

[TOOL] Visual Browsing of Alternative Data-streams in Windows Explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0038.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/09/03

To: list@securiteam.com

Date: 9 Nov 2003 14:42:36 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Visual Browsing of Alternative Data-streams in Windows Explorer

DETAILS

Introduction:

The program uses the NTFS alternate data streams support to create a visual real time viewing and editing of ADS. The program detects ADS in files and displays them inside an explorer window. The program will completely integrate into windows explorer, and will be activated from the menus.

Implementation:

Using the API function Backupread to search for ADS on drives, directories and files. Also, using the class BandObjects to integrate into Explorer.

Methodology:

The NTFS has implemented support for ADS to interact with MAC resource forks (a type of ADS). Today, this option uses many properties of the windows file system including icons, summary information etc. Now, we can use this feature to create, edit and view our own ADS. Using a simple DOS "echo" command, it is possible to create ADS, and using several APIs, it's possible to view them, since they are hidden. The program uses these API functions and taps over the explorer to create a hybrid of explorer and

Securiteam: [TOOL] Visual Browsing of Alternative Data-streams in Windows Explorer

ADS Detector.

ADDITIONAL INFORMATION

The information has been provided by <mailto:alextoz@hotmail.co.il> Alex

The tool can be downloaded from:

<<http://www.codeproject.com/csharp/CsADSDetectorArticle.asp>>

<http://www.codeproject.com/csharp/CsADSDetectorArticle.asp>.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.