266A66D073E081007BFA39D753132AA3 |
| SHA-512: | DB87D105F2EE3737B469EF3E1FE3CF4642E08A87D9A41EAC4213C98255E8F64909F99FEA5BFE1049D2DC59A876657BB007EEF584BA8F8B9D089BFF9C546972E 9 |
| Malicious: | false |
| Preview: | ..U@..^K....1.....C.ErJ...........8G.6x.......MV..b0.....=====================================================================================..; Title . ........: File_Constants..; AutoIt ...EE..\.......1.1..aD.*..........%?.l).........6}......: Constants to be included in an AutoIt v3 script when using File functions...; Author(s) .....: Valik, Gary Frost, .....; ====........[.........7..=.Tb..........8G.6x.......MV..b0.....==============================================================....; #CONSTANTS# ==================================================........[.........7..=.Tb..........8G.6x.......MV..b0.......; Indicates file copy and install options..Global Const $FC_NOOVERWRITE = 0 ; Do not overwrite existing files (default)..Globa..YB..B...~...u.O.. .Id.......BI.`..x1........f..3b......st $FC_CREATEPATH = 8 ; Create destination directory structure if it doesn't exist....; Indicates file date and time options..Gl...Z...U......d...u.C. .lo.......WB.%. |

### C:\Program Files (x86)\AutoIt3\Include\FontConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Public Key |
| Category: | dropped |
| Size (bytes): | 3920 |
| Entropy (8bit): | 7.790799057106601 |
| Encrypted: | false |
| SSDEEP: | 48:6AUEfs0uJLhDwKUBUYBSgInfpTY6OV8u35b/6nPyBRqLMJmBPU9YicPalFF9pSCf:64fsLDlUz0fJYxvb6q24kBc9YillFhh |
| MD5: | B17AE8020A7D1DB046C22AEFC777651A |
| SHA1: | 1CEC7BCC3EFFB46ADB1D3D443B77C1A11BB820A7 |
| SHA-256: | 625A44440C339B7AD67403451F1578DA00646C28E6B792E0FCDA0E590E15A3F5 |
| SHA-512: | 648EBE64D1DA40F94A762DE204FABEF74A02E6B65ACCE0F9667DF3BF6F78707F369709630767AFC31FD383CA5EB4B7CEC24B6569BF1737303C9A269B53FB3FCE |
| Malicious: | false |
| Preview: | .....D"C...l....C.\V......<.4.=m..E ..R.&....D9....).a...N...Y..Z.zS.C.4'..2.^.(%..\|...<.4.=m..E ..R.&....D9....).a...N...Y..Z.zS.C.4'..2.n7.8..5F.../.'..~..B=...WD....j..&..4.)@Ne......NgT.M.:4.!.n7.8../M..d.'..~..B=...Or.....Y@..H..d.5[O.]...D..S3....)\|../..Sa8../I..o@'..k...i....h....W*.l..m..FN_....D..Z.zS.C.4'..2.^.(%..\|...<.4.=m..E ..R.&....D9....).a...N...Y..Z.zS.C.4'..2.^.(%..\|...<.4.=m..E ..R.&....D9....).a...N...i..m.gM.1.ZN..[.@.(%..\|...<.4.=m..E ..R.&....D9....).a...N...Y..Z.zS.C.4'..2.^.(%..\|...<.4.=m..E ..R.&....D9....).a...N...Y..Z.Jd.^.ft ....$Qzz..ai..u.-.W...6I..=f;.....>h..J.W.2GU.W..0.).zN.N.....`..Q5[..2^..VIL.T.z.1Z..O.;.....>h..J.W.2GU.W..1.5a.'.6.)'.?.n7Rt.. F..o@}.$.l.4T..;.&.....sC..I..4.3ZRXS...;.5m.".C.= *....Rwy..E...!.O._.~.-Q..O.;.....>h..J.W.2GU.W..)..u.N.^.9*.H.._tt...D...%u^.S.v.:R..O.;.....>h..J.W.2GU.W.. ..b.".^.),...$Qzz..ai..u.-.W.y.4Y..O.+.....f.....z.(..j$...0..%o.*.C.1 *....Rwy..E...!.O._.w.*\. |

### C:\Program Files (x86)\AutoIt3\Include\FrameConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2382 |
| Entropy (8bit): | 7.651398665206537 |
| Encrypted: | false |
| SSDEEP: | 48:tdGVdYtQdGVdIdGVdG5sJ0Ra7BD4ZFwUvXmXZ74eYvV/XHMr3kEoj/8CCJUldGVO:tdQdYtQdQdIdQde47BsZFwUvXYZ7VYvZ |
| MD5: | C25CAF6145849C5F8DF305F17FB29CE6 |
| SHA1: | 5A9D79C5733EBFE174B422DA7A6F60A84CD15547 |
| SHA-256: | D94C71A910AE0842506E1E7691610B4E383A3DF3A35EA75CBB6AADA54392095E |

| | |
|---|---|
| SHA-512: | B1C30E601A199F95EC5911AB1F0DFE650F870C7B4CB8A07DAE45BF4FA19C6B839A817DEB7C2BF35ABC059E64F85C17E0E2F20EE47A842524CE7A2F5CA7C09ACB |
| Malicious: | false |
| Preview: | @2w.M...w.<!e9;..A...S..c..-......!;jT=(...:3...q7y...0.3...*d^f$..@B.gRo.=....\.q.*..}..-......!;jT=(...:3...q7y...0.3...*d^f$..@B.gRo.=....l.w.C..,K.>......2(mIFg.Y.XM.Q8k*..........^-C.\|.R...zUrq.....T.F.7...I.q.D....2(yS P.S.n}..(w*......~....7wMu#.b.....<6s.W...>.%.V...j.q.g.P._i9.rz...)......0...%.'...9wY{^.S._.(.!6.>...\.q.*..}..-......!;jT=(...:3...q7y...0.3...*d^f$..@B.gRo.=....\.q.*..}..-......!;jT=(...:3...q7y...0.3...*d^f$..@B.gRo.=....k.l.T...z.^.r....!;jT=(...:3...q7y...0.3...*d^f$..@B.gRo.=....\.q.*..}..-......!;jT=(...:3...q7y...0.3...*d^f$..@B.gRo.=....\.A.,..9^.0.G..O.qcZcGy.V.k..L?~d.N.L....Yy^{-.+:..8.>bC[_...E...H...z._.......A;.bt...h`..hN....H.[....S$7v.@._.5.!6 .u...1...G...{.-....z.sd6. V.Z.s...d.U....A......Ti`9.O...;.r1tUE.....8.r..2O.u.+.R.}jw*o{.@.#J.q.H....C.]....7dCka.,w8.5.3. w^..A...T...{.D.o..x.W&jI0m.9.@b.C *....y.*....H.6.M.o-*..Oob0L...&.#.v..A.c....{.OY.<TA.z.FJ..q*t.....b....7..5j..Y;..<..U`e... ...^...k.-....0.[j8.a |

### C:\Program Files (x86)\AutoIt3\Include\GDIPlus.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 305135 |
| Entropy (8bit): | 6.394178807129197 |
| Encrypted: | false |
| SSDEEP: | 3072:Jg/XOc2B1NNSkbN5k/pWI0VFF8oFphjwPWVDui9YmrHFBPOJNxx:JGU1Ok00DD3hjtC3x |
| MD5: | 965C1BCCC92ACADF16571006E216AB80 |
| SHA1: | E46A26AB16C21D4C8929F92BBE46A7E501987C64 |
| SHA-256: | C6AD4809DA41118DBB31A3F70F7D962A91076BBB51F32DB642B7D0ED32EE056F |
| SHA-512: | 6960ADD37A19235B0B1A5E4CFD96D9EC2CB1B717CCB2D3AC68986AD19EE4166C46CDADB917244A7FEA8441E590D2C207AE12BE02B2F112765EA1A63AA0F26B9E |
| Malicious: | false |
| Preview: | ....."..."....(M/.Q.w.X..G.z.."....(f.U.(....^uy.\.6J....).ctureConstants.au3"..#include "WinAPICom.au3"..#include "WinAPIConv.au3"..#include "WinAPIGdi.au3"..#include "WinAPIHObj.au3"..#Z....#../%.2...A.(... .u.d.q........t5...tP...ik-...~....Af.=============================================================================================..; Title .........: GDIPlus..; AuG....6#...#.S...]h......C.%b$M..6....g&.......'>.....K..../.on ...: Functions that assist with Microsoft Windows GDI+ management...; It enables applications to use graphic@K..@ ...-.....V.>...3....#>B..'...-a.V.(....0vd.Z.3\...u..; Applications based on the Microsoft Win32 API do not access graphics hardware directly...; z...."..?..X..V.4.Q..3....#.O..2....?m.U.&....<7\|...%.....8.tions...; GDI+ can be used in all Windows-based applications...; GDI+ is new technology that i@K...3...l....L.).A..C....#>B......: |

### C:\Program Files (x86)\AutoIt3\Include\GDIPlusConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 28347 |
| Entropy (8bit): | 6.920400114882896 |
| Encrypted: | false |
| SSDEEP: | 768:6yQVOxNufTxrpmktSgZZDpcP89KvuB0MxNvH:QVOxsH3ZEP89+OxlH |
| MD5: | 50CD288A03BA7A44DA6715E46F22B48C |
| SHA1: | 2CCDA71D2799086FB3FAA7F8F18AA7FE4BF2C3D2 |
| SHA-256: | D34F8B58FBC7A4E934121EB0459C842EA943F115BCAE933A325BECB303C789C7 |
| SHA-512: | 9D66FAF2CF9F305022B61BCEE23D1537623923E5D01671D865078A17E46C74BE0B350DA744908ED743C85D238ABDD39991E46FEEA84E06DE8138E1090449A12 |
| Malicious: | false |
| Preview: | FE....G.%.\|.(...x..<p.^C..'..L..D.....]UZ....[..[x...... =========================================================================================..; Title .........: GDIPlus_Constants..; Auto,X....P.g.2.m.....l..r..1...o...Q..W....%..K.E.k.." ....RLs ...: Constants for GDI+..; Author(s) .....: Valik, Gary Frost, UEZ..; ===========================================================X..._...5B/.p.....e..E..@^..'..L..D.....]UZ....[..[x...... ======....; #CONSTANTS# ============================================================================================================X..._...5B/.G...x.........c...\|.f.....#..T...!..u9......}o\T = 0 ; A square cap that squares off both ends of each dash..Global Const $GDIP_DASHCAPROUND = 2 ; A circular cap that rounds o.J....K.m.v.m.....;....F.pi..u...Q.N...$!7x.w....u2.......=3 ; A triangular cap that points both ends of each dash....; Pen Dash Style Types..Global Const $GDIP_DASHSTYLESOLID = 0 ; A sol.H....F..8~./....6...\r.43..[...%.m<.. |

### C:\Program Files (x86)\AutoIt3\Include\GUIConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1323 |
| Entropy (8bit): | 7.485417162172661 |
| Encrypted: | false |
| SSDEEP: | 24:Lkotvs++P3/Cgun3RTlkotkonAASoxJ1oZJRodJQw6+ptzKhEP3MkNTHFoffQjJ/:LkotpiPCb31lkotkojSoz1oBo3QIFKTK |
| MD5: | DEA2F731E1900838930E03F5785A2D9D |
| SHA1: | 9139EDCEE123E3AC3B09752CF166719D1A373720 |
| SHA-256: | F4B156FE88728A6BBE099C7715452CB60F46F266BE00A28C443726642B00FFC1 |
| SHA-512: | 3EF6C2594D04772D150FAAC53AEB5EC66D9DD4251ED366098D40B97D70EB57DC3FE285617929C7DCC0559CB494214F4CFE7C4711FFEF39FFA32BE70A39BF130E |

| | |
|---|---|
| Malicious: | false |
| Preview: | q^...1.Ni....R.V@..rNB.0zx<...T.P....%.nCY^..g...?..].G).o..o.Z..y..yDB.e.aF...=;.Ude<...T.P....%.nCY^..g...?..].G).o..o.Z..y..yDB.e.aF... R..5=!...G.C......t.s91*.4O..v..j.ZU.&.v&.1..7.D*YE.k.mO..6.=.$86f....C.....8.=.....W6...g.....`.=..\|.I....E7.....x.4...Xah..<xt..IG.H.....8.#.....U....@..`.=..!.G.j..~Y)...3.\|...6.=.,54!...G.C.......h^Y^..g...?..].G).o..o.Z..y..yDB.e.aF...=;.Ude<...T.P....%.nCY^..g...?..].G).o..o.Z..y..yDB.e.aF...=;.Ude<...T.P....%.nsnn..3R..f..B.,].=.L&V...j.^w[r..6.0...."D..-7o...D.R.....+.^tG..6I.. .....W.<.K3Y...%..ftu...;.)....Dg...1l....C.].....m.qsn@..9P.."....W.<.K3Y...%..ftu...;.)....GS.+66r...C(D......p....>Y...k.."..W.<.K3Y...%..ftu...;.)....Lo...1d....C.].....m.qsn@..9P.."....f.!.\|=Y...*.Xj.....R.5...Ndc.J.1b...D.S....l.}..P..P...n....XG.;.Z t...0.E0.Q..z.VX..Xls..yzR...S.S....l.}..P..P...n....X@.0.P<D...0..%.L.{.2..._e&.<+=d...s.R....k.2.WA..yU..w..@./d.=.QConstants.au3"..#include "WindowsConstan |

### C:\Program Files (x86)\AutoIt3\Include\GUIConstantsEx.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4363 |
| Entropy (8bit): | 7.843845537237017 |
| Encrypted: | false |
| SSDEEP: | 96:+DakxIyhUSWVd+0AGn9gcLOiUoNIfrGEUB+tMb:AveSyDAG9ZyKSzGEIUG |
| MD5: | E37935DD7B9AFC8DE2F25FD5820331BA |
| SHA1: | 9CB758A062EEF9CAD1D3172F9317965CDC99B952 |
| SHA-256: | 95EA7554BB8A1F962C339B10223FBD7C6BEA56632FFCB59CCADB932DB758C5AF |
| SHA-512: | 2E470BCA392A1C47FD60E53D8802C78DFEBB5010840315C7BB188298FED3DB58F565676D62461BB90E33ABDC8FB7F5AAD1AB901F69F97CEEA96CC9737F8696F0 |
| Malicious: | false |
| Preview: | ..di.f....c.6.Hh.9!...o.2......h...;......{PGj(vs..WK1......X..77.....-.=....n.'U...../......h...;......{PGj(vs..WK1......X..77.....-.=....n6.S...C.w......{...<.g..].5..9a8.Z.`M,.B.E..E.xy.\|...0.....lf6.S...Y.gLT....{...<.\..[..`pl5.+Q...\|.^.D..K..*I.}..~.s.O.. 6.o....^.2jf..V.%.L.g..]....LVZ.`?&M.B.%......_..zg.3...y.......?.4F.....<....:.n...;......{PGj(vs..WK1......X..77.....-.=....n.'U...../......h...;......{PGj(vs..WK1......X..77.....-.=....n.'U...../......h./.......\|..,4.Fhn..WK1......X..77.....-.=....n.'U...../......h...;......{PGj(vs..WK1......X..77.....-.=....n.'U...../......h...;..8.w.#..$5* F.....V.O..o..eh.....~.t......~L-...d.\j.....e......T..^.oM(2a><L.J.,.^.M..E.od.=..\|.b.W..-=HnH...~.W{v..h...d.&......#..%{8nC.J.~.V......cd.}..x. .M..6sZt....C.\|IV..^.3.W.g..]..?.Kg=;z)/N.).b.C....,.\O.G...^. ...H.Wu....t.\|^G..p...`.C..m..}..MGw8xC(...n.[.i......M.Z...U.T.v....r@-......'t.DU.9.f.h.....g..(,.[..p.9"C.r....P..Mf.q..S.n.O....rE-...c._lk.f~.....+.. |

### C:\Program Files (x86)\AutoIt3\Include\GuiAVI.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 11564 |
| Entropy (8bit): | 6.344057182824136 |
| Encrypted: | false |
| SSDEEP: | 192:njMY2D8uHFUC1EfXafZyBv1V9utWQJZJ9Rt8nVTofJfZozvnSX0Pf98w09:jMY08uHFd1EfXafZA9PQJZJ9Rt8VTofD |
| MD5: | D0FD168E72C37C5E5668EE5D09844B38 |
| SHA1: | E52D712694657C1808972EFDD8DE69C6850E76D6 |
| SHA-256: | 667B54F8EAAB26B20E1CB5EFB62C7BEC12B1C8F86282AB79E1657CD7BC6BBD78 |
| SHA-512: | F1FFC1CB7D60C3A3EE9DEF5E08F158399861B94E037A845748556879051B84B6CD4972F6110EC8BBF1D62983628FDDF968DC8595AD56C87BC9191D32D9680BD |
| Malicious: | false |
| Preview: | I.T..j..#/..dD.I....+......A.....T.......d.Gt...Y,....>.^..u3"..#include "SendMessage.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#include "WinAPIInternals.au3"..#includeJNmu.^..]9..o=......f...\..~.X.p......{.Y ....u.....n.....===================================================================================================..; Title .........: Animation..; +.Ns.k..k2..n'.[..U.f..K.7...v.R......h.!s.._ ....6.O..tion ...: Functions that assist with AVI control management...; An animation control is a window that displays ...].{..#...d&.(....$.......V...1.\.........D~...!....6.E...;                 of bitmap frames like a movie. Animation controls can only display AVI clips that do not  contain  audio.  O..7..?...`.!i.A..[.h.......ye..t..Z..S.../...t...O'....s._... indicate  system  activity  during  a  lengthy  operation.  This  is..; possible because the operation thread ..Th.q..}`..d*......?.......re..X..Y...T |

### C:\Program Files (x86)\AutoIt3\Include\GuiButton.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 28807 |
| Entropy (8bit): | 6.4004339815395035 |
| Encrypted: | false |
| SSDEEP: | 768:IVKPk3JYygVz06zOLNtRl1PWcHl7qL043b3biX+W:kKshk4 |
| MD5: | 86DE7972532180C2018BB1813738C4FA |
| SHA1: | C6931A3454A520B0584CD48286C8C60CE48B3AB8 |
| SHA-256: | 7BA8C8722490136BFE6796FB021AF27735AC179CF5310AAD4052A6DBBE035ADA |
| SHA-512: | B431F32357B9C151C9AC6BE7123B496B5367CCCA263F82BD95DC50FD3790EFC04A28B1CDDC4EEFD1DA2DFFA0A167B2623EEAAB15D7A13F58BF161F2041D70532 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .+...Q#k;.....K..Z...;w. .S.u.N/].r(.. 8Z..q.I..O.Nz...W.....nConstants.au3"..#include "SendMessage.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#include "WinAPIIcons.au3"...+...Q#k6.........}...-\|.n.-.R..a8..g....R~..s.~...U.2...HQ.N..=================================================================================================..; Title .........: Butto.Oq.e2zy..F..3.......q!.3.-.*..L~.o;...66...}.m..d.Ec..Txf.S..scription ...: Functions that assist with Button control management...;                 A button is a control the user can clic.b...T5a`...../....@..12.r.o.D.I.]./Q...n+...n.~...U.2...HQ.N..===========================================================================================....; #VARIABLES# ======..F..z3+.[..\|.......b/.?.>....Q..<a...n+...n.~...U.2...HQ.N..=============================================..Global $__g_hButtonLastWnd....; ===================================================..F..z3+.[..\|.......b/.?.>....Q..<a.. |

### C:\Program Files (x86)\AutoIt3\Include\GuiComboBox.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 41939 |
| Entropy (8bit): | 6.11908417106541 |
| Encrypted: | false |
| SSDEEP: | 768:I3NC5UrTgdtsau0k2J5hRK62L/VOJgJFGP7bfx7dOk2SzvW4K6ujKKhCXz9aVlJq:+M+GC7+l+G |
| MD5: | 7ED9BFC80CFD179277DC7C1C6BC8BF0A |
| SHA1: | 454003F97371E382D13247B62CB6D720F3169950 |
| SHA-256: | 92DDE6052FBF3067B756EC5B59966BD6BB881A704336DF7D2CA3DE295572398D |
| SHA-512: | 41DDF60C053080157A0012A48426C42527CF19942C19B72B0986E77C72E5E95ED90AD6D8C80B0060959214F5040AA2E587617E5AAE0F69A511F197F640F1DB75 |
| Malicious: | false |
| Preview: | )Z.%...v.........%F..*.....p'.e....O..pH.NU.S.....`...h.HennZ.. stants.au3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3(>.e.........\|IVf..$.M.B..E.$..".I..>...Z.0..`C.`...b..4.f]..C...; #INDEX# ==========================================================================================================================7..{ro.3.....<&(...h.Y.t.^*.E..L..P.kH.)@.6..jY.`.?.[i.3...D; Language ......: English..; Description ...: Functions that assist with ComboBox control management...; Author(s) .....: gafroyG.f/.........{c.%..{.^....u.:..\|..M.#..]..]..$..3.1.Uz.:...s=====================================================================================....; #VARIABLES# ==========================7..{BX........./5;...{.^....u.:..\|..M.#..]..]..$..3.1.Uz.:...s==========================..Global $__g_hCBLastWnd....; =========================================================================7..{BX........./5;...{.^....u.:..\|..M.#. |

### C:\Program Files (x86)\AutoIt3\Include\GuiComboBoxEx.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 49651 |
| Entropy (8bit): | 6.12250870768078 |
| Encrypted: | false |
| SSDEEP: | 768:mfpPuoO5L33Idhj1tbrzvY5EtjFAucFpZBFYr5UUJEcmohKfSCvCG6PHzchFzzBG:4433chdul6R |
| MD5: | 2B9DE08A2D703574F6E176D18B2FC189 |
| SHA1: | 1E67A9187C1DBA849E9F70AC388C47B6F1C50136 |
| SHA-256: | 7B11CCC0D49960EBC9D55B05CBD3965728D30D3D9CF16B73E53F852B5D4762B0 |
| SHA-512: | 1FE7B766D3772194DFEC0C1C169DE3A05369605B21AA97490262411C2B681583833708B1CC9A7390317B1AA9BC4D7A013631F0EE7322F33B16E7067C00764575 |
| Malicious: | false |
| Preview: | S..r.=........D(.M......\|..vM:6,.K(...Y%e?.!I...)H2....G.G....nBox.au3"..#include "Memory.au3"..#include "UDFGlobalID.au3"..#include "WinAPIGdi.au3"..#include "WinAPISysInternals.au3"....; #I>8.I.h...D....t.......].a..".Dd...t.W.Jy-1..~...w.zR...=...A.Q<=============================================================..; Title .........: ComboBoxEx..; AutoIt Version : 3.3.14.5..; Lan...v.h...W...'E.M....[....\|M.)6.P'.D.Y~0JGB L..$Wg..W. .]....!with ComboBoxEx control management...; ComboBoxEx Controls are an extension of the combo box control that provi...1.)..E.Y..&P.......9..vR.>'..D.Q.Wd0,..c..j.gO...T......!item images easily accessible, the control provides image list support. By using this control, you..;                 can provi...e.-..F......(N.P....@.\|..r].y .Gi....+ex.D"N..-.3..[.n.O...Leraw item graphics...; =======================================================================================================MA.,.u...D....t.......m.g.I~+...s..I.J |

### C:\Program Files (x86)\AutoIt3\Include\GuiDateTimePicker.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Secret Key |
| Category: | dropped |
| Size (bytes): | 15857 |
| Entropy (8bit): | 6.298329795753108 |
| Encrypted: | false |
| SSDEEP: | 384:WLg7+TlZ8ElFK9eX7hs+UNHGPV504mB8iWT/D:WllZNjqw5BtT |
| MD5: | F921AA3A28A12E6B1771B942A5B69F43 |
| SHA1: | B778C0A57A6CD2399394C7C3C7C864A5DEB09C7F |
| SHA-256: | E88511D226685CB3ED33ADB8A0AEC30ADDDF67BAFB79D177C3EDD5620CA0BEE9 |
| SHA-512: | 3E7E6C706977CF62733DAA7CE50253974D11C9A6C025338D8FE77C722AC601907A9224C3A5C929D73C4800B7DCC9F63D11FB58B993D3E37207C04712B4BB938 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .1.]0..c{s...E..s.[.t.7..&......Y...i8..."5.G.,....L@..5>^..r*.ory.au3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"...&..5..j#x.....8.{.s....c.....Q..t.\...:3.CA=\|.e.ug..3.U..M!.ls.au3"....; #INDEX# =============================================================================================================.e..a..;k!..B..-.F.r.l..(.JK....."c.......E.zY....o../.O..Z=.ion : 3.3.14.5..; Description ...: Functions that assist with date and time picker (DTP) control management...; ...Z=..&7r...!.Y.[.\|.0..B..ME..^..9jv....?".UA~..b.UB.!4_..Q;.itive interface through which to exchange date..; and time information with a user. For example, with a DTP co.,.Q0..i#<...h...F.r.7..t...E..D..vgv...v'.Bl...+.....`z....o. then retrieve his or her selection with ease...; Author(s) .....: Paul Campbell (PaulIA)..; ===================================.e..a..;k!..u..D...*....;.YX.....k;k. |

### C:\Program Files (x86)\AutoIt3\Include\GuiEdit.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Secret Key |
| Category: | dropped |
| Size (bytes): | 54349 |
| Entropy (8bit): | 6.3246109335626945 |
| Encrypted: | false |
| SSDEEP: | 768:yBhEDDDv7nW9aaFcL57HyFeXWlHUqJIjwDX2ApRTNoSMrhHNr9VSbq346e0Qfzmj:6hEPUsr8LNIMzGq1kFN6gXak |
| MD5: | 8C72F4508DFCFC9A281647A9828BBEBC |
| SHA1: | 031E21775236087FCF2AD5F0D4EF26E653557E05 |
| SHA-256: | 19E5698912374B7707307C36907347E5C541DCC5AE97CECE59CE1F1400CC90F4 |
| SHA-512: | 1061E6087C8E84D32D38AA4C6C7C95E3C9784BEE7F3818C673F6D0FD77A4C6A5A64E1D1A307C62D6B22DC7ECBABE7C14480F048EDC0E0712FB043C69D5C8FAB4 |
| Malicious: | false |
| Preview: | ...,.....zi.S"..U.IT..A.%+.l2. .^.....K6...A&i....v.b.......usBar.au3"..#include "Memory.au3"..#include "SendMessage.au3"..#include "ToolTipConstants.au3" ; for _GUICtrlEdit_ShowBalloonTip...E.......\|,..k.P~HY..O..\|..{.'.I......ilSL.+.h..G.f.b_u[....ude "WinAPIHObj.au3"..#include "WinAPISysInternals.au3"....; #INDEX# ============================================================...r.N.D...$1.d....,..[..\.]r.%L.s....N....8.0._r:..T...}oBE.w..Title .........: Edit..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with Ed..,.......tm.8H..Y.^.k..A.@o.8Q.n....S....DS-..&s....g./>_..]..rectangular control window typically used in a dialog box to permit the user to enter..; and edit text by typin..!.....`n.8]..1...[..\.]r.%L.s....N....8.0._r:..T...}oBE.@..=================================================================================....; #VARIABLES# ===========================...r.N.D...$1.d....,..[..\.]r.%L.s....N. |

### C:\Program Files (x86)\AutoIt3\Include\GuiHeader.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 44619 |
| Entropy (8bit): | 6.287935856263052 |
| Encrypted: | false |
| SSDEEP: | 768:5juLVqv2XLqF6yE/6chi1XmNenrDEVEnR9DhCXKOzMPxnBzF9dY7oxRaJh1W8:NE0XLcGR997lWU8 |
| MD5: | B43B6E42E24FEC281E1A57236D4CCF58 |
| SHA1: | 43BABB396C0C35D5905298CA1478B5633766FF3F |
| SHA-256: | B2A6CFFC858D97D8A1E151A28C3187A44C09FD6E97CD3A7E7B09DE6DE62AD782 |
| SHA-512: | 3615BD054C2C59C8BABEE312C06E5BFFDB9126AF9EBF06951B9963BF4090A828FD43650357026037E0EA049B62205D1B829401E5E93CB3C3C23D321206203617 |
| Malicious: | false |
| Preview: | .....E.}64.............&..S+>@.H._ ..DX..g.*...~\..L..}>..Qsy.au3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#i..}...].04....L.....D..q%..U&/A.+.f:.#yxU.[.\|.vXv^...]^.Ry..!#INDEX# ==================================================================================================================..A15.M.pwt...-..N.....t...j.P.d.Es...CBC.2.(.*.9.C..%g..7..]siption ...: Functions that assist with Header control management...; A header control is a window that is usual..1..H.964....a..N.....h.Y,zQ.s..<...EFN.`.&.$.c...\..1....uitle..; for each column, and it can be divided into parts...; Author(s) .....: Paul Campbell (PaulIA)..; ======.G,\...Bmdg...>...S.J..F;...wg..6..n..N..../.5.9.*.J...P.bN..<=============================================================....; #VARIABLES# =====================================================.G,\...Bmdg...>...S.J..F;...wg..6..n..N |

### C:\Program Files (x86)\AutoIt3\Include\GuiIPAddress.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13083 |
| Entropy (8bit): | 6.273108318235322 |
| Encrypted: | false |
| SSDEEP: | 192:14B2pAuYcVUj5/ZkUlvmHlr3luNgl/Pl1zw3ulffNnlFfxlg:yYpeyKJ6UlOHlrluNglHlRrlf1nlZxlg |
| MD5: | 575F1CF0E7B0FDCD60F74A2D62C782EC |
| SHA1: | 8E5720CD6BB4A325EB76A2BE34D7B1898A86753C |
| SHA-256: | E46EE2963BB7410F53C9F3065C479F8AB7348A5CEBDFFD7E58CD69E988880B40 |
| SHA-512: | 1AFBA925F14B9C8887633E2A0A73731E53E533908F3B2A7A7E78909DE5AAA7B22A56BB9883C2D1F83A470CA1DF7CA896F5B3F644216DA9312BBF89777481DE4E |
| Malicious: | false |

| | |
|---|---|
| Preview: | .C@.Ra.xCq6....8...B.xx..d....e...Kp.fG..C........R.,..I0.<.mory.au3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"...G.]x.y.>z...e.....x/..L..m......{r.......L!:.`.....Yt.QRWinAPISysInternals.au3"....; #INDEX# ================================================ =============================================.....). S#e.......R..0!..{....!..TV..;.........pBY..N.3..&+.0.toIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with IPAddress control management.. ...a.u.lp.......U..ln.......!...^A.a........../%.W..}...-.LM================================================ ==============================================================....; #VARIABLES# ==.....). S#e.......R..0!..{....<.......(........../%.W..}...-.LM=== =============================================..Global $__g_hIPLastWnd....; ================================================.....). S#e.... ...R..0!..{....<.......( |

### C:\Program Files (x86)\AutoIt3\Include\GuiImageList.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 31940 |
| Entropy (8bit): | 6.258468483588935 |
| Encrypted: | false |
| SSDEEP: | 768:kfC0IrAtlK3INENVcAdQBaMmJfb6LS5rrgBQu72:OgK8cBa1leBC |
| MD5: | 271CCFD9AC6A4CB33986D15AF9F472A3 |
| SHA1: | 544BCB123D743C36565B5B6438E1D03784F29976 |
| SHA-256: | 4FBD72B38118CF7710CBD640BFE2BABC2C05DADDBE3A31FB32016B6E2572DBCF |
| SHA-512: | B75A867D839C1223CF62D0844F98011BE4B79F72530D47D0F463122FB142E9BD5EB1E183FAA5848AF8D63A83056C5641D881BE1E7FBEA44EA04A50E9BA8F56FA |
| Malicious: | false |
| Preview: | ..yt..U7.$bJ.Z.#.........S-WFsm.....'......&{)d.d..v.=.e.<..+istConstants.au3"..#include "StructureConstants.au3"..#include "WinAPIConstants.au3"..#include "WinAPIConv.au3"..#include "WinAP\|7ee...3..h.%..7..........y,zyHi..Z..zT.)...g.V#.*..\|.Mde.2..Iau3"..#include "WinAPIRes.au3"....; #INDEX# ==================================== ================================================.O**...o..w<..m*..........-...<..Ty..i".W...*X.iH$..(.T@M.8...t..; AutoIt Version : 3.3.14.5..; Description ...: Functions that assist with ImageList control management...;                  t.7~..V7.#r[.9d.........,.Fg......:V.E...aVP&.o..h.1.I.>...f which can be referred to by its index. Image..;              lists are used to efficiently manage large sets of icons or b\.zv..r..&!F.1pL.......q%^.mG..T..,V.L...m.F#k...2.=..J}.G      in a single, wide bitmap in screen device format.  An image list can also include  a  monochrome  bitmap  that..;          .R77...r.%o[.9yZ.......tbOF!J.....$. |

### C:\Program Files (x86)\AutoIt3\Include\GuiListBox.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 44404 |
| Entropy (8bit): | 6.212966700441744 |
| Encrypted: | false |
| SSDEEP: | 768:N1A0A+tvmdet/XEvqPi3qSOh4MtSDhVtp3O+d5l3HLYnxq/Nszv3XFhkiVNDKA4S:Nz7vN/sjex |
| MD5: | CD11AA751FB7D3F35209CD2B62895BC6 |
| SHA1: | ED68509BB851CFCA3BC1DF9E291D9802EADACEB2 |
| SHA-256: | 66E74CA5A6F397991BCEA912E28DF4889F1C49B8F363BD9DB889AFBA28214D01 |
| SHA-512: | E769C698835852C2E7E4C510B7B64472CEAEF1F1CF135DC6BB8A7B2E1CEBA88E1A26AED3894F2BE3D2AC6E15E594A4FB5228F3C8D9CADD9DFB876C2E94A5A2BC |
| Malicious: | false |
| Preview: | ..h..b.1.>...+?..."g...@8..,]W.E1qlw.c.pK.k.6?z.'..>..t.L8...onstants.au3"..#include "SendMessage.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#include "WinAPIRes.au3"..#inc...n..Q.......o[O../j..ou.S.5v.e3KM..>&X.[.(k).v.Bf.....q...======================================================================== ==========================..; Title .........: ListBox.....~..O..../..H....o8...N/K.e>t.X"ecd.mH+V.H./vQ.,..(..2......iption ...: Functions that assist with ListBox control management...; Author(s) .....: Paul Campbell (PaulIA)..; ===============..6..;..c.`.......\|6..]'{.c#.A.x-?>.p[8E.[.(k).v.Bf.....q...================================== ==============....; #VARIABLES# ==================================================================..6..;..c.`.......\|6..]'{.c#.A.x-?>.p[8E.[.(k).v.BV.T.]-.._g_hLBLastWnd....; ==================================================================================================== =..6..;..c.`.......L...#U..._v(ef0?>.p |

### C:\Program Files (x86)\AutoIt3\Include\GuiListView.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 226127 |
| Entropy (8bit): | 6.616494873479137 |
| Encrypted: | false |
| SSDEEP: | 3072:a7Aw6OT0/ni5zPIFOMvobimds/Ut9HMA8ALBq0i:rwfT0qLHbimSUt9HMtV |
| MD5: | 1454617E0FC632C07ADBC21F592FBF34 |
| SHA1: | 79C26F93FCE1094BED93928E5216884F1B896C9F |
| SHA-256: | 865D385D576C591C709E6EEE2126D77CF18F398CBE2955A04B697CD7111C7174 |
| SHA-512: | 454C9ACA6F7A8771AC6CE10E041FA87F3F3010E8A22D572C91EF1B66979286C97266CAFB6CCE037EA0C36767021D280BA5A3F89949794577323CC081E33E517 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .."xZ............Ha.....X....).....&dS.....@...z..........(An.#include "ListViewConstants.au3"..#include "Memory.au3"..#include "SendMessage.au3"..#include "StructureCon stants.au3"..#includ.nNr..........`...........h.j.!...h...O..P.}..T...z......Z3*Gdi.au3"..#include "WinAPIMisc.au3"..#include "WinAPIRes.au3"....; #INDEX# =============== =====================================..q&...K.R.V...(..2...\.E..0.u..r...SM.\..^.M......Y#.....&^^==..; Title .........: ListView..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assi..Il_..V......5.Na........l.-.!...!UP.A..C.P......D>.....h.5iew control is a window that displays a collection of items; each item co nsists of an icon and a label...; List..)l............z.Hk........a.?.<...................r......v.M For example, additional information about..; each item can be dis played in columns to the right of the icon an. zT..X.e.K..z..\|...O.V..-.)..o...[.. |

### C:\Program Files (x86)\AutoIt3\Include\GuiMenu.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 62224 |
| Entropy (8bit): | 6.205803698944779 |
| Encrypted: | false |
| SSDEEP: | 768:ypujYxK32qF7xwU+hzgH4LPeaTpqFJNpn2NHanaO2:+ujYxMpca9al |
| MD5: | E932AB23577DF2FBAFED0029B94E9C23 |
| SHA1: | 6EE5D4BECE9D5D4B5B215F432B896B1389A11E81 |
| SHA-256: | F21DFB6DC94DF948B8E3DCD9B0C47498291038614A8F97561109640A2ED0F063 |
| SHA-512: | C47DC6EDDB1B5814CE33DADB52F294A6D6FFDADB64E77BA958929FFEE328775CF3B984D14965211B985F24C4F13782C5ECFFC958C9279AD25238778B01723D<br>F |
| Malicious: | false |
| Preview: | ...{...s.&.....r..........u.pd.T8....j0.......4.&........U;l.q.reConstants.au3"..#include "WinAPIConv.au3"..#include "WinAPIMisc.au3"..#include "WinAPISysInternals.au3"....; #INDEX# =========...%...+.t..>.B,..._........#,c.k....#~....../*Ju.KS....t$.8.===============================================..; Title .........: Menu..; AutoIt Version : 3.3.14.5..; Language ......: English...8...u. ...l._?...B.....W.m1*S7....m*S..Z..z7:-..V...N%9.d.agement...; A menu is a list of items that specify options or groups of options (a submenu) for an application...q...x.i...8._1...B......>1~V3...j&M.]..a7.h......N;9.d.ses the application to carry out a command...; Author(s) .....: Paul Campbell (PaulI A)..; =====================================...%...+.t..>.B,..._........#,c.k....#~....../*Ju.KS....t$.8.==========================....; #CONSTANTS# == =================================================================================...%...+.t..>.B,..._........#.T\|:..>. |

### C:\Program Files (x86)\AutoIt3\Include\GuiMonthCal.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 45721 |
| Entropy (8bit): | 6.341924733767278 |
| Encrypted: | false |
| SSDEEP: | 768:qyoVbjeBrouqLRQiHUWwovKH0G9Ps22MPLzrE6bGvEKfjgEPFZZcAmvdR:qyyawrHSd9PxFPLzrxbGDgHR |
| MD5: | 1F090A1379DBF989406842EDD6265678 |
| SHA1: | 3067EFB50D562FED0024B3F84E380F0DE0E5C2BB |
| SHA-256: | D68379A5FE9953EADB5254F09903C7FDA1409823F7C6B249C584EA8B79A0E1A5 |
| SHA-512: | 0FBEF2C59AFA4CC8779930631990768F75D5931FFF202EF9088663E5D47779E46D44D1C4826AF2F497E6BA9495DA3C0AAE43F94D3E2FD26076CAFCC22B8313F |
| Malicious: | false |
| Preview: | L...... ...#.^K.T6.j..u......5PL.m@`2..j..s.e0...b4...g......ory.au3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..T......)..`..(..E.I..c..^..{...WB.[Kka..m....Cz....n(...p.......; #INDEX# ========================================================== ==========================================================R....e..,.so.p;.*.....f......UD.JN\|L..$..).Yw....x3..F9.....4.5..; Language ......: English..; Description ...: Functions that assist with MonthCalendar control management...; O....(..(.0 .;{.e..c._.....IM.CJ`5..e..<.um....g3..Fv.....nterface. This provides the user with a very..; intuitive and recognizable method of entering or selecti......1..B`.;$.=z.p..I..G..V...OH.K\.5..$..-.\|j....d4..]#..... with the means to obtain and set the date information in the control using existing data types...; Author(s) .....: P.......5..,.{..+y.E. ..Y..0...M..INh3. |

### C:\Program Files (x86)\AutoIt3\Include\GuiReBar.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 70114 |
| Entropy (8bit): | 6.284618502805753 |
| Encrypted: | false |
| SSDEEP: | 768:Zg2M0y93gvnGzJ5iYMIboyUMxT3dAgOCUKD45ueH/sWf6AqfUKQNsbPm/CqEaH7J:ZFw15i3mC6UK1brwDIuWPWKHO |
| MD5: | 17940BAAA18CF61CD4E86D413CFC418A |
| SHA1: | A85F3EAE168AD4D385E5B2091B5E1A1FA97354D2 |
| SHA-256: | D9179D3AC5742E16AA0334DBBF298B59D65C958CBC96C9BF2472FFF73600B418 |
| SHA-512: | 01FC89CE80350657CCBD9472B46BF42575BE031418E846954D6E398BFBC214D19ADB064A3E377675E62FBAFD251A2878F92737162F35ACF334D1DB0ACC2DEE<br>3 |
| Malicious: | false |

| | |
|---|---|
| Preview: | ........nt=G..Q......y......;..........y*F..H....'~...[..2.'.au3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConstants.au3".t[....d:\|uqs.J....\|..LmV.'...^..Kd..J.`..!...(m..CI..~.^..; #INDEX# ============================================================================================================.CE.t...uv;.63r4......=... .x.rR..T..<[..i/\..R...h=.SX%..\|.5nguage ......: English..; Description ...: Functions that assist with Rebar control management...;                 Rebar contro..X......!y1Ll\|5t.....o...(...>...L..<L..{6C......(,...A../.7hild windows,..;                 which are often other controls, to a rebar control band. Rebar controls contain one or more ba....s...!:~.8=\|:....=...%G..*....U...I..r'E.....)a...I..3.tof a gripper bar, a bitmap, a text label, and a child window...;                 However, bands cannot contain more than one ch.......v4S(#=.o.....4..oI[.i5......s |

### C:\Program Files (x86)\AutoIt3\Include\GuiRichEdit.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 209491 |
| Entropy (8bit): | 6.583972869596515 |
| Encrypted: | false |
| SSDEEP: | 3072:4IhehBQsmsAcj+GUeQ0Mly1BDP12wLNLyVTHiUdq:lhefhtjnlQ0MQBDd2kLyVeUdq |
| MD5: | 106160B224C55793D2B3A5A9C804CF7F |
| SHA1: | 8665DB16701C6123F101CF475B831095783A1800 |
| SHA-256: | F774EC0A54E6DFCB940F1BE6C5124D3A008440BD4A22D9B1F8B5D3FD2E5606DB |
| SHA-512: | 7C3226E94B556A585F9248BB6AF78B2C4AC7BF8FCDE1D1434933C640363BCF46253EC715AF66E6CF35A040FCF5FFD841F4831AAC450A7A36D48065EDCAE3D1D |
| Malicious: | false |
| Preview: | .+u.9M..{`....tD..Y7..7.).....k.%.g..6=...8.]y1.Uk..?..z.yo3.ts.au3"..#include "FileConstants.au3"..#include "RichEditConstants.au3"..#include "SendMessage.au3"..#include "StructureConstantFlz.f...uf.....,..e.......\...z..f....-m...Pq.i\|*.`.w.5..X..(.X.include "WinAPIHobj.au3"..#include "WinAPISysInternals.au3"....; #INDEX# ==============================================================..&.h...k2...OCt...d....q.....&..y.>..~3...l..(y..v..f.....7&o...; Title .........: Rich Edit..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Programmer-friendly g+x.u}.."/.....&..:b..7.$.B..;..j.-...o...G>.J9d.B#U.w..K.Ju6., KIP, c.haslam..; OLE stuff .....: example from http://www.powerbasic.com/support/pbforums/showpost.php?p=294112&postcount=7..;..&.h...k2...OCt...d....q.....&..y.>..~3...l..(y..v..f.....7&o.===================================================================....; #VARIABLES# ===============================================..&.h...k2...OCt...d....q.....&..y.>..~3 |

### C:\Program Files (x86)\AutoIt3\Include\GuiScrollBars.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 25030 |
| Entropy (8bit): | 6.334041711127321 |
| Encrypted: | false |
| SSDEEP: | 768:wBh9Z94RnWo3n3zqAdJExESrMFe/2dOdQ:ozuntqmWZQ |
| MD5: | 414E752E45BC9FDCE4A485C91E061778 |
| SHA1: | 1A0B20ACC4ADBFFF6EA307FB5B6DD8D53F67C532 |
| SHA-256: | 290A812A696E2B2212A296BCAC988CA685528B657C5D8D3FA3AE418C20CB6FAB |
| SHA-512: | 037135207D4D58D129188D5E1A9904F75A06A0F88BDA49AFF738E27ACFB2E5018E002DDBD0F150B645863ADFB2DD85D1AF2E87F01A589D6EE13D28F8091E0192 |
| Malicious: | false |
| Preview: | .t...s..Qq.Y*.r<.e.J...jH..;..*0Q]...8.N...P$qU.5.5..i...EU--.NtructureConstants.au3"....; #INDEX# ==============================================================================================. ..I;..A#..r.E..{....3...et.e.TK....yQ.....ye..e.W..B..m:.hL.ioIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with ScrollBar management...;      .=..T&..\>.....R.).H...\|.....6(N.....w.U...@w,\.`....t...^.)..rw button at each end and a scroll box (sometimes called a thumb)..;                 between the arrow buttons. A scroll bar rep.x...r...v.. ..C.*.....iY.....25YK.@..w.....Ew0V.c.L..nT.@GX&i.j's client..;                 area, the scroll box represents the portion of the object that is visible in the client area. The .r...o..\q..;..<.}........H^.e\|...@.%.Q...K/.W.g._.. ...^T>h.=the user scrolls a data object to display a different portion of it. The system also adjusts..;                 the size of a s.o...&...9..<..^.*.F..}B.....e5I....4. |

### C:\Program Files (x86)\AutoIt3\Include\GuiSlider.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 27088 |
| Entropy (8bit): | 5.980153509948303 |
| Encrypted: | false |
| SSDEEP: | 768:7hBUOcgS14HJmRbEvpHP/NcsnrhOnbL6JzkeDHqkabpsn4MMy5SWQ:FOmSAf4yIN |
| MD5: | 40CBF059B7C69560F571C943D3F1D007 |
| SHA1: | 6279F919721238452A066951AB14A3C3F0590F07 |
| SHA-256: | F79E19F8B31EE3914CEA5F6655D168A85791F6959DBE847376AF97BCD42D2EC8 |
| SHA-512: | 7593F2D9A9757154DC713EFBA6C9A69770D5E33B5725B9130F2164E29878A4FA82130974FE0E466FCB4A4AB439367122AD2FFA103FF23F7C1442D61B3CDEEC3 |
| Malicious: | false |

Copyright Joe Security LLC 2023

| | |
|---|---|
| Preview: | .2O..EL.:.....@p.dd"..}h1.!.QO4..gn!...S.d.0cK.dC..N.C.....&..stants.au3"..#include "StructureConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#include "WinAPISysIntern.7R..E........4.HRb.$0,.OV..D.X)2{....].T..7..5.I.S.-.....X.U=================================================================..; Title .........: Slider..; AutoIt Version : 3.3.j..Z=".7....*..#$o.771...SB..h.4f......zeK.&.Z.N.e.......Hthat assist with Slider Control "Trackbar" management...; Author(s) .....: Gary Frost (gafrost)..; ==============================.f..R...*....pG.07\|.$0,.OV..D.X)2{....].T..7..5.I.S.-.....X.U=================================....; #VARIABLES# ==============================================================================.f..R...*....pG.07\|.$0,.OV..D.X)2{....'...rf..Wi....\.......b..; ===============================================================================================================================.f..e=".7.......4.^)a.$0,.OV..D.X)2{... |

### C:\Program Files (x86)\AutoIt3\Include\GuiStatusBar.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 31661 |
| Entropy (8bit): | 6.383636533801762 |
| Encrypted: | false |
| SSDEEP: | 768:J+qCFfYHyHCI8kuB4xtKEwNJVL38IrRxo8+p4V9P+KqwMY1nAj:JpCFfWyHkhP9hdV62lS |
| MD5: | 20DC3787BC1CDBF06C6DDF5A5714F5C8 |
| SHA1: | 1F2C044FC3FA2704A97A2DACDD378FAD549723F2 |
| SHA-256: | 583990202C8946172769CA1452D56A802CFE81494EBDED199000ECE272EA2D94 |
| SHA-512: | 901B37134FD5F80365F4A234BCBD3EDCBD835494D8882B4877CFF9FA0BFFC9D1D843F3097408994E2AA17BF619C09DBC8BB130787A265B6D72B764F6B22E267D |
| Malicious: | false |
| Preview: | .......\|.(>..*.....W.:.M..q..Jw.a.+.t..o..._i{.g..........8.3"..#include "StatusBarConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#include "WinAPISysInternals.au3"..jn.b.'W......#....k.........8.rTc.k..;.Q..0#...C..aH.....+..=====================================================================..; Title ........: StatusBar..; AutoIt Version : 3.3.14.5..\D.#..l. 5...0....8.E...1...A.<.,Y&W..h.B..7>..Z...3....b..ssist with StatusBar control management...;                A status bar is a horizontal window at the bottom of a parent windo.G..b..p./p.....n].Z.".F..]..Al.?.?I[).&.L..->..^..\|U.......s kinds of status information.  The status bar can be divided into parts to display more than one type..;                 of in....#..v.JZ.f..v^...........ud.#I.Q;S..j.L.zlk..uW..gU.....+..=================================================================================================================....; #VA..%...=:.zm....#....k.........8.rTc.k.. |

### C:\Program Files (x86)\AutoIt3\Include\GuiTab.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 41781 |
| Entropy (8bit): | 6.35117181723044 |
| Encrypted: | false |
| SSDEEP: | 768:JLEzsjJ6LL0I5YWi9tTPErk+qjpGrNAnItETqiE7hkTdTN/jBuT3aLRE6I4t85Gy:Jgzsd6LLj5YWi9tTPEY1UGIteqimh+de |
| MD5: | 47D762E07EE2C43EE4AFF039A494367F |
| SHA1: | 9666C1675008CBC441657A7622C5F09C947C0E49 |
| SHA-256: | 99629EECEF842760AD3319D24C294F6489913A62FD69572566A3C99300A98F9B |
| SHA-512: | E642ED1573EB3A03B7CA0E429F686E451E5B6B4B7005A5453BD5BF5CA44A65F8BE00F1040E79C4F6FAE047EEA35D2ED98752D2B875A384458D89DC738EFDAE4F |
| Malicious: | false |
| Preview: | .SD...I.Q.Bq....E.3E.b..tt@..:.....y.....Bw....;&_c.\|..........3"..#include "TabConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConv.au3"..#include "WinAPIHObj.au3"..#include "Win.jc...d...^\|...!.[i....@*tA........1......$...G.&91;.%..T^.....L=========================================================================================..; Title .........: Tab_Control..; Aut.s^..._...B2[..!\|.k..;.@*t...0..."......9.....hl...8.........n ...: Functions that assist with Tab control management...;           A tab control is analogous to the dividers in a no._H.......Xz..n-K6X.g.jptB..;....n.....9..Z.hmba.8..I.....Q                control, an application can define multiple pages for the same area of a  window  or  dialog  box.  Each  page.....I..\..2A../o.z..a.9x'...8.....i...H.m...Z.}$eh.w.......... a group of controls that the application displays when  the user..;                  selects the corresponding tab...; Author(....G..F.\|s...L.C*I.b.j9..........m.... |

### C:\Program Files (x86)\AutoIt3\Include\GuiToolTip.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 48851 |
| Entropy (8bit): | 6.408344202657753 |
| Encrypted: | false |
| SSDEEP: | 768:zthHTkZSUp7iY1nQ1r5PO81MnOn+f5x1TtBXTnb8ET:ztlq6P+VOOBbn |
| MD5: | 996C9AF348A8C214C741834C991D9824 |
| SHA1: | FE449A6F095E4ADBCFBD797192006F699D4249F4 |
| SHA-256: | 6935CAE75B400F16FE7768BBC5A36FD762EE1C3E1F4B9B286971599A22D4797D |
| SHA-512: | E4BB85BD2560B222A91F993BA11868FC59D3F34910029D9D7899D301F9AB01227C09DAE352F394C02DEAA4DEA0F87634E4142345B38FCCF4820C51F8B9B6C7BC |
| Malicious: | false |

|  |  |
|---|---|
| Preview: | .U.-..{W..h.5i~.4.Q.2..]-K\|[..:.*O.../........YH.J."...#....3"..#include "StructureConstants.au3"..#include "ToolTipConstants.au3"..#include "WinAPIConv.au3"..#include "WinAPISysInternals..I.l...m._.C.z<W.`T.Uz...B].,...f.$P...{.A.E[...7....zX..y...===================================================================================..; Title .........: ToolTip..; AutoIt Version : 3.3.14...D...%[..}.V...sG.Rg.....G~Z...3.mM../........^B.B....+....l management...; ToolTip controls are pop-up windows that display text. The text usually describes a tool, whi.T.'...?L......y.fI.Hg..._@.1...{.9...).P......k^.O.$... ....dow or control, or an application-defined rectangular area within a window's client..; area...; Author(s) ......../....7U..h.SD\.<.^!....D@.,...f.$P...{.A.E[...7....zX..y...============================================ ================================================....; #VARIABLES# ===================...s...k.A.0..YI.`T.Uz...B].,...f.$P.. |

### C:\Program Files (x86)\AutoIt3\Include\GuiToolbar.au3

|  |  |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 89730 |
| Entropy (8bit): | 6.185814103367309 |
| Encrypted: | false |
| SSDEEP: | 1536:OZHAt5P9cu3XW0btQVZpwgU0guiMOe3Ou8qjo:OY520u6RMx1c |
| MD5: | 0E8BCE372A4F59618259AAB50A9B6F29 |
| SHA1: | A5B28C6D503A847B5BF481B5D57ABF15F4D7C146 |
| SHA-256: | 2937C4E07EBE13FFC4FE30F8BD512E55A6953F23F9D7CF55D34154FFD29B1BC2 |
| SHA-512: | 4A305B39E327E163D0B49AC0B1523FEA698C9149AFFAEC4CDA9FDC80AD8ABA16FD079610FDB0DC08E6B05319F544779CE2AE9A654A22EDC381A999295F06D7E |
| Malicious: | false |
| Preview: | .}..%JX.I.H]..J...O........-IS....,.P3G........3.{b..T./..:.Cth3"..#include "StructureConstants.au3"..#include "ToolbarConstants.au3"..#include "UDFGlobalID.au3"..#include "WinAPIConstants.au.6.jVR...B[.....m0h.....X..j)6....5].[m....&...v..f..;FV..3..`ye "WinAPISysInternals.au3"....; #INDEX# ====================================== ===================================================.).t..SY.....}..].P.......u...`..A.R(...I...=..'0.v'>..PsV5\utoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with Toolbar control management.../.i..ND.....`...@.,....U..:.U.J..:G.J?.......d.\o..9(3..<..f=one or more buttons. Each button, when clicked by a user, sends a..; command message to the parent window. Ty.}..%SEBD.N[.."..X.O........h.H....8ZR.........w..s..9"(...YM\|s the..; application's menu, providing an additional and more direct way for the user to access an appli.u..&Q..i.....`...@.M.......hGS....=[\3G |

### C:\Program Files (x86)\AutoIt3\Include\GuiTreeView.au3

|  |  |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 125619 |
| Entropy (8bit): | 6.415772617166331 |
| Encrypted: | false |
| SSDEEP: | 1536:frTsU7xHHRUEnkpkrGdoghSLwAEqBfg1Buljf8qo3cfrtch93un:xnUGKhd+Dfg7uljf833uZcCn |
| MD5: | 69EC7FAE1A7883B3DC8D9E8BBA2B0DB1 |
| SHA1: | FC207AB5227B26CA5EB2C113E949A7BCDA0B2E52 |
| SHA-256: | CACD1FCFB9EF1C8D178CC27F32D43EB1B6F44C231D66939B50B5E74A4E918902 |
| SHA-512: | D6D56474BC9BBB694BE140EC09CCA9D1A145EA1D94E4DA3D4E2DB0C2694BB9921634D7994AF5C049DA39BB2C77DDF4A44465DC967C88EC5FE95C75F8C0DAC394 |
| Malicious: | false |
| Preview: | z.f.!e.).H.55).(&..a.P.qm..$.~.+..!..Y.\|%/>...[..s...6.>n_...%u3"..#include "SendMessage.au3"..#include "StructureConstants.au3"..#include "TreeViewConstants.au3"..#include "UDFGlobalID.au3"T.+.#s.9.B.t.M.d\|.`.J.t}..n.4.(..1=....t>]L...[..jO...7/5`\...d"WinAPIRes.au3"..#include "WinAPISysInternals.au3"....; #INDEX# ============= ==================================================d.5_p-.q...km......2...(5..^.*.{..yd.... m!!....W"A....L`#d...! .........: TreeView..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with Tre<.a.:0.#.S.9<..DB.j.Y.a&..X.7.f..dy....=p<<.....z....cf8l^...( is a window that displays a hierarchical list of items, such as the headings in a document,..; the entries in 8.(.#t.4...$pP.@..c.O.tf....e.%..60.Y..sp}<...Y.JZ....}2>n....7ists of a label and an optional..; bitmapped image, and each item can have a list of subitems associated with i-.(B.i./.N.=9J..M..f.Y.9(....7.5..IS.... |

### C:\Program Files (x86)\AutoIt3\Include\HeaderConstants.au3

|  |  |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7327 |
| Entropy (8bit): | 6.717429900783855 |
| Encrypted: | false |
| SSDEEP: | 192:AomZEKwwggKfPSaUo7ElAJgJiM08xcgCoOE9ZxY+nJK10:AlZ8wgHfPVR7EeJgJiM0q6taZC+K10 |
| MD5: | 447B12FF73A96F42F8821573CEFAA9EA |
| SHA1: | 5E7A574A37CA8EF435F394EBF846FF0882D5F912 |
| SHA-256: | 64FD0B32A64209B32AFA9ACEEDF22BDE522B0F97ED2D38CFDB51080B2ED81DE1 |
| SHA-512: | C09FE3F6D54B2B7E25717102EAE7FF5ECF08CD0B241BA20D06C39BD38E06E2FA047B5EA86BC08AC2F1D3D5723E32DC3FA4C2CAFFA3002F27EC858053293CD50D |
| Malicious: | false |

Copyright Joe Security LLC 2023

| | |
|---|---|
| Preview: | .V..,%w$.V. 43.J.+.@...wI.[..L*.0.q...2.~\P.\|I=.*!.Bb..~En..D.=======================================================================================..; Title .........: Header_Constants..; AutoI..?.2#z....cb.&i.$.V..]T.....r.#.b..5.....(.h..'.;:B..*.'.......: Constants for Header functions...; Author(s) .....: Valik, Gary Frost..; = ==================================================..T.}m.\|...~l.(z.-.^...,.F..L*.0.q...2.~\P.\|I=.*!.Bb..~En..D.=============....; #CONSTANTS# ========= ==================================================================================..T.}m.\|...~l.(z.-.i...PpY[...c.)..v..J..AP.q.0.',.Oo....<.... Const $HDF_RIGHT = 0x00000001..Global Const $HDF_CENTER = 0x00000002..Global Const $HDF_JUSTIFYMASK = 0x00000003....Global Const..!...Q..t...q[..Y.+.. ..!MK..@'.=.Fw..m./A../.t.3T.9.s...9...Y.x00002000..Global Const $HDF_STRING = 0x00004000..Global Const $HDF_OWNERDRAW = 0x00008000..Global Const $HDF_DISPLAYMASK = 0x00../.p`.K.3./>\t+.S.....Yq=..=ExL..~..2 |

### C:\Program Files (x86)\AutoIt3\Include\IE.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Public Key |
| Category: | dropped |
| Size (bytes): | 153859 |
| Entropy (8bit): | 6.76034110363429 |
| Encrypted: | false |
| SSDEEP: | 3072:M5mluq5VkVWJpHUOV1C6+kFOu1LpgYckwaKum3tIOI6SP3im9EjSnjQiAWYPTrLx:xPRX0OVykY/kQhCDPI |
| MD5: | D4EAB9CA24B8BBC6049907681B468D2C |
| SHA1: | A0A19E59C00679D01D6C97033FB69E0C518E8E20 |
| SHA-256: | 2140A4115547543C4EC1D479539E134C36A91E9739F76072B30DD50780DCF109 |
| SHA-512: | 0A8F4BD74E630A798032D44D37990DEA8DCB3E4703ED1DB332C9ED8CC226BE024D8E7C5CC9AB61FB6260DA057DED757E2B75A262827A80B729FAC772E76AE EF5 |
| Malicious: | false |
| Preview: | ....QU0..^.a.....;9....X.+d...c.g...*.j........OC(.*..B...onstants.au3"..#include "WinAPIError.au3"....; #INDEX# ================================================ ==========================.....h....9....0oj....E1W,H.}*..4^.y..yV........XC8Va.s*Q...: Internet Explorer Automation UDF Library for AutoIt3..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...e.6..\.g...-=1.....e....&x..j...0.#G...w.[..BH}. .}v...ng from and manipulating Internet Explorer...; Author(s) .....: DaleHohm, big_daddy, jpm..; Dll ...........: user32.dll, ole32.d.....HT4....h....-oj....E1W,H.}*..4^.y..yV...>.....`Kr.`9B..============================================================= ===================....#Region Header..#cs...Title:   Internet Exp.....p ..].p....X........~.1..27.}...w..M-...m.U.....3a.(7r...escription: A collection of functions for creating, attaching to, reading from and manipulating Internet Explorer...Author:   Da....I<_.._.m...7r=......bg.\|.%e.f..d |

### C:\Program Files (x86)\AutoIt3\Include\IPAddressConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1688 |
| Entropy (8bit): | 7.46406613604768 |
| Encrypted: | false |
| SSDEEP: | 48:kkD6OD65lPl7ZD6OD6eD6OD6BDOx9ZtC8nBD629dA:kHxltZ4F |
| MD5: | 1532810052C8AB99B5045EE91B69CEC0 |
| SHA1: | B39B10E4CF6DAEB70054E9CFE5CFEB27D340720F |
| SHA-256: | 912E9D0BFF3A9FF344FA351C5BE2DF7525B3920E9808F98F2E82EEA15A63A1F6 |
| SHA-512: | 2CD2BA9DEC9A374619407BAE6CA03FEA296C5F2B17E6A53A3DE7DEDE54C8C997527002A0AFCE60C51D62878EFA43F387047325E6E9630B3B57F4E7E42B0D1F 30 |
| Malicious: | false |
| Preview: | Q..C.i.E.T....F.G 1b..vmi.$..o(.B..R....9.D.=..=..c..k...(\|..O.D..!.....O. q$p&,\|.....w.$..o(.B..R....9.D.=..=..c..k...(\|..O.D..!.....O. q$p&.K...ZA&.9..\|;.Q..U.w..`...s.C...*.."A/..a.]..0T. J.R.R...'l*c(?p..>?q.U...'t....A....>.<.g..s..e.3AA.\|1.A..Y..2...T...\|"m>;w....ct..k...rs......P....B.A.h...-..x...;{.~...K.<.A.B.4.r?ma;?o....w.$..o(.B..R....9.D.=..=..c..k...(\|..O.D..!.....O. q$p&,\|.....w.$..o(.B..R....9.D.=..=..c..k...(\|..O.D..!.....O. q$p&,\|....8@.....Z.,..!.m..9.D.=..=..c..k...(\|..O.D..!.....O. q$p&,\|.....w.$..o(.B..R....9.D.=..=..c..k...(\|..O.D..!.....O. q$p&,\|.... .w.$...y....O.Q..p.]._.A.......}l.A..\|-.4..O.r...B.)\|)@.V-.._...w..v\.2..#....@.+.S..=......sf.G..{1.7s.].t.l.-.N.Km01p...>?..v...rV....O.w..[.<.A.R...~..~.}.\..l6.<s._.n.o.<.B.T.NB.....z.0. .>z....,.P..$.0.M.E.......a..5i.w-.)a.X.e.h.=.N.X.ON...`p..2..`<.u...._..G...t..I.......sl.Pa..Z.&..L.d.i.!.^.W.OP...~j..\...r$.L..e.R..e.Y.o..t.......wv.Z..{R.Y..C.i.z.6.X.J.T_...gj..F....5._..[.3 |

### C:\Program Files (x86)\AutoIt3\Include\ImageListConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2059 |
| Entropy (8bit): | 7.617977068402092 |
| Encrypted: | false |
| SSDEEP: | 48:TNlv7amYa3tlNlQ+NlRPTYfUq+6uS73WFD3KYhxtJlNl+w8RI3mwy:xcmY0fTT+jSD3bfJYI3m3 |
| MD5: | EC425E7C1C4097319295BAEAB4E162D3 |
| SHA1: | 97FCDB66ACDC490F5C6BD0BC5028C6A678AAAB7D |
| SHA-256: | 35805AB022C37DDB16EAA7B466B300F1910AFED041ADECD9BB30787F8E77A01A |
| SHA-512: | C299320BF97214F7CBA5DAAD6FC76398028DCA4CEF02A6A24C6812E3EDF9C1096A7E1312873A6B11682E455E5C1E4CF87C299B1538147EE5586B290DC918B17 1 |
| Malicious: | false |

| | |
|---|---|
| Preview: | ............8..}.~Z.^.8.DDA...?n..&.8.p)zl...C...`.E.<..j....!.Y...@......`..)r&.&.DDA...?n..&.8.p)zl...C...`.E.<..j....!.Y...@......P..4.r.w.YWR...,}..;`h.*q.8..\|=WI.)...r...w.....h.............s..:z...5....Cgs..5.+.w4.?..J.P*.f.<.r..@'....2.^.......A..;.E4.v.\|.5.....Ql0..tGv.@.\|q..W.WU...X./..m....<......w......`..)r&.&.DDA...?n..&.8.p)zl...C...`.E.<..j....!.Y...@......`..)r&.&.DDA...?n..&.8.p)zl...C...`.E.<..j....!.Y...@...?..~.xZ.O.U.*Z\...?n..&.8.p)zl...C...`.E.<..j....!.Y...@......`..)r&.&.DDA...?n..&.8.p)zl...C...`.E.<..j....!.Y...@.....1W.[{-z.;......mN...ZzN.p4w)...N...l.r.m..H;....h.-...>......m..$.+.+.Itv..Fc?..tGv.m0....`1th...:.<.Qg....Z..n.......Z.O)..].X.X.56....2+..+.5.} J[..L.YK.....u.`......S..D..........e.=S#t.z.Y:....&...DjJ..Fvg...N@..m.H.0.#......<......Y...v.p... o&.+.IIL....:^..wFg.!4.>..W^.n...;.M...e....,.T...M...Z.]1.t{!h.;.05?..hG...;.%.5$wa...N.*.....`..j8.....U..;.../.....Dm..$}+.+.s>...H"...h] |

### C:\Program Files (x86)\AutoIt3\Include\Inet.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 15435 |
| Entropy (8bit): | 6.665781778855703 |
| Encrypted: | false |
| SSDEEP: | 384:J8G90uumGhH0POUwWmlrPK/Nech66rqDDFzGb72wZZ:f9KmGhHy5mlrC/Nh66vb6w3 |
| MD5: | 2FDBA91BE3B2A9E463E085A88060BDA2 |
| SHA1: | A07446E9ABDC2460A42EE60823CF51F50B47C263 |
| SHA-256: | E5AB898BC734F3F2463D24C480863425BEC43E7EB20B7C97D096014C0E4DFE5A |
| SHA-512: | 7F91EADB205929D36DAB48EF768184CB1F7217D2BB67DD17E88C020CA5132FB738D34CD89888CD364DCA7DC64483E9686B3ED5A90C3E370FD39D396D921C1 44 |
| Malicious: | false |
| Preview: | ...........8...;..0.Q.f..UL...B.........;.5.....pi.......AiG3"..#include "StringConstants.au3"..#include "WinAPIInternals.au3"....; #INDEX# =================================================..@....D._l`,.....c...?.J5.........B..b.(.r....;..#..TR5.=======..; Title .........: Edit Constants..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Function...........)1..EW...l.p...&..b....V...q.;.o...A....d....j[, Jarvis Stubblefield, Wes Wolfe-Wolvereness, Wouter, Walkabout, Florian Fida, guinness..; Dll ..........: wininet.dll, ws2_32.......D._l`,.....c...?.J5.........B..b.(.r....;..#..TR5.=====================================================================....; #CURRENT# ==========================================..@....D._l`,.....c...?.J5.........B..b.(.r....;..#..TR5.===========..; _GetIP..; _INetExplorerCapable..; _INetGetSource..; _INetMail..; _INetSmtpMail..; _TCPIpToName..; ===============..@....D._l`,.....c...?.J5......... |

### C:\Program Files (x86)\AutoIt3\Include\InetConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1610 |
| Entropy (8bit): | 7.4490271488340145 |
| Encrypted: | false |
| SSDEEP: | 24:wthZKRUBX1Bx2D7sG1bL1SN2B5HZDzWdQlcGWK9bVrXVzQN:wth0OYHrpTHNWdYcZK1QN |
| MD5: | 2FB1824D646FD9684191A65AD45BE708 |
| SHA1: | 4974BC3D6433E111B4E47C6F47CACC07AE5FF77A |
| SHA-256: | 7C5CFB4F04EB8649F1ED059C0ECD0061874309F9079161D3527BD2F352B07F20 |
| SHA-512: | 8ACDA75AFBAFEF296BC4AB6FD862C1482CC56F4C46D1A6C5350F8196A3240813246781A117CC9003DD007E38E7F92536517CE954762593729118CC97FE5543B |
| Malicious: | false |
| Preview: | 8...!f...\|.Q......e.y..d.J.y.&a..73}.#..#.).......\|_..h.d.x..&.K.p.[.....L..........y.J.y.&a..73}.#..#.).......\|_..h.d.x..&.K.p.[.....L........U.[!.Y.j.5r..$4`.p.A.{.I.Q...Lh....-.._.M...$\|...3..B......].P1...d.5r..$4`.p.w.\|.0....."..!.6.e..5.V."}..}.AQ........H.I.R ...d.u\|.~a..>..>.w.S.D..$...&.7.eb.~.V.8}..\|.A_.......D....d.Y.j.!\|..c`..m....4.......\|_..h.d.x..&.K.p.[.....L..........y.J.y.&a..73}.#..#.).......\|_..h.d.x..&.K.p.[.....L..........y.J.y.&a..73}.#..#...7....,.....f..&.K.p.[.....L..........y.J.y.&a..73}.#..#.).......\|_..h.d.x..&.K.p.[.....L..........y.J.y.&a..73}.#..#.)......-..9...+X.;.?..G9..P.~2.......&.{.X&.....u/...G..J.Q.W.h.\|...a_..X...*I.w.5.#`...Z.w%......x....v.}.(.y=..Ia..j..W.Q.e.c....0......e../.\|.!\|..3.].........t.u.v..#...H..*3`....r.v.V.s...5B.......d.X.4..R5.....G.......J...X*...`.U..NA..R.Z.U.n.....K%.7.5..D.h.V..]#.W.e?......l.s.y..J.u..Q..fa".r..q.g...y....&.......y.Z.V.m#k....P..........r.c..8...T..CT.. |

### C:\Program Files (x86)\AutoIt3\Include\ListBoxConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5338 |
| Entropy (8bit): | 6.7287943615489265 |
| Encrypted: | false |
| SSDEEP: | 96:+ZUGTJt/Z0xvOXAqH4mhslGRWPrel79phF9nJ:+ZBLZ0BZqHxGRIexRJ |
| MD5: | 1048C15A123B98ACE6E9D8637CB132C2 |
| SHA1: | A8616A498A53C43A33A2DBBA6CFA618A9FD42B1C |
| SHA-256: | BEF55B9AC640A7665023A1F2AF7FDDBD3AB2011DD0048F66E41D637E60971AB9 |
| SHA-512: | 58902D471C9CF2654FFE7D43EBEF1F87901BB2FB126C6BC40DCB6A14B26921DDB6BB4456C1F19A90C49306B0B46CCCDCB8B7FF13A3E76251D0E69B6B6D9DA E8A |
| Malicious: | false |

| | |
|---|---|
| Preview: | ..lD*.;.."^R...9./.H...LK.>....Zc.......Y..^....L..m^.A*S..X..====================================================================================..; Title .........: ListBox_Constants..; Auto~."q#.,..#.......%.E..23....].;.......D.R.R_HH\|0.p'..t...... ...: <a href="../appendix/GUIStyles.htm#List">GUI control ListBox styles</a> and much more constants...; Author(s) .....: Valik..EF4...."CE.......P...4..#....Zc.......Y..^....L..m^.A*S..X..=====================================================================================....; #CONSTANTS# ==========================..?.{.bU.p.......).V...4..#....Zc.......Y..^....L..m^.A*S..X..========================..; Styles..Global Const $LBS_NOTIFY = 0x00000001 ; Notifies whenever the user clicks or double clicks V.qS4.1..Gw]...X.W.....-_.M..n3~......T..Q ...s.H.#C..e....... the list box alphabetically..Global Const $LBS_NOREDRAW = 0x00000004 ; Specifies that the appearance is not updated when changeD.cU#.2..(=;...V.x. (..}3.R..q2......m |

### C:\Program Files (x86)\AutoIt3\Include\ListViewConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 23534 |
| Entropy (8bit): | 6.799082273889017 |
| Encrypted: | false |
| SSDEEP: | 384:E8nUaxG3ZmrKC9ton20xqdTR+XiBH55X1dOj9ylT1DdflGoYLhD2YGiuU57:qAy2XTRJrXOj9ylTpdflGNLhD2YGiuUV |
| MD5: | 42B49A46D23CA8FC56423E1B5087C607 |
| SHA1: | AC826D8226727CF028F4B21D3F3CB32FCA7B1BA3 |
| SHA-256: | DC445A20C79D682B6BD57CBD6E17BDD1725497260224C8B3F356C420C1FE5B85 |
| SHA-512: | 0630D80328B511D41EB6D8DF45329E9F12D7CAA524207D6CFF0BE817F443A0F3EC801FC4372F9E19DA70CE1177E78D669DB06D5845C1156AE3290D79706A3F5 |
| Malicious: | false |
| Preview: | np.m...RV.}2<.W.s.c....."...p.}R...@lK]1..<..x...]F.P.`.4U3.============================================================================..; Title .........: ListView_Constants..; Aut"P.....D..}qc.n.J.r...h!....8.'....S.XZ,.f..6T.>[[u..>..y.g.n ...: <a href="../appendix/GUIStyles.htm#ListView">GUI control ListView styles</a> and much more constants...; Author(s) .....:mO.b....<.a(y./...o...Y:...p.}R...@lK]1..<..x...]F.P.`.4U3.=================================================================================....; #CONSTANTS# ====================p$.3....F..ld.`.D.~...n<....p.}R...@lK]1..<..x...]F.P.`.4U3.===============================..; Group state - Vista..Global Const $LVGS_NORMAL = 0x00000000..Global Const $LVGS_COLLAPSED = 05).>....J...5.?....U..wM......+...]a.P< ..1.w1.s..S..}..g.z.$LVGS_NOHEADER = 0x00000004..Global Const $LVGS_COLLAPSIBLE = 0x00000008..Global Const $LVGS_FOCUSED = 0x00000010..Global Const iU.I...r7.P...}.Y.;....c3...!."......" |

### C:\Program Files (x86)\AutoIt3\Include\Math.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4961 |
| Entropy (8bit): | 7.581153906883698 |
| Encrypted: | false |
| SSDEEP: | 96:psszdr6dzdpzduhzdTzdzsdzddzdSdzd9lzdp8E4KJTT6zdz1HzdzEPzdFdzd4FS:bglHw5plslj4l3938E1al1TlYHlu5lhe |
| MD5: | 7EE14CF0DF1E8FA31E356FD8E6E49BE3 |
| SHA1: | 34475264786777D510C43A8FB90146352FC710F4 |
| SHA-256: | E78A0EE8382E570C82BEF910FEF98F2593C8D56A047299CA2BD92656A7B18D23 |
| SHA-512: | 89EA2D198C258A18BBFBB64226AF0513D4C77FE3BC2C0B151411B9A1547CE5177F0926B783C7BCE95C5401612284C6BDCB4D4150A7E4BBA2C6A36A0FFB3A60 E5 |
| Malicious: | false |
| Preview: | .....o..._..[.;.x1.JRf9.4Z.....#:X..D.....u..%.sx%..b.p.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~8......n.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~.-..N.?D...:.O.. ..D..S.E..:4.J_. >.x.6...7A^..._......Lu\..-%......b..../.....o....U.....{..NRz...ry.5.7/&B..C....h.'i.. qN.....;@....g.....s...]..V.\..2;.E.p<.w.....+"'....(..)[/\.Ym+......2M...S.....h....[.K._..(+...=P./X..L.yqi....T.. {.:..D~8......n.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~8......n.....).\..'....F.....fe....`.)uH.{.do.d..e.6...}N`.Zc8......n.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~8......n.....).\..'....F.... .fe....`.)E..L.IFo...K.....%BCF.tl>......n.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~8......n.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~8*.....pb...Z..A..'....F.....fe....`.)E..L.yqi....T..{.: ..D~8......n.....).\..'....F.....fe....`.)E..L.yqi....T..{.:..D~8......Y.....s.....!..Q..4....26.#.3..u.+...Nwt....T |

### C:\Program Files (x86)\AutoIt3\Include\MathConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | COM executable for DOS |
| Category: | dropped |
| Size (bytes): | 1240 |
| Entropy (8bit): | 7.251278679247984 |
| Encrypted: | false |
| SSDEEP: | 24:SyAfAjhH8DqejmAfAgfAs/0r0YlEUAyWH2l7nP:84jhH8eO4g420rLlEbTHiP |
| MD5: | 260B9B3A7731DFB9EADD0EFC2382EE3A |
| SHA1: | 6534F39C5E7BD1AAFF38190B8EE961121DC00D40 |
| SHA-256: | 62B68BF9A031CB98CE52651EFC59259D36B7463EC5D926DD7F2BA240618AB501 |
| SHA-512: | B1736F0C57ED05B28DEE591D958BF86B4E4F196209C645724C09ADD66AC557956189B461DD17A578962B0CC9FFF85D5CD6410D3FE3F2500932C2E7E3C6982F4 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .1.w.(+.......fEO9.... }.;.=....v.....\|.*...b.Q*L.H3....q.V...e.)E`r.....B..Vrl$.f..X..&.=....v.....\|.*...b.Q*L.H3....q.V...e.)E`r.....B..Vrl..`...Q.~......e...}.5.Hg.F,..y..x....A8."...=.g.2!....L.._aA..`...K.nZgC...e...u.&.~W.%U.LS...\|Z..]#.K.b.W.3<.R..._..K-.9.5...A...iH.H.....D.7.7W.Z6..7...`...]".K...0.r.3,.Z..Q..Po5l.3..MV.;.......,..U.2.....b.Q*L.H3....q.V...e.)E`r.....B..Vrl$.f..X..&.=....v.....\|.*...b.Q*L.H3....q.V...e.)E`r.....B..Vrl$.f..X..&.=....v.....\|.*.."R.W7R.:@`..z..H.e.)E`r.....B..Vrl$.f..X..&.=....v.....\|.*...b.Q*L.H3....q.V...e.)E`r.....B..Vrl$.f..X..&.=....v.....\|.*...b.Q.{.UQ~..\......1.<QPE._......!.m....1m.RhNi.m.....u.\|.&).o3..v..6a]...h.*.....P1...z.._..YB~..`..!@.i^e........^.h..c.G=..72..}G..y..#.....Q=.o.....M..\xM,.h..W........v.....\|.*...b.Q*L.H3....q.V...e.)E`r.....B..Vrl$.f..X..&.=....v.....\|.*...b.Q*L.H3....q.V..============================....\,.Z.{Oh.2SF....(...@.s..#.QmeI....1....uy..WH?......C..*V............ |

### C:\Program Files (x86)\AutoIt3\Include\Memory.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 17664 |
| Entropy (8bit): | 6.268275658439905 |
| Encrypted: | false |
| SSDEEP: | 384:jd1/7LLZyzFZfgUrKz6hzCXK6zrXlp9yt1HnTriEBQmNd/q9OmWAG5:Tw3+zuCFRdWQmNdS4I0 |
| MD5: | 7D2AE203760F5C3E045037400CD9D6CF |
| SHA1: | 1168D26D9F5655C95856D29CC0336C4D1D463D0A |
| SHA-256: | D056808B7E2D6196DC413A4CD2E531AB8B87D5A32ABDEBAA9B1C05D29946AFA3 |
| SHA-512: | 79F63956A835ADFD580BC905437C6ABD139C15D660C3D254428723447ABDAEF3E2F557DF19EAB1414AFAEACF58F45E711293E10905F3E8F161B1C783F3A04E3C |
| Malicious: | false |
| Preview: | ..o.Fwu...*.......M,..8......$......D.5B..O...d...l.@.-h..59.ssConstants.au3"..#include "Security.au3"..#include "StructureConstants.au3"....; #INDEX# =====================================..<..?,..Ty.....,.....Na......v....K..f....Z .T-.V?...t0..Qgg.=================..; Title .........: Memory..; AutoIt Version : 3.3.14.5..; Description ...: Functions that assist with Memory ..o.Mg\|...j.....1..b..S\|......k.....U.4D..C.s..uGKk.\.,`....z,.rtual memory, provides a core set of services such  as  memory  mapped  files,..; copy-on-write memory, large m.n.S"b...+.......7....Y....8........4D.CF.=..s].".M.(j...aPa.Author(s) .....: Paul Campbell (PaulIA)..; =====================================================================================..<..?,..Ty.....,.....Na......v....K..f..:$j..I3{$].c..K..8...# ===========================================================================================================..;..; Used by GU..T.l"...I0....u.G7..(.D....A.....v.> |

### C:\Program Files (x86)\AutoIt3\Include\MemoryConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2747 |
| Entropy (8bit): | 7.75636970817957 |
| Encrypted: | false |
| SSDEEP: | 48:lv0TUvE6vuLMMWbFduz3egSN1mgsfpPsboHjf6gvOsvnrUcxaj:oFfL/zfbgs1s8HOeOSE |
| MD5: | 65F6CEFE268BF1777F5BE5FD9CA6DC25 |
| SHA1: | 11E7B54E3405B111ABD6CEFB5CC8E4132C251777 |
| SHA-256: | C423E9B7C40ECAD6C0F14574726DE355CFE915A17A5128958C923F8695BC0715 |
| SHA-512: | 055FA487FB00DAFFF4C8F8C702ECE5159DD8719F970A6679146C8EFBD519BD54F7A1DFB791A25F39AC8AFA477EDC7C5ECAE5CDF3040A3C6EFA005F3CFEC65E6 |
| Malicious: | false |
| Preview: | :.^...#.+.8.gj.J.!V...8E......6.....1c,Dk..m.s+..u;R7.M....E$...._z.;Ck.?Z4z.'K...A=......6.....1c,Dk..m.s+..u;R7.M....E$...._z.;Ck.?Z4z.'{...(i......%.....,.t.9....!x...&r..-K..6.1m.f.....h^l.1I:i..X...G ......n....."d1<8..9.&...c.iU....-.X7....!(.u.7.v.)!.hV...r.....b.....7~P."..".=?..f(A0. ...b..t.R...g.V.#.K& J.!V...A=......6.....1c,Dk..m.s+..u;R7.M....E$...._z.;Ck.?Z4z.'K...A=......6.....1c,Dk..m.s+..u;R7.M....E$...._z.;Ck.?Z4z.'{...G ......E.....1c,Dk..m.s+..u;R7.M....E$...._z.;Ck.?Z4z.'K...A=......6.....1c,Dk..m.s+..u;R7.M....E$...._z.;Ck.?Z4z.'K...A.......+.....(.\<......R..x~_:.@....x.....4.&Z..G*V..L3..9 .....9....m21:9..$.jQ....H Ih=....E9.H..Sw..9:.`.eg.u....XG......B.....1~!.f..`.DQ...)jOIH....f.5\.o..0..H7..?G9?.*B...;l.....e......I.N4.....n+..x6W:*z.. ..9._...g.A3..]#@..[$..0E......;.....n?}Y...#.n2....Y!Es/....<9...Sw.6s\.n.k&.:5.. ......C.....<&#If..Z."y...hE.dT.....5F.t..*..C^k.2.;w.*{....b...........S. |

### C:\Program Files (x86)\AutoIt3\Include\MenuConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5208 |
| Entropy (8bit): | 7.8055231689919955 |
| Encrypted: | false |
| SSDEEP: | 96:2pxKra3aj/Iou6XMx5aNEYfZd0ldVCppwj9I7RvbL69KVPed:yMC6XMx5aNEYfQ4wjoTL6sPw |
| MD5: | 4483CE0A481343842782588E62A42087 |
| SHA1: | 28E5E7760FC3B5A187148AED0A4FF0048467564F |
| SHA-256: | 696A56C9897FCF3FB9E200EBCCBD31EFC6C89300F7E14981D12C9A2CDC5BDB71 |
| SHA-512: | 5558CC1AA2D1B514881E2C40D6C33C7E8EE9AB84E45C5E5D19A2A9C68F19FF11364B964100C0D6F47AE8892E06BBFF9D75DCBC16A6393A4787F7BFCE32364AB2 |
| Malicious: | false |

Copyright Joe Security LLC 2023

| | |
|---|---|
| Preview: | .E...~#_V.......kK.>..i..w..S.DOj.PK.s.(7..C.8.]..._..1(...uP....OT6z.F.....2&.mV.J......w..S.DOj.PK.s.(7..C.8.]..._..1(...uP....OT6z.F.....2&.mf4L...E..j..@.W\y.CL..G{....Cv....o. .,T.._....I...d).A....>/.ef4L..._..+.\N.W\y.CL..Lrf... ..@...O\|a..^hC...1.e4N.....`i...P...._..#.W..txl.,.O&Mg"..^.+.N...4.Je~..w)...j....k.U...../&.mV.J......w..S.DOj.PK.s.(7..C.8.]..._..1( ...uP....OT6z.F.....2&.mV.J......w..S.DOj.PK.s.(7..C.8.]..._..1(...uP....OT6z.F........ZP.T..b....jM.DOj.PK.s.(7..C.8.]..._..1(...uP....OT6z.F.....2&.mV.J......w..S.DOj.PK.s.(7..C. 8.]..._..1(...uP....OT6z.F.....2&.mV3}..S..j.V...Rs.+)n.j\F..;.8.P...h.Jcw.......X.V$M..5.../&.`..z...^..&.z....w. 0d.IVB..5hA.]..R.,Ky..Q$M..B..I/.\|$...H;.p[FG..]..+..-...#.I;}.eGK..:.8.P.. .R..<%..:....M.R*d)I......KR..)r2.....z..^.IBe.g1W!@tf..Cv.@...=.oXX...uM....BY;w.O....mz.p(Q........q+.27..PV.6.%:..N.=.j...J,V..C<M..j."&[.j[....?+.`[.G..]..+..-...#.I;}.oPD..?.G .%..._..t%...x].!.5.d%[......{;..-a:..s.....S.I.g.]F.~ |

### C:\Program Files (x86)\AutoIt3\Include\Misc.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 32280 |
| Entropy (8bit): | 6.596791172605695 |
| Encrypted: | false |
| SSDEEP: | 768:COwRqoIyXsPre0jPWHI2JZT13pOTyDf1b4aQVu1:COwQHyXyPWo2JZRZOTyj94aQVu1 |
| MD5: | F3541EFA50D8C679D41D846562818C8B |
| SHA1: | D16D02E40D04BC2D8056B9A7CE75AF72EFB8EDA5 |
| SHA-256: | 00A4AC60D56C669ED3292BE44BFDFB625D2E092B4DC1ADE19F38369C97B02A63 |
| SHA-512: | 94B8515775C874A2D872AB37DDDEC0E273452AB06854D18B90AB5F91DF8ED3DB5277B2366D84AF3DD872A847B4F10AD5845C55456090860DC7DBB7ECE0CF7E 66 |
| Malicious: | false |
| Preview: | ..M..8!..qSO.,.:~s.G.......Y@....\|..:..v...X....+....)QM.LreConstants.au3"..#include "WinAPIError.au3"....; #INDEX# =========================================== ==========================...Rpx..#......Im.........t..P...G. ..tl.>...o.........*.u........: Misc..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with Common Dialog....Tm..vR^.R..Z~......Pip\...Z.q.. 0.#...3.......c..EB..(Klaatu) Thompson, Valik, ezzetabi, Jon, Paul Campbell (PaulIA)..; ========== ==================================================...Rpx..#......Im.........t..P...G. ..tl.>...o.....r..r.f....==....; #CONSTANTS# ================== =========================================================================================...Rpx..YQC.@..7?.Z......`.um".;.I.....M.........7 ....QcB.[al Const $__MISCCONSTANT_CC_FULLOPEN = 0x0002..Global Const $__MISCCONSTANT_CC_RGBINIT = 0x0001..; ====================== =======...Rpx..#......Im.........t..P...G. ..t |

### C:\Program Files (x86)\AutoIt3\Include\MsgBoxConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4434 |
| Entropy (8bit): | 7.813449692689937 |
| Encrypted: | false |
| SSDEEP: | 96:HnyyNgEg0IdgYLpVRfaDoPrbmz4ss9VaP1sbw0JV:HdIjlVRrP+bsVaP1spf |
| MD5: | 025C5992A6A02EAF7DA57F6D8798FEFE |
| SHA1: | BC2DEF2CB0CBE365A26C00351F008DB9BB5B6356 |
| SHA-256: | 7F706AA11518CC6B09E0F20AA1BD3C26BD114258D8142B5ABF6FB151B3FDDB99 |
| SHA-512: | 4A11F5B08BF86806965DAF11276E13EF6A3160380886CC7665A922D95EC2472026C54DC87B9980803D02C34B5AF40120D9E48C40BC83B1DF8387EBDB7BC0E5B |
| Malicious: | false |
| Preview: | K;..?.L.t...%D..s(.a........A.A..B.8R..I.-P..a=..PM.....\|.CUo.n....&....t..n6...aj.....A.A..B.8R..I.-P..a=..PM.....\|.CUo.n....&....t..^....5#........R.R.._.v...).S.E.(a...}....A5.7.r..!..F.;....g..}>. %.\|.....A..R.R..Q.%*..=.c.&.g .......]..^F\|..s.G.o.....=..1n.F.?;....O....\....L..b.c.Y.,t......]/.^.'..'.G.V....Wg..h+.Z.48........R.F....k..".0.[.Q..PM.....\|.CUo.n....&....t..n6...aj.....A.A..B.8R. .I.-P..a=..PM.....\|.CUo.n....&....t..n6...aj.....A.A..B.8R..I.-P..a=..g}....w..-<........&....t..n6...aj.....A.A..B.8R..I.-P..a=..PM.....\|.CUo.n....&....t..n6...aj.....A.A..B.8R..I.-P..a=..P M.....a...!..6..F.;....[(. .....9....C.........q...q.y.[.=y..M...Qa...!..6..F.....M(...d.\.\|s.......L.G....%...9.r.._.3n.";...[#..H... ....Y....n...+...\|I...V.........k.....0.E.\|C......X....r..=....V....`..._.v. .........G.(....%...9.r.._.3n..M1....a... ..s.M.R....JD..?d.N.\|........#.9..0.D!....-M..g ......G)...&..=....~...@e..=o.I.24....J....\.... |

### C:\Program Files (x86)\AutoIt3\Include\NTSTATUSConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 240988 |
| Entropy (8bit): | 6.717991314195826 |
| Encrypted: | false |
| SSDEEP: | 3072:gGkuAinBVecezUGOKUrP7WNU0W2jwS3KcTABtGU4:gBRcsU+mjW+ijwkTJ |
| MD5: | F400F900E4D2E5F7A97A9DF3391E8CFE |
| SHA1: | 3279A3D80B8B62AD58A41F87126A477A356A0EA2 |
| SHA-256: | 6003370803F60AF4D892FD38CC0608E4EC4A9D9A725A3FD72DC423D4A5DBFE09 |
| SHA-512: | BDF9C04CA4271DCA4B083DA53D657A23C3711DC1CCBA14D6845D77DFA5FDE5677263AA00A83CFC5856545EADE3B24C8FDE2C4348D26131AE03BA7F1CA4C4 00C |
| Malicious: | false |

| | |
|---|---|
| Preview: | #..=i8.....Xe.9S...PrE.~..q.m...X.....V..._...P{....~Hn.N..t..M=========================================================================================..; Title .........: NTSTATUS UDF Library for A..1L9....zu.\...`.Ix.T..k.c...T.....P.._....R./....m[i.=l.,...r codes (NTSTATUS) to be used with WinAPI* UDF library..; Author(s) .....: Yashied..; ==========================================..c8p....=..c...N.6....l.m...X.....V..._...P{....~Hn.N..t..M=====================....; #CONSTANTS# ===========================================================================================..c8p....=..c...N.6....\4....@.......1..w>...\|..&..N..1..@00000 ; The operation completed successfully...Global Const $STATUS_WAIT_0 = 0x00000000 ; The caller specified WaitAny for WaitTy..~d#......o..*...Rx.Z.9["...I.......N....@.#....1.2.SP.:...en set to the signaled state...Global Const $STATUS_WAIT_1 = 0x00000001 ; The caller specified WaitAny for WaitType and one of th..:l>....^r.\<.U.H+.U..9[p...O.... |

### C:\Program Files (x86)\AutoIt3\Include\NamedPipes.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 14339 |
| Entropy (8bit): | 6.448140494799627 |
| Encrypted: | false |
| SSDEEP: | 384:mKmzKo4oyUS0UlZIDGcZDrSTLbFcYXrkV/9O:UMlZChYcO |
| MD5: | FDEB37392811E45B19E57470B7B32080 |
| SHA1: | F2F7F960A5CF0D55A2C7A792F0B6880035F7844C |
| SHA-256: | 2CAFEA40521D4DD5426D5ED226DE8EE8B278C373F9E4EBA9D5887A501BA21DFD |
| SHA-512: | EB39092CB170237E801FB7A5405D4193BF168527669DF25FFBC97FF07CD7D44BDC9DD5EE42FEBC319247C3CE92EB35F775F3F82184F13C4769416D9085D8E03 |
| Malicious: | false |
| Preview: | J....I...v.=..N.t...rcw.#F.#.......DyJ.:.9...GS.1.../kZx...kk..==============================================================================================================================..; TitleI..X.....7.~".4g..._cg.J..........=6..}.fH..+,.3.B%.<3iz.....: English..; Description ...: Functions that assist with Named Pipes...; A named pipe is a named, one-way or d.........\|.8..da....wur.j..w.......'bL.n.>...UC^e..D>.{9'1.\..more pipe..; clients. All instances of a named pipe share the same pipe name, but each instance has its own .....N...x.:..."^..>63.#D.w...Q...czA.b.6...VTCe..Vp.{%,$OA.e conduit for client server communication. The use of instances enables..; multiple pipe clients to useI....O...9.?.. ".....m.~.o..9.......'6e.7.'...CU_3...1.83:'.].ed pipes, subject..; to security checks, making named pipes an easy form of communication between related or .....]...9....'g.......(.#D.w...Q..'6.. |

### C:\Program Files (x86)\AutoIt3\Include\NetShare.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 46121 |
| Entropy (8bit): | 6.559979685804381 |
| Encrypted: | false |
| SSDEEP: | 768:iFBjFT4E1JrFs6x69g0s2yAPHR0xGkg5SEIohkn8k:ejFEE1JrFs689gD3APHqwxT8J |
| MD5: | E09A8841C06514B06A343C0357184106 |
| SHA1: | C2747D2E57EAD8F56299F1C0B701B36937651FFB |
| SHA-256: | E395C4B79DC47D84B4B9013E284870EA59292F10A9F0AFE083A6C8C41BA77790 |
| SHA-512: | 1D86345BEABD725E230F2C352E45AA7B3606D2295EFB388F5CE62CB7C1B22E8F8A9D810CA1740AC496812230EF941D6DB748E012F14D6124CF955F62E348026 |
| Malicious: | false |
| Preview: | XND..L4.H..}...dN.nD......._..y....s...1..k..7.......^[*..0..nAPIConv.au3"....; #INDEX# =========================================================================================================F...P.m.X..#H$.Ty.. .....,...4G..K.... .....l.....s[:..f..ersion : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with Network Share...; /OO..\$....>.q..!.a_......,...n...EC... ...6..v........]&..w..resource is a local resource on a server (for..; example, a disk directory, print device, or named pipe) that .FD..\p....m.\|.I&.'_....M.h...j....D...6....e..a.........n..2.. network...; Author(s) .....: Paul Campbell (PaulIA)..; ============================================================================F...P.m.X..#H$.Ty.:....P..1...'T..X....x...x..9.........s.....; #CONSTANTS# ===============================================================================================================F* ..V2....q.j.I`.Ss...$.X..:T...... |

### C:\Program Files (x86)\AutoIt3\Include\PowerPoint.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | COM executable for DOS |
| Category: | dropped |
| Size (bytes): | 58031 |
| Entropy (8bit): | 6.499992988453552 |
| Encrypted: | false |
| SSDEEP: | 768:oZsZQ4cH6YnwKMK9lcJpfEoFuawr1Q1G4fRBxHj9FY43ZO+02:WSX/RpXwp6G4fVBJLP |
| MD5: | 6699E3BD26F711648A4F15B1FD66B93D |
| SHA1: | D360DD15CFD9D9B8FD7DE36DE763BE5AC8375B3E |
| SHA-256: | 35BD6DB61A8880E4706FB979AD09CBCE71DC42B000FFFA67D2F9354E1869D3DB |
| SHA-512: | B408C3E064365329CDC4CA2DF3A84549B367C4E99ED98CF2C982EF536A1DC7B3D15B15A9057F7EA258A815D9B2A5D1BA7FAB3415DE38707F3AEC1ACBECF2D655 |
| Malicious: | false |

| | |
|---|---|
| Preview: | .,....-f.5.]-_...J..~I.I+.n........&.A..o.V../W.....*.^.L=_tintConstants.au3>....; #INDEX# ========================================================================================================.x.]C.t>.g..uo.._.N.6....:..s........\|.....8.....R....Os.a.@!{;Function Library..; AutoIt Version : 3.3.12.0..; UDF Version ...: Alpha 5..; Language ......: English..; Description ...: A coll.&....il.z.K&1..J..mB...y<.t.........?..I..=.(..&.....We.W...`lerPoint files..; Author(s) .....: water..; Modified.......: 20170606 (YYYMMDD)..; Remarks .......: Based on the UDF written by t.$..^.:f.z.W&9..o.H.GD..4qH).......&..S..~.+.. A....Ku.X.]altm/forum/topic/50254-powerpoint-wrapper..; Contributors ..:..; ======================================================================.x.]C.t>.g..uo.._.N.6....'b[:.........o.....l.a..\|......+..K.B...; #VARIABLES# ==================================================================================================================.x.j9.&a.6.....2p,. nO..'.V'.......7. |

### C:\Program Files (x86)\AutoIt3\Include\PowerPointConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7475 |
| Entropy (8bit): | 6.638945299853551 |
| Encrypted: | false |
| SSDEEP: | 192:+fEV3U2QyDwR5a9eIFddlZzDtLcxapPpXOVWb9jA9:+fEVPF40Nz9xpMYA9 |
| MD5: | 520BA436BE0866699F4C55A88C8CC923 |
| SHA1: | C63309203FAC1451243E28B87F844D3F48C93737 |
| SHA-256: | C4A8EE8483BA558EB701372A94C6A3FA50F06D59066E73C60D553E6B4A82F157 |
| SHA-512: | 453DA6E25E59E9DD4994AB9E2766C23E8EAF4F964223125FB67E6BF64C4C04AF371A28FD8440EDA3E47184C544E5F6B650F5B18BE3E9370387894A688AE44864 |
| Malicious: | false |
| Preview: | .=TA..P..;~..4Y...g.....d....$.Q.~k=...3Y..^.....CuR..B..6...=========================================================================================..; Title .........: PowerPointConstants..; Au.;sVA.Q..=..C.s...ut..O.\|...~..O&v.... J....^.. tsO.....b...on ...: Constants to be included in an AutoIt script when using the PowerPoint UDF...; Author(s) .....: water..; Resources ......tjM..F..=~.C.c..q*3..0.3....#..\7&s...c......E..B.<A....e./library/ff744042%28v=office.14%29.aspx..; ============================================================================================.i..\...i-.^.n...y{....z....$.Q.~k=...3Y...X....c-....,..6...=============================================================================================================..; PpFixedFormat.-JGA.Z..1b..P<..g4#..$.g....m..Mc9f. ..v......V..K.$......s...t...; See: https://msdn.microsoft.com/en-us/library/ff746754%28v=office.14%29.aspx..Global Const $ppFixedFormatTypePDF = 2 ; PDF.2UP..@ ..\|..X?..Z72..2......_..E""TE.. |

### C:\Program Files (x86)\AutoIt3\Include\Process.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | COM executable for DOS |
| Category: | dropped |
| Size (bytes): | 4135 |
| Entropy (8bit): | 7.664947986064948 |
| Encrypted: | false |
| SSDEEP: | 96:v/Be3BuBvBPBFBTz6BoQEECBJBzrMXbKDGGyKBqBRdqpy:v+UzvMsGHdqpy |
| MD5: | 78AB65F36E907217273D5F72D941C739 |
| SHA1: | C827CFCA80E96FF64FFC66E8298E43CC94DEE333 |
| SHA-256: | ED3011A2EB826F0D7C8B3292375AD19B9A5F9873D01CE358B5DC699DD181BB5A |
| SHA-512: | 8D16DB0E19DBB95D481078B5ADD7167FB98CF148415123A1B9ACD4FFF1FFF9119239382BF181F4E8A4860E1C523001468AF7F01501AF3CD8A3FD78C3EE9261EB |
| Malicious: | false |
| Preview: | .d.Z&...c.....bx....p+%......q.._.........x......>......\.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8...e..B.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8=".x....#..#..dG..t.5. .....&.W3.%......`..r..O...P8.....kW].?...Q.-..7.\|$...=.h}..,..H..c39.....2...........-.W..%GA.0....f..-.X$...#.....bN.j..{(".....<...Y........x.A...dD\.=.....h..!.s/...7.)...........;.....2...2..A... .h.J...+TD.U..B.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8...e..B.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8...e..u......l.;....EJ..UH...Q.zm...../...!..R.....C0.....8...e. .B.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8...e..B.>......9..-......;.F.a.\|p......a.L.......E-.v..V=".x..B.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8...e..B.>..0..wT..s.XJ..UH...Q.zm...../...!..R.....C0.....8...U..D. ..C.m.&.n.XJ..UH...Q.zm...../...!..R.....C0.....8...e..B.>..0..wT..s.XJ..UH...Q.zm...../...!..R. |

### C:\Program Files (x86)\AutoIt3\Include\ProcessConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1783 |
| Entropy (8bit): | 7.524562665040159 |
| Encrypted: | false |
| SSDEEP: | 24:FFOlDUlfhn4aIR5DUlDUClDUldHCZUmqhsZhLeoUXCQDUUmGJM9EC:DP4aIRaHi4hsZCyG9JPC |
| MD5: | 3985625F63F44530E1BF29DA53E4B193 |
| SHA1: | D07E655E0A5CBDB48C48D77C52840BFE3CA9458F |
| SHA-256: | 98030A2A2789E6515748A2E991D49428B680D56B419FE32506F62DDE50EE258B |
| SHA-512: | 359D97A510466F7AD7CB9E087158A2B42436F51E9AFF76C5763E646376C6C52F770D7BEE47F59FF43EDE443521EB464D7312618F5A51CBB51CB8BF6A925FC546 |
| Malicious: | false |

Copyright Joe Security LLC 2023

| | |
|---|---|
| Preview: | Qe..d. .:.;j..QG.d...Z)R\.[.j].^.W...v.-......d.=.7.L....Fn..O1..5.y.*.h4..:ap.y..#Q7B.[.j].^.W...v.-......d.=.7.L....Fn..O1..5.y.*.h4..:ap.I..J.~..F.yN.M.D...k.b......7.t.d......:&U.;x..m.7.x.u3..)oc.p...W*3..D"....D...e.*.......T.;.N....Q..:N.R"..2...y.!h..t\|9.d...w.i...F3@......>.......+.p.*.......:O.R\.k.7.7. g..n3#.j..>-....Q...C.D...q.F.....+. .x.....U},.I,..5.y.*.h4..:ap.y..#Q7B.[.j].^.W...v.-......d.=.7.L....Fn..O1..5.y.*.h4..:ap.y..#Q7B.[.j].^.W...v.-......d.=.7.L....Fn..O.....d.T..Z..I...d..#Q7B.[.j].^.W...v.-......d.=.7.L....Fn..O1..5.y.*.h4..:ap.y..#Q7B.[.j].^.W...v.-......d.=.7.L....Fn..O1..5.I.P.:k..'.".7..N>E<.5p.4.1.#....-......i.1......Y.[.N..x..X...R..V..B......[-N_.F./P.S.Z...F.W......7.t...#..}.(.r.&S.[...Y..)..7$}.t...X.u..L5..C.....k.@........O.O.0..w.[n...<..8.t./._N..e=!....jL./.)`.3.<.'....0.......i.1...6..Z..sb.....,...T..Z..J......#L:..V.gP.Q.g...$.q.......}.R.I."..\|.+.i.<H.(.d.o.e9..7h}.N..\|.f_..M$..G.8.... |

| **C:\Program Files (x86)\AutoIt3\Include\ProgressConstants.au3** | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2381 |
| Entropy (8bit): | 7.69809566928601 |
| Encrypted: | false |
| SSDEEP: | 48:w3td5qKcJZ+tdMstdthf6884nP04x9uEanvjSpWkurChPc723AdtIle:WjqKc0HPhnncy9ckWkuqUy3APIle |
| MD5: | 1912BCB54080A281733BAC22819DFBDE |
| SHA1: | D6EE1CA6E29B5D8BC31AD201F42B200BDCE64661 |
| SHA-256: | 87DB817558061F4F18B2624681136B44BD119C274ED7E38B7B43CD8922B61F1E |
| SHA-512: | B64C14B10978FC38359719C24B1D5C1BB45570B3781617CE9310502E0AF9BC5A652E39506A9511CAF788A621914F549119B7C6D6BEF2692940B2FC970E4062AA |
| Malicious: | false |
| Preview: | ft.....k..'!.....?P....).2.S.z9ax..f.....&r. -..X}>....v.F(C.xx T].3.Ht.H..."Nm..wL./.S.z9ax..f.....&r. -..X}>....v.F(C.xx T].3.Ht.H....yk..#..w.@.i*rk..u..g..\|=.nc....p...F-@5?.1*T.@...}..'bO......G~..@J.^...2e; ..u.....;..z\|...M....(U.e..*+=GN.2.U!0......0. ..$..j.)..W(<NH(..C..K=.zb...b=....$I.g..e.o.....}..=;....!S1..j..q.N.(v9eAB5..V..ha..+...4k....k.U;P..eK.......;;U.....3S~..G{.2.S.z9ax..f.....&r. -..X}>....v.F(C.xx T].3.Ht.H..."Nm..wL./.S.z9ax..f.....&r. -..X}>....v.F(C.xx T].3.Ht.H..."Nm..wL...c.\|$..mc...y.;r. -..X}>....v.F(C.xx T].3.Ht.H..."Nm..wL./.S.z9ax..f.....&r. -..X}>....v.F(C.xx T].3.Ht.H..."Nm..wL./.S.z9aH(.{..N..hB.Z\|...,#....k.+W-...O85..3.E1rE...'Sk..".b...5a/6.O:.Z..~<.qy..E!#......Bv.9.*'\|.@...}.Um.7.....P'...j@.....%e0eaB5.....Y..N]..1.Q......F5N.tu=R@...z.xC......\.>..jU.P.1..V..al.......B.&0...4q....-F.y..61d.....I..+#......kSt.....A.*..E..vr...p..H.. 0..oM....8F.p..O.q....M..:6U.....P4....3.@.!..P..vr...b |

| **C:\Program Files (x86)\AutoIt3\Include\RebarConstants.au3** | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6733 |
| Entropy (8bit): | 6.752815555123502 |
| Encrypted: | false |
| SSDEEP: | 96:plFk/Vj1HD+ZzU8dYeAX0fr1DTRRA1vTqxyom6iQcum81M:HFk/VjN+Z5YemgJnRRAQgom6iQcxwM |
| MD5: | 89519C322A99198C14A57897346748E3 |
| SHA1: | 9F80E89E4DF2DBDC6F14409B0CFD597FEA78F57E |
| SHA-256: | 5B712C98904C889879512870FBA6ADDE71D3E4905C5F28A0D1EC272BE2CE051D |
| SHA-512: | EFC248FF1B4D1EA0EFEEEC2C90B7B5CB60FC4B5C206159C780641351B00427D11EE4B6B3AFE7ACD900D36A726AD25EC5DBC0540E86998E0C153FF2088004CD66 |
| Malicious: | false |
| Preview: | .3`..ri.....0q..Ir.?.......o..u.8....V\|P./...Qn".$L-svU.K..$.==================================================================================================================================================================================..; Title .........: Rebar_Constants..; AutoIt..k..nb....\{O...\\^Ji..P..K.7.f.+...../..{...fh?q\|.s<"...U.9...: Constants for Rebar functions...; Author(s) .....: Valik, Gary Frost, .....; ====================================================================================.g3.N:0@...RhA...TliLt......o..u.8....V\|P./...Qn".$L-svU.K..$.================....; #CONSTANTS# ===================================================================================================================================================================================.g3.N:0@...RhA...Tli\|C.s..Y.5..E.B.A.O.a..\|...H.@g\3Q..'.%n.W._WM_USER = 0X400..Global Const $RB_BEGINDRAG = ($__REBARCONSTANT_WM_USER + 24)..Global Const $RB_DELETEBAND = ($__REBARCONSTANT_..Q. B_]...FXv.....=t2&..J.x......H.x..VaE.M.....MvV?C..&.)m.F.SER + 26)..Global Const $RB_ENDDRAG = ($__REBARCONSTANT_WM_USER + 25)..Global Const $RB_GETBANDBORDERS = ($__REBARCONSTANT_WM_US....S49T5...:.....?'.i..\|..o......J.`.. |

| **C:\Program Files (x86)\AutoIt3\Include\RichEditConstants.au3** | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 14689 |
| Entropy (8bit): | 6.817873657083667 |
| Encrypted: | false |
| SSDEEP: | 384:dU+OQHy8m3tGPDpr2+91KQYsimTO0g4fnSjtDvvDmftxmbw1uriuXAeaSQjEJ6E5:9dKfHQEk73+mUh5Gy |
| MD5: | CAC94EF74A5A92E1702891CE1EBDE860 |
| SHA1: | 547296ECAEE8CDE51067C48E4A4E0941CB91882A |
| SHA-256: | F04849CCDFFD6648ACC6BBF57A694E7CFAA535316B9174FD0B239C437F6BB1E5 |
| SHA-512: | FF088CDD33AA034A96B2BE0E9A31DBF60D52C39BD1101DAAE47104B06FF14594691478A75EF9BDA421305DF282EA9F8C2C384DB78C0D12A643CF99D3EA83DEFF |
| Malicious: | false |

| | |
|---|---|
| Preview: | ...S@._......}.F...R..{..m<..S/..f..d#..P..<.4...Oc.....R..===============================================================================..; Title .........: RichEdit_Constants..; Aut.'..z...........h.Q.r[......7t...2..u..w$.....r.....6;....H...n ...: <a href="../appendix/GUIStyles.htm#Edit">GUI control Edit/Input styles</a> and much more constants...; Author(s) .....: G....j.......f.X.zk*..f..m<..S/..f..d#..P..<.4...Oc.....R..=================================================================================================....; #CONSTANTS# ============================.S......O.....{.X.zk*..f..m<..S/..f..d#..P..<.4...Oc.....R..======================..; Messages..Global Const $__RICHEDITCONSTANT_WM_USER = 0x400..Global Const $EM_AUTOURLDETECT = $__RICHED.:..b..<........N.~g..7..1m..\|..{...A.#..U.)...-.....}+..CONSTANT_WM_USER + 50..Global Const $EM_CANREDO = $__RICHEDITCONSTANT_WM_USER + 85..Global Const $EM_DISPLAYBAND = $__RICHEDITCO.=.qb..?.......s.h..:x..7..?o..N6...b. |

### C:\Program Files (x86)\AutoIt3\Include\SQLite.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 56915 |
| Entropy (8bit): | 6.680710941312092 |
| Encrypted: | false |
| SSDEEP: | 768:Gg9G30APn8l1Q3w2slIpVazmT7ZKRhXlxjlvEk7UFEhPSRuhWrq7Mn:WIp27RXZu0FsPSRDr5n |
| MD5: | 4BEA424DD78F2112DCD9BD8533AA6A71 |
| SHA1: | 3FC88F7B36EFA2737F709CACA47ED540B5327AE8 |
| SHA-256: | 37EB8652A4BA33E71B033A345031AA5DF6B933F9F9FC4649B2F58A4D81D1900C |
| SHA-512: | DB9BC41D6664711B64D3E13644F029154329459A733110709E8747F5F587578BE54FC7D52F7A1544A0230545780810852B939E8D63BEFA22F5F05580C6103650 |
| Malicious: | false |
| Preview: | ...........(T.(B. .@;W....'..i......K&.......v]..../..M...mu.ine_Modified....#include "FileConstants.au3"..#include "InetConstants.au3"..#include "Array.au3" ; Using: _ArrayAdd(),_ArrayDele.....>.....(8yhC.gm8}X...8+T.i..b...h.m.....#...+....H.Q.)...; #INDEX# ===============================================================================================================================....A.....cw%%..`N.d....(+y.. ..8.....?.....#...}.M...s..W.nguage ......: English..; Description ...: Functions that assist access to an SQLite database...; Author(s) .....: Fida Florian .............1o'..>.?T.....\|`Z.....b....h.<....7W..C.G...D..&.=====================================================================================================================....; ---.....L.\....`t&&..cM.s.....qcY..-..a....e.`.C...4...c.Q...T..6.-----------..; This software is provided 'as-is', without any express or..; implied warranty.  In no event will the authors be h..........."++jE.Cj.~U...9=T..i.."..P |

### C:\Program Files (x86)\AutoIt3\Include\SQLite.dll.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 611 |
| Entropy (8bit): | 7.015697746157304 |
| Encrypted: | false |
| SSDEEP: | 12:iUuJ4YIivDO3VNNz/696k15nvrzR8pWLRC:iHE+Dmz/25vpD4 |
| MD5: | 0F085AA5B86B5186F59007B6D1C1761F |
| SHA1: | 0EA0A20D6F44EFE8B34F39FED09399B302658A49 |
| SHA-256: | 0DDDDC6560993D92BD67CBE882F026E69E45DF992D3F4F5A381B1413F7BF8559 |
| SHA-512: | D6EA4209B3CCABBDAEA40349B2F5BF0EB7FFA0D34FE51E44E9CBA108D62427211AA44E63C1CC122927EF3A0CA2EC2B7A14D8208165FDDCF0E43059CCA0A919F4 |
| Malicious: | false |
| Preview: | 9@A5.......52i..........[..].\..,>.}~0.db..C..d).Y.Z..g.\9......f.%4....=<.78=....&.W...P..Z.m.%!:..;f.\|W8. .."{.N.[..l.`..V.E..3B(`.S...UTht/...P...r.3.3Z.t.$&s.ge?.k.m.#.#l.'....1h.\B......jN....h)5.2i......M...[..].\.cHY..;v.'4..A..e9.^.Y..o.b..T.F....EndFunc   ;==>__SQLite_Inline_Version....).......}=.H..NI...<k..\..1q..W....(u^..2...2....t.K.w.w...A...HR.L.R.)..2i.,F%'.....d...X....-.Uu..b....d.N~j...T.=..:.l...k....'.Rb.O.v.RX...=..V.wgS...."....Y.0...B..T..)..#..,...#c.E....."..........................................................................................vux2f891j9j. |

### C:\Program Files (x86)\AutoIt3\Include\ScreenCapture.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 11343 |
| Entropy (8bit): | 6.490436248566944 |
| Encrypted: | false |
| SSDEEP: | 192:EewUEzewJeEeV8eDee4tjZhdiJQJS+ghxslLk9p8c0QMSSpBLJeq2HGJt0U7nmxA:ezGNoLSVxslLO0B22exxAb |
| MD5: | BD640EC1577CDD6D8D51BEF3070C1C22 |
| SHA1: | 2263837829C9804CF1BE53E0AAA4B412250DB697 |
| SHA-256: | 01D021EF9D6594619F504043618D698BF9E23E1A244801E45BA9A7B950FA96D2 |
| SHA-512: | 607AD2D9C0A2F569563EC5CB6C25C49125D3762E0873A890A474DEDDF91ED45ABD15D4F7B4DBF7AC3DF8B2B36676146F9FFB72B82877660C3F2EC28BE6E1F5FA |
| Malicious: | false |

| | |
|---|---|
| Preview: | .k...\{..2rZA+..]./,/e=..@A.5..z.......A...DfMgGNN..Ea.%.08R..rnals.au3"..#include "WinAPIHObj.au3"..#include "WinAPIInternals.au3"..#include "WinAPISysInternals.au3".... ; #INDEX# ==========.?O..."P.`!......C.\|r~-d.._;.Ay.2C......_.T....?ZQ$.9.._LdL...=============================================..; Title .........: ScreenCapture..; AutoIt Version : 3.3.14.5..; Language ......:.G...@l..W'.`C.....5&,~y..L<.:1.l........l.[`@q.Ln..l....<.R..apture management...; This module allows you to copy the screen or a region of the screen and save it to file. .g...Mv..}sW.R....1*N.b..B&.\d./^....B...A~He.@9..q....y.Y..various image parameters such as pixel format, quality and compression...; Author(s) .....: Paul Campbell (PaulIA)..; ==========.?O..."P.`!......C.\|r~-d.._;.Ay.2C......_.T....?ZQ$.9.._LdL...===================================================....; #VARIABLES# ===========================================================.?O..."P.`!......C.\|r~-d.._;.Ay.2C..... |

### C:\Program Files (x86)\AutoIt3\Include\ScrollBarConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 812 |
| Entropy (8bit): | 7.050454064110725 |
| Encrypted: | false |
| SSDEEP: | 12:kgtnvil+yynf1ynfwpY98XPy+eynfvVfTVgOd5GdbIwBYC:kgtkVU9U8zfy+eUF7VfdcUwB/ |
| MD5: | 2C6312413263901EEC8D14AE4546A343 |
| SHA1: | 84D174071E392B3615B94EB08185AE1CA1DD8473 |
| SHA-256: | D4E90F288B8F085E986FA91852341383B2906ED87388CBC3C4F07B9EE9E141D0 |
| SHA-512: | EFD42A4C972D2773A36141317C6E5736AFB528BC8E24E93CC3A0617A257C67AFD49B651CE146CFABB335D510C70F57B337843F5888880432794DB4B6D59FEB4 |
| Malicious: | false |
| Preview: | ."..b....8psR"2u......i.qp..8*=u.v........Q..O.0.L...EX&...]...vCW3.R..j#-...E......!.)m..feo$.)...[.RG.....>.\|. .CE8...%...vCW3.R..j#-...E......!.)m..feo$.)...[.RG.....>.\|. .Cu....q...kPD . A..y0*.\|[..R....C.{>.:6&j......./.O,@.BG.m.{...MV4.........i...Dw0>...V......u.\|]..{.7j.f....F.AT..zK.w.'.o...h...q."......Iwq\|S.V..W.....4..37 1.=.....\...H.;..>.\|. .CE8...%...vCW3.R..j#-.. .E......!.)m..feo$.)...[.RG.....>.\|. .CE8...%..=================================================....D.0....?a..{.t.J......%]..1..%[.(...P..}.....#.%........b......h.R..... .R9..!....Rsc>.>Mu.t......71..FEX......J.......9....3...BS....c.YE.~..`.a0.B.}~!.D.I:v5.2.n.. *A.]H.j.\|.-..W@H.h.....A....<...................................................................................... ......vux2f891j9j. |

### C:\Program Files (x86)\AutoIt3\Include\ScrollBarsConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2275 |
| Entropy (8bit): | 7.651991314690144 |
| Encrypted: | false |
| SSDEEP: | 48:bZjm3LZjm3xeo1bXlZjm3LZjm3tcca3LZjm3rf4Hp18Bfz/rkT6xcEB7Nm3LZjmc:dMieo1PMKoUeUB7/rkTAcEB7NMgCH3 |
| MD5: | CA7B14F5AADFBF451146C99290491EA1 |
| SHA1: | 7E4AFA4075A7453BDCCD8B9EF25C95CEA925DDCE |
| SHA-256: | 3ED24ED03E28A388B41BE0C390A6F0250B103AF06D556B6A056B3615DE68C26F |
| SHA-512: | 4674A040420BF83D74CA2E1946E987F37D5BCC4A6106DFF91B744C17DCAF2045074B46007B7BEDFDF02669BAEF4666A261731D61AEB98B9D91A9360BEC7E4C<br>6 |
| Malicious: | false |
| Preview: | ....!}.y,*{R.....SC.`..z...U..]<.s3L..O<...uf....}'.Rc...4R...C.p5O!<x(...#...M7....d...U..]<.s3L..O<...uf....}'.Rc...4R...C.p5O!<x(...#...z1.p..5...F..N/.` K3..s....:....i..0...)...7.m^.nr, z_..>...A>....b.......f.n _=.\/...&<...M..O.....y...^.c&H<B*{B..p.....x.w..6.......t.-z.\|../...h....22.F~...3O.....a(5}s<5w..m....^$....d...U..]<.s3L..O<...uf....}'.Rc...4R...C.p5O!<x(...#.. .M7....d...U..]<.s3L..O<...uf....}'.Rc...4R...C.p5O!<x(...#...M7....S...H../O..O?G.Q!...uf....}'.Rc...4R...C.p5O!<x(...#...M7....d...U..]<.s3L..O<...uf....}'.Rc...4R...C.p5O!<x(... #...M7....d...e...n./bQP..r........:.On....N.......g.oue1b..A..s.P7....k......m..a.`.R%.........`'._&...e....^."f.h!aFx..J..w. E....i...e...n./bQP..r........:.O....-<..,.O70!aFx..N..q.P..m. ....H..)G..\0P."N...BV..."{.O.....-<..1..(O<1H.v..\|.....d.P.....-.@<...{T..c...4....dI.0.....;b....,dR_n+fE..M..v.$B....T.../...`.nM.}..!..........\.Oc...e....^."f.h!aFs..W..f.7B....h......m..a.`. |

### C:\Program Files (x86)\AutoIt3\Include\Security.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | COM executable for DOS |
| Category: | dropped |
| Size (bytes): | 18390 |
| Entropy (8bit): | 6.3663350814781365 |
| Encrypted: | false |
| SSDEEP: | 384:hsUHmeyhpDYNGY3d+qsx+5AUHmAQr+5/8cmpXHukHm9a214iv0UXa8i0hsqQY8NE:IVgtNSY9VWA1b |
| MD5: | 98C47914CDD9067FDC5F78F376A01C47 |
| SHA1: | 3D85354D4AA6C8AC6BEC83EE881B3B6389A46858 |
| SHA-256: | A93E07FF9B4888E161349DB0CB4F82F92F3001BD530E9755C96CC1CC46A51D4D |
| SHA-512: | C232E6F12E37D7F52E470411586437AF6A3C0E1E3F24A50A01CE7F233205A61A8CB60393E39C4A31D318C163811091357340348E79898CAB47FFF140F25F2187 |
| Malicious: | false |

Copyright Joe Security LLC 2023

| | |
|---|---|
| Preview: | ..N\`...*S..<......S.{'9Fx.e..:...A-.^.S'nu..ct...N0P.....0.w.APIError.au3"....; #INDEX# ============================================================ ============================================....1..E:.]\d.2."..7..Z*(.?..(.}.L..y\y.^&o2..]\..pR*\....`5w.n : 3.3.14.5..; Description ...: Functions that assist with Security management...; Author(s) .....: Paul Campbell (PaulIA), tra..EGt..C'.]\d.2.".....3~a[g..;.n._..~A...n f..mk...c..H../{#.========================================= =================================....; #CURRENT# =========================================....1..E:.]\d.2.".....3~a[g..;.n._..~A...n f..mk...c..H../{#. =============..; _Security__AdjustTokenPrivileges..; _Security__CreateProcessWithToken..; _Security__DuplicateTokenEx..; _Securi...`K.9d_..7.\.{.....]&?.(........K- .^.n:yV..p...RR,Z.....w2J.kenInformation..; _Security__ImpersonateSelf..; _Security__IsValidSid..; _Security__LookupAccountName..; _Security__LookupAccoun..I[...XXo.. ,.f.f..q..e6,6(.o..4.4.B6.' |

### C:\Program Files (x86)\AutoIt3\Include\SecurityConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8272 |
| Entropy (8bit): | 6.908627837046587 |
| Encrypted: | false |
| SSDEEP: | 192:eVR1Yaa0uOhLtVgZwwmCIjPC5Y4NgJLv0EY:eWUdWTKjPIY4qJD0R |
| MD5: | 3CFB497B628CA71910F499CB4CA45728 |
| SHA1: | 97D8280700EFCCA36B077466D8EFDD8A0680F078 |
| SHA-256: | A1A048471746983DC741D4A933E132C3E2E1F5C29E6D539D5C60C956B6C81581 |
| SHA-512: | 795648F1AF039DFAB2B5BF9BE7064A7FE603E9A02AAD6C04D06B1D420268DCAA1E19EB986BC2E043DA4859AF46138508A6B0E86CFA6E739BF8A0C97979A6BE C0 |
| Malicious: | false |
| Preview: | PZh...4\|.[..n%...s..r...+...h"..\|.g....._%....I..m...r...+..===========================================================================..; Title ........ .: Security_Constants..; Aut.zrM.."j.[.1..8.f...D.H..;x..$.t......B]..X.....k..<[.Bf...n ...: Constants for Security functions...; Author(s) .....: Paul Campbell (PaulIA), trancexx..; ===============================N.;P..m$....6..+.u...t.N...h"..\|.g....._%....I..m...r...+..=================================....; #CONSTANTS# ====== ======================================================================N.;P..m$....6..+.u...t.N...h"..\|.g.&....y..w.....t....k.bQ...IMARYTOKEN_NAME = "SeAssignPrimaryTokenPrivilege"..Global Const $SE_AUDIT_NAME = "SeAuditPrivilege"..Global Const $SE_BACKUP_NAM6.;M..5[.W..{x...!..\.k.y...7~...._).....!P..s..: .......y.n6..SeChangeNotifyPrivilege"..Global Const $SE_CREATE_GLOBAL_NAME = "SeCreateGlobalPrivilege"..Global Const $SE_CREATE_PAGEFILE_NAM ES.&O...k.U..[I.s.!..k. .....0=...-^8.G.. |

### C:\Program Files (x86)\AutoIt3\Include\SendMessage.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | OpenPGP Public Key |
| Category: | dropped |
| Size (bytes): | 2694 |
| Entropy (8bit): | 7.522035787678073 |
| Encrypted: | false |
| SSDEEP: | 24:V2vNdaWa22T2ZP42T5+nF2hmTkH7i7a0iGixp+wj229g2DC2moE0IZT9LGsLT54r:CNd43kbi7uF+wVg5NRLdL94KZ06hAf |
| MD5: | 08EBD5778DFD33AA9CE0D18B3C19A55A |
| SHA1: | 9F3B8E801798BCD85A960FB058441CDEAB4F6C13 |
| SHA-256: | 454F4AD9431CF6749B2AA11B2430384DC2EE5C4E7F04D38D4C19591F99BF3862 |
| SHA-512: | 7E5A72CCAED44184854F499DCFF911458675B72B8764A53B3F662E52EFE1B1A034F772799E1516DC257BF99BCF1B2259BF44FFE110C5FF7CC0228EE3E99CCB4 6 |
| Malicious: | false |
| Preview: | .J......8.O.L.<..q..\|..f...Hq.....j3....1..*...Y.4.x.9...6P....M\..j...\|....o....mx...Hq.....j3....1..*...Y.4.x.9...6P....M\..j...\|....X.l.$)P...[b.....m..^..A.MdE..._.H.1.M...n..J...JA..d...o.<....._ .1"P...[b.....9i.R.....7`....[}.*.$...1M.V......w.D.5.P..!..k.>!x..V.+.....;}.6..,.KcL...M.'.k.*...j..H........C.5.;...o....mx...Hq.....j3....1..*...Y.4.x.9...6P....M\..j...\|....o....mx...Hq.....j3... .1..*...Y.4.x.9...6P....M\..j...\|...._.....g..k!o.....j3....1..*...Y.4.x.9...6P....M\..j...\|....o....mx...Hq.....j3....1..*...Y.4.x.9...6P....M\..j...\|....o..5.kej..K...C...2....._.Psi....NH.O.$...6P. ...M\..j...\|....o....mx...Hq.....j3....1..*...Y.4.x.9...6P....M\..j...\|....o....mx...Hq.....j3....1..*...Y.4.x...2.0M.e..$(.t...\|....o....mx...Hq.....j3....1..*...Y.4.x.9...6P....M\..j...\|....o....mx...Hq.....j 3....1..*...Y.4.x.9...6`.......w...o....r..T.;H?.h.(.V...y ...."..PE.....Dz.e.C.M.M..P.......0.J...E...r....mx...Hq.....j3. |

### C:\Program Files (x86)\AutoIt3\Include\SliderConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 4578 |
| Entropy (8bit): | 7.835681910651439 |
| Encrypted: | false |
| SSDEEP: | 96:8dqC3kYqC1qCq8VVjrzzJKLSXHW9P2IyVFtX6wk3y3mx/jATsQY2aqCjO:840O7R8LrzzJmSX29PoFe3HATsQY2ZSO |
| MD5: | 9A47FC36BFF97AE1356C65E730CBB0AD |
| SHA1: | B6B4971E0D38C24AEEB194AA016A9DC7E7962204 |
| SHA-256: | 154BA06682935620C18C4B71167D80C9F847873457728C4ABA51E92186F9E7F6 |
| SHA-512: | EA0CB847DEAB807B193598D52C85472B3EB35EC0690771700C098663D6D989AEE568E7A61232E3018BC6E7F30DA1270747D0C7BA64F236E390307B4EA678ECF |
| Malicious: | false |

| | |
|---|---|
| Preview: | ...(.'...,..~. ...v.b7.C*..l\|.._c^LV..SB..I.?).L.C...*..........v.o_..~..&.....k..D.;O..l\|.._c^LV..SB..I.?).L.C...*..........v.o_..~..&.....[..Y.o..Wqo..LpM_E..N,.@..pK.......c........-......!...c..(. ....x.&s.&>.\64...~M_E..@E.l..n}...t...r......,..q.n...1..&.....&.N..o..u.....2..E...\.E..gf.O.+...x.......+....8.+......%.K...;.H..k..Wq"...*.....cu..5.v\|......9......+....*.+B..,..7.....\..D.;O..l\|. ._c^LV..SB..I.?).L.C...*..........v.o_..~..&.....k..D.;O..l\|.._c^LV..SB..I.?).L.C...*..........v.o_..~..&.....k.&s..I......6.-%8..SB..I.?).L.C...*..........v.o_..~..&.....k..D.;O..l\|.._c^LV..SB..I.?). L.C...*..........v.o_..~..&.....k..D.;O.8ja...*..K........wq.Q.=...x......#...g.4...&..v.F..7.NY.v..[7(..B7.Q...N..`..oG...^...u.....'......-.....;.^..".Y...x.^>#..B......J+.j0.A\.?.;..7......,......r ...c..z.D..."J..r...%3...<..K.....F..q4.......v....&....'.<..I..t.K.9.X.."&.q....7.!QV...M..=.gz.......c...... ....$.&...d.o._...;.Y..t\.f9(...-C...... |

### C:\Program Files (x86)\AutoIt3\Include\Sound.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 23262 |
| Entropy (8bit): | 6.520713472074832 |
| Encrypted: | false |
| SSDEEP: | 384:h7Kfik8ru/R1aeN3Pk0Z+tiZeKSbeh08W1nbzEys72oDdy9gwGM6hUn8L59ZTyOd:FK6RaAMPEnKKeO8kbz+72oDdA1QvJyOd |
| MD5: | 6657829B329EDFA043BE34BE0752154B |
| SHA1: | E38DF192A782B342A493A505A998EF0D0589C865 |
| SHA-256: | 3802B9A8D30D6892D916420D4E0F5CDA0DE938371E872F04B280DE45C71A0345 |
| SHA-512: | 874F707870E71CCA933B2C8339CEEE2215CACE3196CE86FE0C2D33D7C2119C6F723591AD031D985CCA42E4B93EEE50F2E4671CB79895E90F0DC8F0A402C9B6 7 |
| Malicious: | false |
| Preview: | $Dx].C{..Q....d...y.%.U...S..t.)....f......S........A.)"..B3"..; Using: _PathSplit..#include "StringConstants.au3"....; #INDEX# ================================ ===========================:.+..."....Y..T..P*.t..D..(....z..AU/.....d...A..^..xJ..Title .........: Sound..; AutoIt Version : 3.3.14.5..; Language ......: English..; Description ...: Functions that assist with ShXxZ.[~..Z....G.?V7.<.Y.V.f....i..\:s.....<....P....$+.gsaltyDS..; Dll ...........: winmm.dll..; ========================================== ==========================================:.+..."....Y..T..P*.t..D..(....z..AU/......z.....=..@..xz...========================================== ==============================================================..Global Const $__SHxXz.yQ...q.;..-.q2Z...t+..5.....s.N.......d...A..^..xz...======= ===================================================================================================....; #CURRENT# =======:.+..."..  ...Y..T..P*.t..D..(....z..AU/. |

### C:\Program Files (x86)\AutoIt3\Include\StaticConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2291 |
| Entropy (8bit): | 7.676983155168195 |
| Encrypted: | false |
| SSDEEP: | 48:DVYEoGUYxVTdVFpuh4Dzl+WhEtF0WIvwhFsr/GE+Ljh9NX24T:lGUUWwBCFZP6GEY24T |
| MD5: | B2D767D2C8F54E884E73B01E64BE185C |
| SHA1: | EABB11EBC598385710D8FA4C0087E9603475DB6C |
| SHA-256: | 82B44ABA8B5D68EA84E2A26A5FE20C72FC9E4165666A93A9C596CCBB1CE37A77 |
| SHA-512: | F229C9AB5D490AB44C2D12ED96D3A5B2835C7591C6DA09F9E5327D17AFFD83F6232E634B23876548506D554E25C846FBC1FCFBC02EF0F930E3A3AF3B7540E38 E |
| Malicious: | false |
| Preview: | ...B.K...#.....W.....QB..3....c'...k...Y....W\.Rv.m*....-..).......[.VpD.$2.`.....(:.......c'...k...Y....W\.Rv.m*....-..).......[.VpD.$2.`.!+..An..v....p4..x....M......B.*.$d...Q].{.....\.F..KwY.7<.l. .....'.}..T.;:..x...!W....l;Tk.5d...dA.z.....NF..(..;!.r.\Q..qn..T..f.'v...>.....[...-4xO(.>c..\l.q....Z.LF..4..j3.<..@..5W.?..V.0:..%.........+.E.$.xd..>........E..!..4Y.k`.).............c'...k...Y. ...W\.Rv.m*....-..).......[.VpD.$2.`.....(:.......c'...k...Y....W\.Rv.m*....-..).......[.VpD.$2.`.....(:.......}Y.......G....W\.Rv.m*....-..).......[.VpD.$2.`.....(:.......c'...k...Y....W\.Rv.m*....-..).......[ .VpD.$2.`.....(:.......T!..4.....Z....l;('.2v....~[.4....k.{F.K}.....1.N@..Vh.g..f..Y......TA......S.'..x..4{.K.......V.Y@s.u`.<..b..fs..@..\|..T..f...#U....J"^.8.p3...\i._.........fG>.vm.1.oN..a'..@.. g..H..v....Q4.....]O..>d...Cw.\....m..[.[5O..H.2.MM.zi.3.f..V.......D.....gkv.$.1{....c\.0....o.i4.&.Y.9?.e.&f..wf..P..F.~>...... |

### C:\Program Files (x86)\AutoIt3\Include\StatusBarConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3530 |
| Entropy (8bit): | 7.781108347567863 |
| Encrypted: | false |
| SSDEEP: | 48:+y6ccolvxP5qyuyXjbwlBOU/PO7kz5bMUwpxpyBqMHvORU1nUy/w7Kc9:+yhvOyuyXWoYvMUwHMHzBUy4Oc9 |
| MD5: | 9E2EB070D21B9F4E9EB08A3A1F09C795 |
| SHA1: | B2755EFAC9481316482E53C8DD6BC7A5BC164648 |
| SHA-256: | 2412AD11F8CD2A4F610691B836F4CDE74F0C2961872FDC4FC71D0440F47C86E4 |
| SHA-512: | 1246CE80474685E96A002CC35B00B2BA4DB870C36A7A0E5ADBB6EE26978FAF52CBE41E3E684DB8F4521A766B68FC0151196749325C04033F206BCDF95F05CDD 5 |
| Malicious: | false |

| | |
|---|---|
| Preview: | ..4....O..."O.C..u..o...p.*.m.........P[X..Cs..Vi_F..P..#.O....g..Q._.S.z..s..h.......m.*.m.........P[X..Cs..Vi_F..P..#.O....g..Q._.S.z..s..X....S..5.9.~........D......<...:........R......:......gx.}.. {....7..p.v.7........C\E..."I..Yh@.....l.....z..B.!...3#.:..3...N..%.U.".....Y..CCko..?;T..&J...C..0.H....3..L....N.5-.:..{..,....m.*.m.........P[X..Cs..Vi_F..P..#.O....g..Q._.S.z..s..h.......m.*.m.. .......P[X..Cs..Vi_F..P..#.O....g..Q._.S.z..s..h.......].,.s....~...M[X..Cs..Vi_F..P..#.O....g..Q._.S.z..s..h.......m.*.m.........P[X..Cs..Vi_F..P..#.O....g..Q._.S.z..s..h.......m.*.Z....U.: *.....nc..'.[../..M.!......L.R._.wO...\7...U..$.3......d..cM[E..F~..a........q........?..-."....n..e....7..Z.7........w..R..E...=T.O. /..8..[.R....j..(......JH.".Q4..b.T..p.D......t..cM[E..O~..P...... ..>.....-.........g .<.V'..,.}..2.{........c..o=)5..*n..[,PK..V..v.R...z.L......0+.&.Ru.S.\_.$.7. ....Y..U.F....nT..t.......x......3....o.).( .".p:.U......E......w.. |

### C:\Program Files (x86)\AutoIt3\Include\String.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 8624 |
| Entropy (8bit): | 6.203096138769738 |
| Encrypted: | false |
| SSDEEP: | 192:bdOe2ev+PaKF3mhLQmzRuiYdAw5GIR94W9z:bdOeT+SKF3QQmzRnYdAw5GIH4Wx |
| MD5: | DE5881B860CEF8A747E4948992CDC2B3 |
| SHA1: | EB1A53DD5611BF54FF65AD28F34A7C0E28AB41CA |
| SHA-256: | 7610D8A9392B2F8A10CD56CE200327278D1BF9364713EC5B6B30254F939A69E2 |
| SHA-512: | 233BC9E12C8BD4BD9927A36F4197BB5C78120473514A35166E70C6ABD94670C0AF9BF2F382E7FB2A96659EC9540E532EDBC50EABBFF9148900A96DDF95175DFD |
| Malicious: | false |
| Preview: | ....h....h...;..9l{@W..y.p7.n.6'\..s..\#....?....:....qr..V=========================================================================================== ========================..; Title ......."...de..;.../tamF.gO.q7.g.ci.S.3kX\w.....W..J.....,r\|..Q Functions that assist with String management...; Author(s) .....: Jarvis Stubblefield, SmOke_N, Valik, Wes Wolfe-Wolvereness, W... ..~+..C..2,.nV.s.RH;.l. ic..y?.^b....X..\.S"..5.3.b#, guinness..; ==================================== ==================================================================================......1....0...;....U\vw.e.R?c.4.dt.@. gQO..........N]...oo. .V====================================================================================..; _HexToString..; _StringBetween..; _StringE........yy.V..? rz)8..u!v,.g..;@..oWflb...\..].....Hir...ringTitleCase..; _StringToHex..; ====================================================================== ========================......1....06......g=3.....O?c...TC.].[ |

### C:\Program Files (x86)\AutoIt3\Include\StringConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 3168 |
| Entropy (8bit): | 7.754676693402763 |
| Encrypted: | false |
| SSDEEP: | 96:ozTk5gMeozL/FgA85umqYWLpNiMWqeLM9:jgMeGV85XqYXLk |
| MD5: | 61994A28BAA0A0D14F452E60541F8B1A |
| SHA1: | CAD410D8CA51CE99A41F43C6E5B197B7B3B01B95 |
| SHA-256: | 34789A9188C50EDDC1AB1B1593D58255E17A1E54A7E9290B521F8CAAA7424D14 |
| SHA-512: | 34CF35AA4A65BDF40EAFD9D3E1F8A3C026369C20AD338D224BE4FF9990CC6296B2D8EFE73424F5BDC53F987D8BF38AD6A597AC80E4FE9E13BCEB346353BD88D3 |
| Malicious: | false |
| Preview: | %.P3.}..{%?xn.....\|...[..V.......:.....-...Kp..J..%.4Za..D.B.;.;..m.5[.kwl&6..!..a.yi".mH.......:.....-...Kp..J..%.4Za..D.B.;.;..m.5[.kwl&6..!..Q..tK.$.......).....C...*.p...l.g./..B....i.r.h5.{..8jk; 8..2..r.l^$......U..).....*...!.@...#.M./.......h.(..j.K..%>0u...h..>.d=q.<........fF.......~.@...h.).4..Y....a.U.L9.oF.#$2ob..o..V.d.j.8.......)....e...>..W..u..\\|..D.B.;.;..m.5[.kwl&6..!.. a.yi".mH.......:.....-...Kp..J..%.4Za..D.B.;.;..m.5[.kwl&6..!..a.yi".mH.......:.....-...Kp..J..%.4ZQ..s.\.I.U....[E.kwl&6..!..a.yi".mH.......:.....-...Kp..J..%.4Za..D.B.;.;..m.5[.kwl&6..!..a .yi".mH.......:.....-...Kp..J..%.4Za..D.u.&.r.W>.K..&+#~'.h..2..:L."Y...F..YUM...u...>.R.....2G........u.o..#.z..1j>kn..h..2.d'w.%...Q.._tM....c...(.90..z.eG......[.R.Y.q..[#....^+..,..\|.+ ? .1...Q..WsA....t...!..z..t.k.0......".R.a..[#....^+..-..\|.%'z.#....@..[."...q...#.GW..L.V)...*..:.U.D.m..([.djj;E..<../.d'z.#....Q..KtA...0.....P...y.`.3..s.D.U.t.P7.\|..&..;H..o..2.7Y..p<...W..[t....d |

### C:\Program Files (x86)\AutoIt3\Include\StructureConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 64599 |
| Entropy (8bit): | 5.547525183690798 |
| Encrypted: | false |
| SSDEEP: | 384:c6vAyZcqjkLmz6be22gnlzHlrQLCgzihSW0ciYiTyQDG1zkjSGidJxOEJMWGTiIa:pvtUZs3qrWzPgbnGJs/rpnU8RwnuPR1 |
| MD5: | 338A2D1F44487405B231D8C2A35A2539 |
| SHA1: | 6FCB6FA68E273E9FF4697C13C177F17B46C043FA |
| SHA-256: | 91DAE519F1FABAC666412B5CF1A5F8EC23FF522C1A1DD6DF6878697DAE81F59D |
| SHA-512: | B93E10F31F96A88700A4ECFACC08369E7F442620962B2A07269769D74D3E96EB8C28A3407B64C6694C6421D3963224D5C4BA8251EDB37EC3403B980F35BBF3FE |
| Malicious: | false |

| | |
|---|---|
| Preview: | g'..nk.&b.G&.....P...W.NCO.$..J.h.M...w...D*a{F..@..F...E..=========================================================================================..; Title .........: Structures_Constants..; A1:..v>2&=.@*.. ..].....U^6]j....<.....d.....d('..S].E.....S.ws API functions...; Author(s) .....: Paul Campbell (PaulIA), Gary Frost, Jpm, UEZ. .; ==========================================ys..?#Y~r..x..'..N...2.SCO.$..J.h.M...w...D*a{F..@..F...E..=======================....; #LISTING# ========= ==========================================================================ys..?#Y~r..x..'..N...2.ctl.=..'...$2..j....+R..v..].^.Q..*p.NS..; $tagSIZE..; $tagFILETIME..; $tagSYSTEMTIME..; $tagTIME_ZONE_INFORMATION..; $tagNMHDR..; $tagCOMBOBOXEXITEM..; $tagNMCBEDRA....KPilt..1..T...6. ..F.ctl.=..9...=}......s,\|b..G9.z)w..=:.; $tagNMDATETIMECHANGE..; $tagNMDATETIMEFORMAT..; $tagNMDATETIMEFORMATQUERY..; $tagNMDATETIMEKEYDOWN..; $tagNMDATETIMESTRING..; `:..GH!...f...Y....y...n.):;hF..2...1m |

### C:\Program Files (x86)\AutoIt3\Include\TabConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 6507 |
| Entropy (8bit): | 6.641337848225666 |
| Encrypted: | false |
| SSDEEP: | 192:iQrUQasRgBCE0RDymSCuBkTcYQ6ZzClrAVNiEL:ieVZRXqMTclpdAPiC |
| MD5: | 5557852C7A6CE4AC47F97F875BC35AA2 |
| SHA1: | 49FA91A338CAA02240CE4099FB9319A8181671D0 |
| SHA-256: | 44DB89F9B898D1613686AA3EEE535195209D02B1F2AF8DD925E03B5D3D106E2E |
| SHA-512: | 5BAD0FFB427EED82583092EEDE54A112C7354FBC068417C501DB4EC1765847EE0AAB4FB246867D70B9ACDC4B74FE7FFF945499C145B6BAE9BF0BB183CCE218E4 |
| Malicious: | false |
| Preview: | $M..cG.~............*}........E.j.".V...a....W.{...l....)c..o======================================================================..; Title .........: Tab_Constants..; AutoIt VbV..`\.!...........C....%...V.y.1.K..P0U...`...O..#..VV{0..\|: <a href="../appendix/GUIStyles.htm#Tab">GUI control Tab styles</a> and much more constants...; Author(s) .....: Valik, Gary FrhW../..5....=....^..........E.j.".V...a....W.{...l....)c..o============================================================ ============....; ================================================:...2..&....=....^..........E.j.".V...a....W.{...l....)c..o================....; #EXTSTYLES# == =========================================================================================:...2..&....=....^>....#....$V?.?..h.d..+...z.....pl4c...b0000001 ; The tab control will draw separators between the tab items..Global Const $TCS_EX_REGISTERDROP = 0x00000002 ; The tab chJ..`^.\|.......s.n<t.........#Ky@... |

### C:\Program Files (x86)\AutoIt3\Include\Timers.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 12166 |
| Entropy (8bit): | 6.382556446120079 |
| Encrypted: | false |
| SSDEEP: | 192:ULjJ7aK2BxIdD9lHH3CzvOl8ah1l2klefo7ljze0S6Rfqe+fUq9PtxOiekhcDvqs:ULjIKZdRl3Tl8Qevo7lrqCoEoEoQHV |
| MD5: | B846C13113983FBBD88F8CF73858BDAE |
| SHA1: | 1403130E0DCD03CC3F18AA0694F65CDCE3ABFB6F |
| SHA-256: | A9875BA42880BDEE2A4D0C3A032F5723E5A67582361135CE89E97FED5A0F9BE7 |
| SHA-512: | 21D1DE818FF91E486AF6D995DD8CAEEE44361AA5A2173F569D48968B00A73AC0B46ECA0F02A7DB46051EE7DA976C7FB63C83374345E7A4FE4F91E607E9CC966B |
| Malicious: | false |
| Preview: | .....6pz........3z&..I.(.............8)+w..IY#...,c.A.g.v.B=================================================================================..; Title .........: Timers..; AutoIt Version .OCK.m%+......p.f8...".%.......N..D.$...Aqe)....w..?p.F..G%\.ions that assist with Timers management...; An application uses a timer to schedule an event for a window after..P..&wv......{.{8...`.{..............%46j..TD>...y~\..?.?W. specified interval (or time-out value) for a timer elapses, the system notifies the window..; associated with ...E.*yz.....m.38O.a.y......[..N.M.Xkpej..T.v..h-\..zQ'P.k rate and how often the..; application retrieves messages from the message queue, the time-out value is only a.....*y~.......k.{6...%.%.......H....[.I..-j..IY#...,c.A.g.v.B=============================================== ===========================================================....; #VARIABLES# =.RMX.~)".....#..dR..1.6........... |

### C:\Program Files (x86)\AutoIt3\Include\ToolTipConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5840 |
| Entropy (8bit): | 6.653169009437166 |
| Encrypted: | false |
| SSDEEP: | 96:vYCJ3kJ3iZNtgwuxPKdTm7VMd7cOoyYkptchUCC:vYCVkViXtgwuxPKdT8eWSNSUCC |
| MD5: | 4DFB2702A30AB1F3CB8B6DB594031562 |
| SHA1: | 23C06B4B48BA1E87E261D88C809F05C2E9F59F02 |
| SHA-256: | 92DC72B0517092A7CAC0CE0D0392B795CBB90FCC63A2D00DAFFE2DE4C26EAEB6 |
| SHA-512: | E391C982AEBE3D76B0868D0DBCE1E7A22E2E608652BE40D14CA13544D2203CAB0169927F7686E3A686F69558A4778D12457A32483BBA0216E43230415481EA45 |
| Malicious: | false |

| | |
|---|---|
| Preview: | ..i.A.y.OB6....H..mQig.a..mm.j.....P6`...j4..T^.wf.e..1c...U.=====================================================================================..; Title .........: ToolTip_Constants..; Auto..'&H.n..Cx..6.3l....'....N7%.0.....C%g.~@0e...n<q{.=U.~7..... ...: Constants for ToolTip functions...; Author(s) .....: Valik, Gary Frost, .....; ==========================================..:M.. ._.e..8.=...."......mm.j.....P6`...j4..T^.wf.e..1c...U.=====================....; #CONSTANTS# = ======================================================================================..:M.. ._.e..8.=...."...O.g<?.6....^..+ygoh.@..:+a. ..e..tn...X.01..Global Const $TTF_CENTERTIP = 0x00000002..Global Const $TTF_RTLREADING = 0x00000004..Global Const $TTF_SUBCLASS = 0x00000010 ..@.B.\|.Bn7.q.$....pMla.b..`(.g.....`.._TL6e....E>{..r.S....$.TE = 0x00000080..Global Const $TTF_TRANSPARENT = 0x00000100..Global Const $TTF_PARSELINKS = 0x00001000..Global Const $TTF_DI_SET..B=..=...h..=.0r..$.o.1.A75.Z...R..+ |

### C:\Program Files (x86)\AutoIt3\Include\ToolbarConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 14047 |
| Entropy (8bit): | 6.819041615709756 |
| Encrypted: | false |
| SSDEEP: | 384:+QsXVsKM2O3hBfzTKLcCZBsaetBluVEfENi+gs0:QX6p2O3hBfsTqPluVEfENik0 |
| MD5: | 81D86879D8BFF245555E59E78DC7A461 |
| SHA1: | 3767A5A9111C7865B106BA17C3911A7DA6CCDD41 |
| SHA-256: | 8543E8E80999522CE567AA0CF652A8C339AC7DFBAE4186D60A9171A30CD9FFEF |
| SHA-512: | 7A7FD773F64B9E2172BBF8FE6093BF9F9C01E71788FE9CFDD8C352506A881676FFE8C942D020B88F1E84727488C28DFFB38F1F500E5C2D616AC70E10AD2256C |
| Malicious: | false |
| Preview: | ..R.x.V#...!:.Z........;;..7...Y3.D.Wt7cn.....i.5...ph.W.zd..=====================================================================================..; Title .........: Toolbar_Constants..; Auto....q.A/..x..~.*....P.CT.m..H...W..Dg0~..M.z.<.....(&...7-.. ...: Constants for Toolbar functions...; Author(s) .....: Valik, Gary Frost, .....; ==========================================....)H.{....b.m.9....g.^%..7...Y3.D.Wt7cn.....i.5...ph.W.zd..=====================....; #CONSTANTS# ==== ======================================================================================....)H.{....b.m.9....g.^...f..N.......i....l.Z...M...}-.Z.wi....Global Const $TBIF_TEXT = 0x00000002..Global Const $TBIF_STATE = 0x00000004..Global Const $TBIF_STYLE = 0x00000008..Global Con...@7{.........9....j.S(....C.l... ..'y*s.~.Z...G.v....W.w!..00020..Global Const $TBIF_SIZE = 0x00000040..Global Const $TBIF_BYINDEX = 0x80000000....Global Const $TBMF_PAD = 0x00000001. .Glo.P.W.\5........Fi...z.C(..:...T>.t...& |

### C:\Program Files (x86)\AutoIt3\Include\TrayConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2976 |
| Entropy (8bit): | 7.7697352110078715 |
| Encrypted: | false |
| SSDEEP: | 48:DCauUcWvfHmC9/Bca2yooO9j+mEBpphocjVjskUQqpcZkqyXgi7uM:ma+WWC1BqLS7fjVAxpcZkRz |
| MD5: | 1AC36A51DD9DDEAAEB1A4EFAF8FED8AA |
| SHA1: | E997E0D2EC81F963FDA3B1EBC809BF1170AE16D4 |
| SHA-256: | 1E71A65B50601FE50219C056ADDCF04DB747A576AF8A360F6C57BECF45225C49 |
| SHA-512: | 9DAD6291D073181E656EA375885BBB99D6B3D296B036232FC7C8060A29F35202E7A52A1A4B66E291CA320454C54297992FECBF09E289D567BF3A126F6B1B409F |
| Malicious: | false |
| Preview: | p.R.K.....}.5.Cc~t..`.....rPgH.[....{.kp....D....;......X....n........@P#X..sTxi..........rPgH.[....{.kp....D....;......X....n........@P#X..sTxY...L..H3.aCt[.H.....8>B....0 ..G.BN...3....<.. ......LY0P5.uI.5...B...=.aCtO.#..5.[G....^XMCr.YO...K...=.H.J....M\|... .)!...L..L}...........5.$$F..s..eFr.YS..E....}..._....A>+M.=. &....G..~..(Az=......f.xc;...D....;......X....n........@P #X..sTxi..........rPgH.[....{.kp....D....;......X....n........@P#X..sTxi..........rPgH.[....{.kp....s0 ..%.yo...+....n........@P#X..sTxi..........rPgH.[....{.kp....D....;......X....n........@P#X..sTxi ..........rPgH.[....{.kp....D...>..<......6.Y.P...4)9.5...*6...J..Y3..?.,./..........t7mH\d.Z...........e.j...-,K6}.slqY....G...P.!..U.2......i..*i...1.<,...1....>.R..W...].j.L.n.$8.../..Bq.#M........ ..u..2xn..&.;+.......<.O......$2K+{..*.........j..-.6U.....b...o..8.fa.;..........s.S.J.../,G:\|..(......... ..#.8..F..2.r.d..?riq`&......o....2...P...Y9L$a..,..........!.E`PN.2...# |

### C:\Program Files (x86)\AutoIt3\Include\TreeViewConstants.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 9715 |
| Entropy (8bit): | 6.7509168396685455 |
| Encrypted: | false |
| SSDEEP: | 192:gMVkQUigi7Cc6pNXchhFU+6ZxEWmd2DhejiWTdBhANpG:gMiQUDEx6NshhFUTnEWI2DUWWTdBaa |
| MD5: | 9C1A84718BDE8A33B326AEA0A24E12EF |
| SHA1: | 7199146AA62729E5352D40C649C57BBA144B6076 |
| SHA-256: | A241449FA191C8149FCB0F0E808378032F6EAB69DC2E620864BD16D3A987E1F4 |
| SHA-512: | 4CCD3AB2DFF27A057A049DC6C5E316B378A7A9B3840B248F2509D8B5DCAA2EB26393B94A908FF8A50B7577DE94748A544C80EE3A39EC6205AD3E5DD6133F75 5A |
| Malicious: | false |

| | |
|---|---|
| Preview: | .y..........N.Z&KX...f.j..(.yx....FdM...dGI,..:......4..E.b==========================================================================================..; Title .........: TreeView_Constants..; AutHY...._..T.c.y.^I.../....t.#0....Uw^...y?.v..o....jl...D0n ...: <a href="../appendix/GUIStyles.htm#TreeView">GUI control TreeView styles</a> and much more constants...; Author(s) .....:.F......q......8_.T.....8..(.yx....FdM...dGI,..:......4..E.b========================================================================================================....; #CONSTANTS# =====================.-K.......I.~.j.ME........(.yx....FdM...dGI,..:......4..E.b=================================..; Styles..Global Const $TVS_HASBUTTONS = 0x00000001 ; Displays plus (+) and minus (-) buttons nBh....W....c.#I.....N.P.5.++.../.#....3:T...'......9...C..ses lines to show the hierarchy of items..Global Const $TVS_LINESATROOT = 0x00000004 ; Uses lines to link items at the root of tOuV....Y.~./.5M.X...Q....C......r:.5. |

### C:\Program Files (x86)\AutoIt3\Include\UDFGlobalID.au3

| | |
|---|---|
| Process: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 7003 |
| Entropy (8bit): | 6.537506045115929 |
| Encrypted: | false |
| SSDEEP: | 96:nMgyu/PJGiukQryzyHuAKLZnEeNZi3Hr22xyo7CY:Mgyu3J1ukD4mLZEeNZi39ApY |
| MD5: | D94CB8D758186C40A2E1C5894C22DF9F |
| SHA1: | 69E588184BE32D9944E1756000455294A4FC4364 |
| SHA-256: | CED85D11BC4774921B43D6F4158A5E87E740E44CA0A128F899F2867C0F702BFA |
| SHA-512: | A8BBB5E1A6C44E267BD24271811617B89F7917663001E78FCC5B94F82D239E016998A4087C667D69A036A604BF7B9DCE81DDDD41E707CBCA9FC658684051BEEA |
| Malicious: | false |
| Preview: | ..E....PeTk(A..z..*..6...K8...M.I....c.;?t=....'...:)...o===================================================================================================================..; Title .......]_~Nm.~........ah...J#.!.X.U...L*.idt1.....?...!.....r......: English..; Description ...: Global ID Generation for UDFs...; Author(s) .....: Gary Frost..; ============================.....@7.5pq/.M..t..Vn....q.h.3...Z..Q-.gwz".....9...r_7.o=========================================....; #CONSTANTS# ===========================================================================.....@7.5pq/.M..t..Vn....q.h.3...Z..Q.3.&(}.....w...7N...>obalIDs_OFFSET = 2..Global Const $_UDF_GlobalID_MAX_WIN = 16..Global Const $_UDF_STARTID = 10000..Global Const $_UDF_GlobalID_MA..b....H?.;xA..z...+..K...Jl...[.a.2.#^j...K.....F...B7...b0010000..Global Const $__UDFGUICONSTANT_WS_VISIBLE = 0x10000000..Global Const $__UDFGUICONSTANT_WS_CHILD = 0x40000000..; =======.....@7.5pq/.M..t..Vn....q.h.3...Z.. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.044268283359809 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.94%<br>• Win16/32 Executable Delphi generic (2074/23) 0.02%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | HkObDPju6Z.exe |
| File size: | 1489920 |
| MD5: | 6441d7260944bcedc5958c5c8a05d16d |
| SHA1: | 46257982840493eca90e051ff1749e7040895584 |
| SHA256: | 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224 |
| SHA512: | af88fd3a0a2728c811be524feee575d8d2d9623b7944021c83173e40dbec6b1fbe7bea64dcdd8f1dbebc7d8df76b40e5c9647e2586316ea46ceb191ebcf14d89 |
| SSDEEP: | 24576:1p2gwjk6ikYhJ9lvGnYZvy48/V33ck7LnBAyldFu8hod/Qodly:1AgxkmvGnYWccjBAwFadRd |
| TLSH: | 9B65D000B680C036FA722870556AABB2897EBC30976555CF23C43D7B6E726D19D3672F |
| File Content Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......PE..L......W.....................L.......7............@..........................P............@................................ |

## File Icon

| | |
|---|---|
| Icon Hash: | 3fc7a3c665f3c37d |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4237d9 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |

| | |
|---|---|
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, 32BIT_MACHINE |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x5717C407 [Wed Apr 20 18:01:43 2016 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: | e7481059b799ac586859298d4788584d |

### Entrypoint Preview

| Instruction |
|---|
| call 00007F8B78D9ABFDh |
| jmp 00007F8B78D9A358h |
| retn 0000h |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov eax, dword ptr [eax] |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov eax, dword ptr [eax] |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp eax, ecx |
| jnbe 00007F8B78D9A533h |
| int3 |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp eax, ecx |
| jnbe 00007F8B78D9A537h |
| push 00000041h |
| pop ecx |
| int 29h |
| pop ebp |
| ret |
| retn 0000h |
| push ebp |
| mov ebp, esp |

| Instruction |
|---|
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp eax, ecx |
| jnbe 00007F8B78D9A543h |
| cmp dword ptr [0047E620h], 00000000h |
| je 00007F8B78D9A53Ah |
| mov eax, dword ptr [0047E620h] |
| pop ebp |
| jmp eax |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| cmp dword ptr [0047E620h], 00000000h |
| je 00007F8B78D9A53Ah |
| mov eax, dword ptr [0047E620h] |
| pop ebp |
| jmp eax |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov eax, dword ptr [ebp+08h] |
| mov edx, 0048E840h |
| mov ecx, 0048E840h |
| sub eax, edx |
| sub ecx, edx |
| cmp ecx, eax |
| sbb eax, eax |
| inc eax |
| pop ebp |
| ret |
| push ebp |
| mov ebp, esp |
| mov ecx, dword ptr [ebp+08h] |
| mov eax, ecx |
| sub eax, dword ptr [ebp+0Ch] |
| sub eax, 0000E800h |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x90c70 | 0xf0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x11e000 | 0x50378 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x16f000 | 0x5110 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x8e780 | 0x70 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x8e880 | 0x18 | .rdata |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x85578 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x90b68 | 0x40 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x7c9ea | 0x7ca00 | False | 0.41879348984453363 | data | 6.631020869912357 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x7e000 | 0x14e72 | 0x15000 | False | 0.5792178199404762 | data | 6.1426369171952455 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x93000 | 0x8a5b0 | 0x84800 | False | 0.9093639445754716 | data | 7.357984406581138 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0x11e000 | 0x50378 | 0x50400 | False | 0.501323379088785 | data | 5.824284929352815 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x16f000 | 0x5110 | 0x5200 | False | 0.784108231707317 | data | 6.756606998856607 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_CURSOR | 0x147588 | 0x134 | Targa image data 64 x 65536 x 1 +32 "\001" | English | United States |
| RT_BITMAP | 0x1476d8 | 0x3c28 | Device independent bitmap graphic, 240 x 16 x 32, image size 15360, resolution 3779 x 3779 px/m | English | United States |
| RT_BITMAP | 0x14b300 | 0x428 | Device independent bitmap graphic, 16 x 16 x 32, image size 1024, resolution 3779 x 3779 px/m | English | United States |
| RT_ICON | 0x11ec00 | 0x1011a | PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced | English | United States |
| RT_ICON | 0x12ed20 | 0x10828 | Device independent bitmap graphic, 128 x 256 x 32, image size 67584 | English | United States |
| RT_ICON | 0x13f548 | 0x4228 | Device independent bitmap graphic, 64 x 128 x 32, image size 16896 | English | United States |
| RT_ICON | 0x143770 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 9600 | English | United States |
| RT_ICON | 0x145d18 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x146dc0 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 1088 | English | United States |
| RT_ICON | 0x147288 | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512, 16 important colors | English | United States |
| RT_ICON | 0x14baf8 | 0x10828 | Device independent bitmap graphic, 128 x 256 x 32, image size 0 | English | United States |
| RT_ICON | 0x15c320 | 0x4228 | Device independent bitmap graphic, 64 x 128 x 32, image size 0 | English | United States |
| RT_ICON | 0x160548 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 0 | English | United States |
| RT_ICON | 0x162af0 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 0 | English | United States |
| RT_ICON | 0x163b98 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 0 | English | United States |
| RT_ICON | 0x164050 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x165110 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x1661d0 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x167290 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |
| RT_ICON | 0x168350 | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512, 16 important colors | English | United States |
| RT_ICON | 0x168650 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 4224 | English | United States |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x169710 | 0x2e8 | Device independent bitmap graphic, 32 x 64 x 4, image size 512, 16 important colors | English | United States |
| RT_MENU | 0x169a10 | 0x53e | data | English | United States |
| RT_DIALOG | 0x169f50 | 0x1a8 | data | English | United States |
| RT_DIALOG | 0x16a0f8 | 0x1b0 | data | English | United States |
| RT_DIALOG | 0x16a480 | 0x1dc | data | English | United States |
| RT_DIALOG | 0x16a660 | 0x1dc | data | English | United States |
| RT_DIALOG | 0x16a840 | 0x130 | data | English | United States |
| RT_DIALOG | 0x16aaa0 | 0x210 | data | English | United States |
| RT_DIALOG | 0x16a2a8 | 0x1d4 | data | English | United States |
| RT_DIALOG | 0x16a970 | 0x130 | data | English | United States |
| RT_DIALOG | 0x16bbe0 | 0x560 | data | English | United States |
| RT_DIALOG | 0x16c140 | 0x244 | data | English | United States |
| RT_DIALOG | 0x16acb0 | 0x4a2 | data | English | United States |
| RT_DIALOG | 0x16b158 | 0x4ae | data | English | United States |
| RT_DIALOG | 0x16b608 | 0x3ba | data | English | United States |
| RT_DIALOG | 0x16b9c8 | 0x218 | data | English | United States |
| RT_STRING | 0x16c928 | 0xa6 | data | English | United States |
| RT_STRING | 0x16d510 | 0x1e0 | Matlab v4 mat-file (little endian) i, numeric, rows 0, columns 0 | English | United States |
| RT_STRING | 0x16d738 | 0x1b0 | data | English | United States |
| RT_STRING | 0x16c800 | 0x124 | data | English | United States |
| RT_STRING | 0x16c9d0 | 0xb3e | data | English | United States |
| RT_STRING | 0x16c388 | 0x478 | data | English | United States |
| RT_STRING | 0x16d6f0 | 0x48 | data | English | United States |
| RT_ACCELERATOR | 0x14b728 | 0x1a0 | data | English | United States |
| RT_GROUP_CURSOR | 0x1476c0 | 0x14 | Lotus unknown worksheet or configuration, revision 0x1 | English | United States |
| RT_GROUP_ICON | 0x147228 | 0x5a | Targa image data - Map 32 x 282 x 1 +1 | English | United States |
| RT_GROUP_ICON | 0x1650f8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x168638 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x167278 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x168338 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x1696f8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x1661b8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x1699f8 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x147570 | 0x14 | data | English | United States |
| RT_GROUP_ICON | 0x164000 | 0x4c | data | English | United States |
| RT_VERSION | 0x14b8c8 | 0x22c | data | English | United States |
| RT_MANIFEST | 0x16d8e8 | 0xa90 | XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (2644), with CRLF line terminators | English | United States |

## Imports

| DLL | Import |
|---|---|
| SHLWAPI.dll | PathGetDriveNumberW, StrCmpNIW, StrDupW, StrChrA, PathRelativePathToW, PathIsPrefixW, PathFindFileNameW, PathUnExpandEnvStringsW, PathIsRootW, PathCanonicalizeW, PathFindExtensionW, PathCommonPrefixW, PathCompactPathExW, PathRemoveExtensionW, StrFormatByteSizeW, PathStripPathW, PathRemoveBackslashW, StrRetToBufW, PathMatchSpecW, StrCatBuffW, PathUnquoteSpacesW, StrChrW, StrTrimW, SHAutoComplete, StrCpyNW, PathQuoteSpacesW, PathRenameExtensionW, PathIsDirectoryW, StrRChrW, PathAppendW, PathIsRelativeW, PathFileExistsW, PathAddBackslashW, PathRemoveFileSpecW, PathIsSameRootW |
| PSAPI.DLL | EnumProcessModules, GetModuleFileNameExW |

| DLL | Import |
|---|---|
| USER32.dll | OffsetRect, OpenClipboard, BeginDeferWindowPos, GetSubMenu, TrackPopupMenu, LoadAcceleratorsW, DeleteMenu, ShowOwnedPopups, CopyImage, MessageBoxW, EqualRect, IsWindowVisible, ShowWindowAsync, GetMessagePos, LoadMenuW, CharUpperW, GetKeyState, DefWindowProcW, GetMenuItemInfoW, DeferWindowPos, GetMessageW, CloseClipboard, SetMenuItemInfoW, EmptyClipboard, RegisterClassW, SetWindowPlacement, FrameRect, SetMenuDefaultItem, EnumWindows, GetMessageTime, IntersectRect, SetFocus, BringWindowToTop, TranslateAcceleratorW, GetWindowDC, EndDeferWindowPos, SetClipboardData, CheckMenuItem, IsZoomed, KillTimer, PostQuitMessage, GetSysColorBrush, EnableMenuItem, RegisterWindowMessageW, UpdateWindow, IsIconic, GetWindowThreadProcessId, DrawAnimatedRects, FindWindowExW, GetDC, MonitorFromRect, SetActiveWindow, LoadStringA, SetWindowTextW, LoadStringW, DdeCreateStringHandleW, DdeConnect, GetMonitorInfoW, DdeInitializeW, SetTimer, SetWindowCompositionAttribute, SystemParametersInfoW, SetPropW, RedrawWindow, SendMessageW, wsprintfW, GetSysColor, CharPrevW, GetWindowPlacement, GetSystemMetrics, DdeUninitialize, DialogBoxIndirectParamW, DdeClientTransaction, SetLayeredWindowAttributes, CharUpperBuffW, SetRect, DdeDisconnect, SetForegroundWindow, LoadImageW, ReleaseDC, GetPropW, RemovePropW, DispatchMessageW, PeekMessageW, TranslateMessage, GetWindowLongW, GetWindowTextLengthW, GetSystemMenu, AdjustWindowRectEx, PostMessageW, CheckMenuRadioItem, GetWindowRect, GetFocus, DestroyWindow, SetWindowPos, CheckRadioButton, MessageBoxExW, CreateWindowExW, EndDialog, MessageBeep, CreatePopupMenu, WindowFromPoint, DestroyCursor, ShowWindow, DestroyIcon, GetDlgCtrlID, SetDlgItemTextW, MapWindowPoints, GetDlgItemTextW, SendDlgItemMessageW, IsWindowEnabled, IsDlgButtonChecked, DestroyMenu, GetMenuStringW, CharNextW, LoadIconW, LoadCursorW, GetClassNameW, SetCapture, InsertMenuW, SetCursor, SetWindowLongW, TrackPopupMenuEx, GetComboBoxInfo, GetClientRect, GetDlgItem, AppendMenuW, CheckDlgButton, GetParent, ReleaseCapture, InvalidateRect, ChildWindowFromPoint, GetCursorPos, EnableWindow, GetWindowTextW, DdeFreeStringHandle |
| KERNEL32.dll | RaiseException, GetSystemInfo, VirtualQuery, GetModuleHandleW, LoadLibraryExA, EnterCriticalSection, LeaveCriticalSection, DecodePointer, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, WaitForSingleObjectEx, ReadConsoleW, GetConsoleMode, VirtualProtect, CompareStringOrdinal, FreeLibrary, LoadLibraryExW, ReadFile, lstrlenW, WriteFile, lstrcpynW, ExpandEnvironmentStringsW, GetModuleFileNameW, SetFilePointer, SetEndOfFile, UnlockFileEx, CreateFileW, GetSystemDirectoryW, MultiByteToWideChar, lstrcatW, CloseHandle, LockFileEx, GetFileSize, WideCharToMultiByte, lstrcpyW, lstrcmpiW, lstrcmpW, FlushFileBuffers, GetShortPathNameW, LocalAlloc, GetFileAttributesW, SetFileAttributesW, FormatMessageW, GetLastError, GetCurrentDirectoryW, LocalFree, WaitForSingleObject, CreateEventW, SetEvent, GlobalAlloc, GlobalFree, ResetEvent, SizeofResource, SearchPathW, GetLocaleInfoEx, FreeResource, OpenProcess, LockResource, LoadLibraryW, LoadResource, FindResourceW, GetWindowsDirectoryW, GetProcAddress, GlobalLock, GlobalUnlock, MulDiv, CreateDirectoryW, FindFirstFileW, GetCommandLineW, SetErrorMode, FindClose, GetUserPreferredUILanguages, FindFirstChangeNotificationW, GetVersion, ResolveLocaleName, GlobalSize, FileTimeToSystemTime, FindCloseChangeNotification, LoadLibraryA, FileTimeToLocalFileTime, FindNextChangeNotification, SetCurrentDirectoryW, GetTimeFormatW, ExitProcess, VerSetConditionMask, CopyFileW, VerifyVersionInfoW, GetDateFormatW, MapViewOfFile, CreateFileMappingW, LocaleNameToLCID, FindResourceExW, LCIDToLocaleName, UnmapViewOfFile, GetVersionExW, GetLocaleInfoW, GetUserDefaultUILanguage, GetSystemDefaultUILanguage, SetLastError, UnhandledExceptionFilter, GetConsoleOutputCP, HeapReAlloc, HeapSize, SetFilePointerEx, GetFileSizeEx, GetStringTypeW, SetStdHandle, OutputDebugStringW, SetConsoleCtrlHandler, GetProcessHeap, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, LCMapStringW, CompareStringW, GetFileType, HeapAlloc, HeapFree, GetCurrentThread, GetStdHandle, GetModuleHandleExW, FreeLibraryAndExitThread, ResumeThread, ExitThread, CreateThread, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, EncodePointer, InterlockedFlushSList, InterlockedPushEntrySList, RtlUnwind, InitializeSListHead, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, QueryPerformanceCounter, GetStartupInfoW, IsDebuggerPresent, IsProcessorFeaturePresent, TerminateProcess, GetCurrentProcess, SetUnhandledExceptionFilter, WriteConsoleW |
| GDI32.dll | GetStockObject, SetBkColor, ExtTextOutW, EnumFontsW, GetDeviceCaps, SetTextColor, GetObjectW, DeleteObject, CreateSolidBrush, CreateFontIndirectW |
| COMDLG32.dll | GetSaveFileNameW, ChooseColorW, GetOpenFileNameW |
| ADVAPI32.dll | RegOpenKeyExW, RegQueryValueExW, RegCloseKey |
| SHELL32.dll | SHGetFolderPathW, SHGetSpecialFolderPathW, ShellExecuteW, SHCreateDirectoryExW, SHFileOperationW, SHBrowseForFolderW, SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHGetFileInfoW, SHGetDesktopFolder, SHAppBarMessage, DragQueryFileW, Shell_NotifyIconW, DragAcceptFiles, DragFinish, SHGetDataFromIDListW |
| ole32.dll | OleUninitialize, CoCreateInstance, OleInitialize, CoUninitialize, CoTaskMemAlloc, CoTaskMemFree, CoInitialize, DoDragDrop |
| ntdll.dll | RtlGetNtVersionNumbers |
| COMCTL32.dll | ImageList_AddMasked, InitCommonControlsEx, ImageList_Create, ImageList_Destroy, PropertySheetW |

### Possible Origin

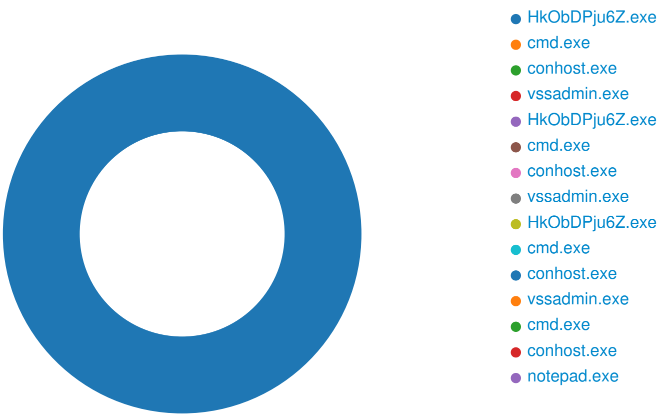
| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States | |

## Network Behavior

⊘ **No network behavior found**

# Statistics

## Behavior



Click to jump to process

# System Behavior

## Analysis Process: HkObDPju6Z.exe PID: **332**, Parent PID: **5700**

### General

| | |
|---|---|
| Target ID: | 3 |
| Start time: | 21:33:29 |
| Start date: | 12/06/2023 |
| Path: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Imagebase: | 0x7d0000 |
| File size: | 1489920 bytes |
| MD5 hash: | 6441D7260944BCEDC5958C5C8A05D16D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 00000003.00000003.22575159083.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

## Analysis Process: cmd.exe PID: **312**, Parent PID: **332**

### General

| | |
|---|---|
| Target ID: | 5 |
| Start time: | 21:33:33 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0x3d0000 |
| File size: | 236544 bytes |
| MD5 hash: | D0FCE3AFA6AA1D58CE9FA336CC2B675B |

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

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **2280**, Parent PID: **312**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 21:33:33 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6a93c0000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: vssadmin.exe PID: **8948**, Parent PID: **312**

### General

| | |
|---|---|
| Target ID: | 7 |
| Start time: | 21:33:34 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\vssadmin.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysNative\vssadmin.exe  delete shadows /all /quiet |
| Imagebase: | 0x7ff7fcb60000 |
| File size: | 145920 bytes |
| MD5 hash: | B58073DB8892B67A672906C9358020EC |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: HkObDPju6Z.exe PID: **1508**, Parent PID: **5700**

### General

| | |
|---|---|
| Target ID: | 10 |
| Start time: | 21:33:47 |
| Start date: | 12/06/2023 |
| Path: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\HkObDPju6Z.exe" |
| Imagebase: | 0x7d0000 |
| File size: | 1489920 bytes |
| MD5 hash: | 6441D7260944BCEDC5958C5C8A05D16D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 0000000A.00000003.22756871962.00000000028F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 0000000A.00000002.22781985168.0000000002A40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **3292**, Parent PID: **1508**

### General

| | |
|---|---|
| Target ID: | 11 |
| Start time: | 21:33:52 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0x3d0000 |
| File size: | 236544 bytes |
| MD5 hash: | D0FCE3AFA6AA1D58CE9FA336CC2B675B |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **2452**, Parent PID: **3292**

### General

| | |
|---|---|
| Target ID: | 12 |
| Start time: | 21:33:52 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6a93c0000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |

| | |
|---|---|
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: vssadmin.exe PID: **4644**, Parent PID: **3292**

### General

| | |
|---|---|
| Target ID: | 13 |
| Start time: | 21:33:52 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\vssadmin.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysNative\vssadmin.exe  delete shadows /all /quiet |
| Imagebase: | 0x7ff7fcb60000 |
| File size: | 145920 bytes |
| MD5 hash: | B58073DB8892B67A672906C9358020EC |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: HkObDPju6Z.exe PID: **5560**, Parent PID: **5700**

### General

| | |
|---|---|
| Target ID: | 14 |
| Start time: | 21:33:55 |
| Start date: | 12/06/2023 |
| Path: | C:\Users\user\Desktop\HkObDPju6Z.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\HkObDPju6Z.exe" |
| Imagebase: | 0x7d0000 |
| File size: | 1489920 bytes |
| MD5 hash: | 6441D7260944BCEDC5958C5C8A05D16D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 0000000E.00000003.22839485707.0000000002980000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 0000000E.00000002.22856927512.0000000002A90000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe

PID: **1808**, Parent PID: **5560**

### General

| | |
|---|---|
| Target ID: | 15 |
| Start time: | 21:34:00 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\system32\cmd.exe /c C:\Windows\SysNative\vssadmin.exe delete shadows /all /quiet |
| Imagebase: | 0x3d0000 |
| File size: | 236544 bytes |
| MD5 hash: | D0FCE3AFA6AA1D58CE9FA336CC2B675B |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe

PID: **4152**, Parent PID: **1808**

### General

| | |
|---|---|
| Target ID: | 16 |
| Start time: | 21:34:00 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6a93c0000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: vssadmin.exe

PID: **8264**, Parent PID: **1808**

### General

| | |
|---|---|
| Target ID: | 17 |
| Start time: | 21:34:00 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\vssadmin.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysNative\vssadmin.exe  delete shadows /all /quiet |
| Imagebase: | 0x7ff7fcb60000 |
| File size: | 145920 bytes |
| MD5 hash: | B58073DB8892B67A672906C9358020EC |
| Has elevated privileges: | false |
| Has administrator privileges: | false |

| | |
|---|---|
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: cmd.exe PID: **3944**, Parent PID: **332**

### General

| | |
|---|---|
| Target ID: | 28 |
| Start time: | 21:36:08 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /c start /MAX notepad.exe c:\instructions_read_me.txt |
| Imagebase: | 0x3d0000 |
| File size: | 236544 bytes |
| MD5 hash: | D0FCE3AFA6AA1D58CE9FA336CC2B675B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: conhost.exe PID: **7328**, Parent PID: **3944**

### General

| | |
|---|---|
| Target ID: | 29 |
| Start time: | 21:36:09 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6a93c0000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: notepad.exe PID: **1352**, Parent PID: **3944**

### General

| | |
|---|---|
| Target ID: | 30 |
| Start time: | 21:36:09 |
| Start date: | 12/06/2023 |
| Path: | C:\Windows\SysWOW64\notepad.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | notepad.exe  c:\instructions_read_me.txt |
| Imagebase: | 0x120000 |
| File size: | 165888 bytes |
| MD5 hash: | E92D3A824A0578A50D2DD81B5060145F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_BlackBasta, Description: Yara detected BlackBasta ransomware, Source: 0000001E.00000002.27586886931.0000000003343000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Disassembly

⊘ **No disassembly**

Copyright Joe Security LLC 2023