Journal scientific and applied research, vol. 7, 2015
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

DETECTION AND IMPLEMENTATION OF ALTERNATE DATA STREAMS IN THE COMPUTER AND NETWORK SYSTEMS

Petar Boyanov

DEPARTMENT OF COMMUNICATION AND COMPUTER TECHNOLOGY, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,
E-MAIL: peshoaikido@abv.bg

ABSTRACT: *In this paper a common detectionand implementation of Alternate Data Streams in the operating system Windows Server 2008 R2 is made. Nowadays it is very important each system administrator and security professional to detect and analyze different types of alternate data streams. These steams can hide sensible secret or malicious files that can damage some of the computer and networks resources.*

KEY WORDS: *Alternate Data Streams, Computer and network systems, Detection Implementation, Windows Server.*

1. Introduction

Each computer file must be detailed and at regular intervals analyzed and scanned with specialized antivirus programs and anti-malware applications.Over the past few years have seen an interesting trend where cyber criminals, hackers and crackers hide executable file to another system executable files. There are cases where malicious files can be hidden behind a normal text file. The cyber criminals use alternate data streams in order to accomplish their malicious work [1,2,3,4,11,13,15,16,21,22,28,29]. The Alternate data streams cannot be seen and found by normal computer users. One of the ways of their detection is the use of specialized software scanner called “ADS Scanner 2.00”.In practice there is a difference between “AltDS” and “ADS”. AltDS is an abbreviation from Alternate Data Streams and ADS means Active Directory Services. In the practice still being used the following programs like “AlternateStreamView v1.35”, “GMER”, “RKDETECTOR v2.0 Beta 1”, “StreamArmor” and etc.The advantage of “ADS Scanner 2” than any other is associated with its speed and efficiency in the computer and network systems[6,7,8,10,18,19,20,24,25,26,27].

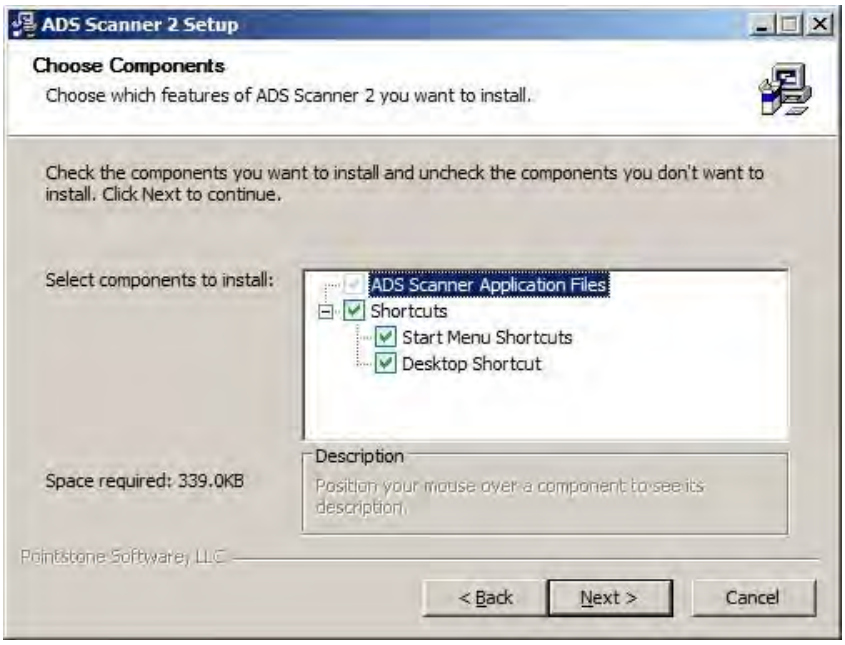
This paper is structured as follows. First, in section 2, a related work for detection and implementation of alternate data streams (AltDS) is made. After that, in section 3, a sophisticated detection and implementation of the specialized software scanner “ADS Scanner 2.00” on server operating system - Windows Server 2008 R2 Enterprise is performed. The achieved results are presented in section 4. The conclusions and recommendations are made in section 5.

2. Related work

In [1] forensic analysis of Windows hosts using UNIX-based tools by Cory Altheide is presented. In [25] some different methods for creation, management, and use of files containing multiple virtual data streams using standard file system applications byK. Randall Stokes is made. In [29] an analysis of hidden data in NTFS file system by Kai Cheong Wee is illustrated.In [22] some adaptive filters for continuous queries over distributed data streams by Chris Olston, Jing Jiang and Jennifer Widom are made. In [11] special methodology and apparatus for detecting executable software in an alternate data stream by Patrick A. Gardner is shown.

3. Experiment

The experiment in specialized university computer and network laboratory is made. The used software program is “ADS Scanner 2.00” which is owned by Pointstone Software, LLC. This scanner is totally free of charge for any one user. The scanning and detection host has usedserver operating system - Windows Server 2008 R2 Enterprise x64.Initially was necessary to be configured the software product. During the installation process there were selected the following items - “ADS Scanner Application Files” [6,7,8,10,16,18,19,20,24,25,26,27], “Start Menu Shortcut” and “Desktop Shortcut”. The following experiments only with educational intends and purposes are made. A common view of the installation process is shown on fig.1.



ADS Scanner 2 Setup

Choose Components

Choose which features of ADS Scanner 2 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ ADS Scanner Application Files
- ⊟ ☑ Shortcuts
  - ☑ Start Menu Shortcuts
  - ☑ Desktop Shortcut

Description

Position your mouse over a component to see its description.

Space required: 339.0KB

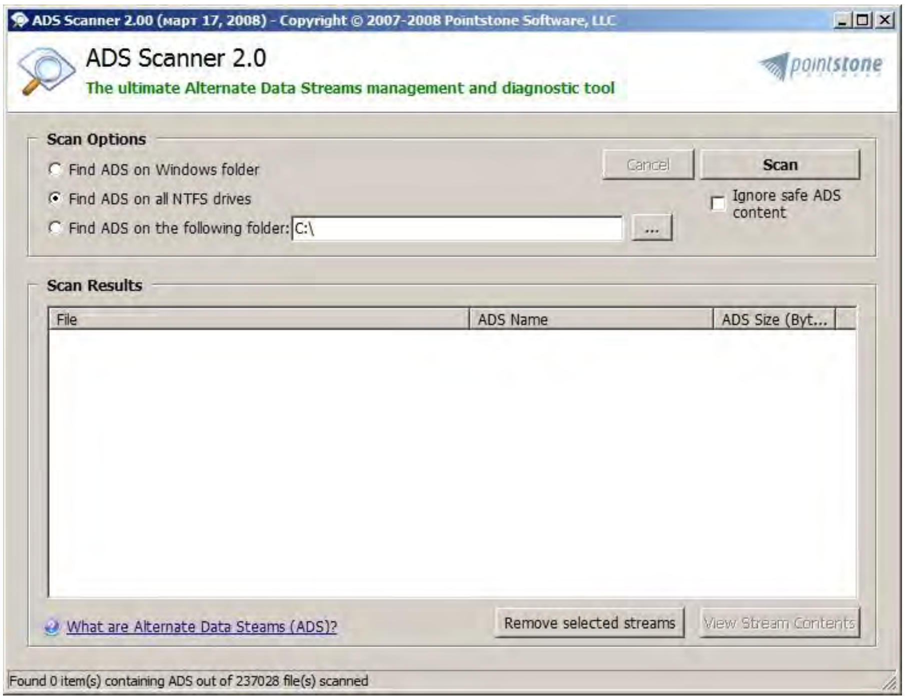
Pointstone Software, LLC

Fig.1. Common view of the software program

The first step with the detection alternate data streams was connected. The scan options were[1,2,3,6,7,8,10,11,13,14,17,18,19,20,21,22,24,25,26,27]:

- Find Alternate Data Streams (ADS) on Windows folder.
- Find Alternate Data Streams (ADS) on all NTFS drives.
- Find Alternate Data Streams (ADS) on the following folder.
- Ignore safe ADS content.

The preliminary preparation before scanning and detection for Alternate Data Streams (ADS) is illustrated on fig.2.



ADS Scanner 2.00 (март 17, 2008) - Copyright © 2007-2008 Pointstone Software, LLC

ADS Scanner 2.0

The ultimate Alternate Data Streams management and diagnostic tool

Scan Options

○ Find ADS on Windows folder

● Find ADS on all NTFS drives

○ Find ADS on the following folder: C:\

□ Ignore safe ADS content

Scan Results

File	ADS Name	ADS Size (Byt...

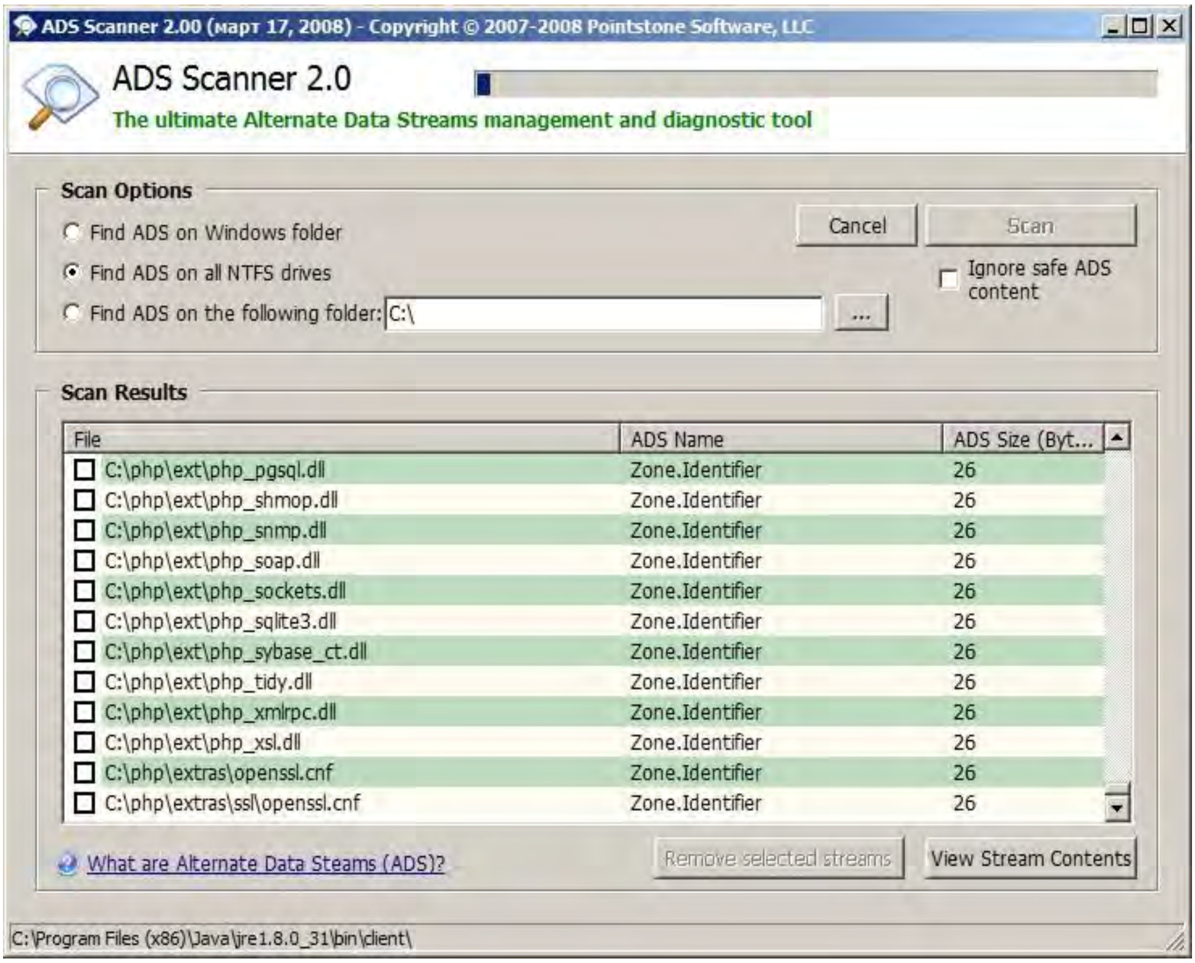
What are Alternate Data Steams (ADS)?

Found 0 item(s) containing ADS out of 237028 file(s) scanned

Fig.2. Preparation before scanning and detection for ADS.

On fig.3 the number of safe Alternate Data Streams (ADS) is shown. The selected scan options was connected with the finding ADS on all NTFS drives. Some of the found files after the scan were [1,2,3,5,7,9,11,14,17,19,20,21,25]:

- C:\php\ext\php_pgsql.dll.
- C:\php\ext\php_shmop.dll.
- C:\php\ext\php_snmp.dll.
- C:\php\ext\php_soap.dll.
- C:\php\ext\php_sockets.dll.
- C:\php\ext\php_sqlite3.dll.
- C:\php\ext\php_sybase_ct.dll.
- C:\php\ext\php_tidy.dll.
- C:\php\ext\php_xmlrpc.dll.
- C:\php\ext\php_xsl.dll.
- C:\php\extras\openssl.cnf.
- C:\php\ext\ssl\openssl.cnf and etc.


ADS Scanner 2.00 (март 17, 2008) - Copyright © 2007-2008 Pointstone Software, LLC
ADS Scanner 2.0
The ultimate Alternate Data Streams management and diagnostic tool
Cancel
Scan
...
What are Alternate Data Steams (ADS)?
Remove selected streams
View Stream Contents

Scan Options

○ Find ADS on Windows folder
● Find ADS on all NTFS drives
○ Find ADS on the following folder: C:\
□ Ignore safe ADS content

Scan Results

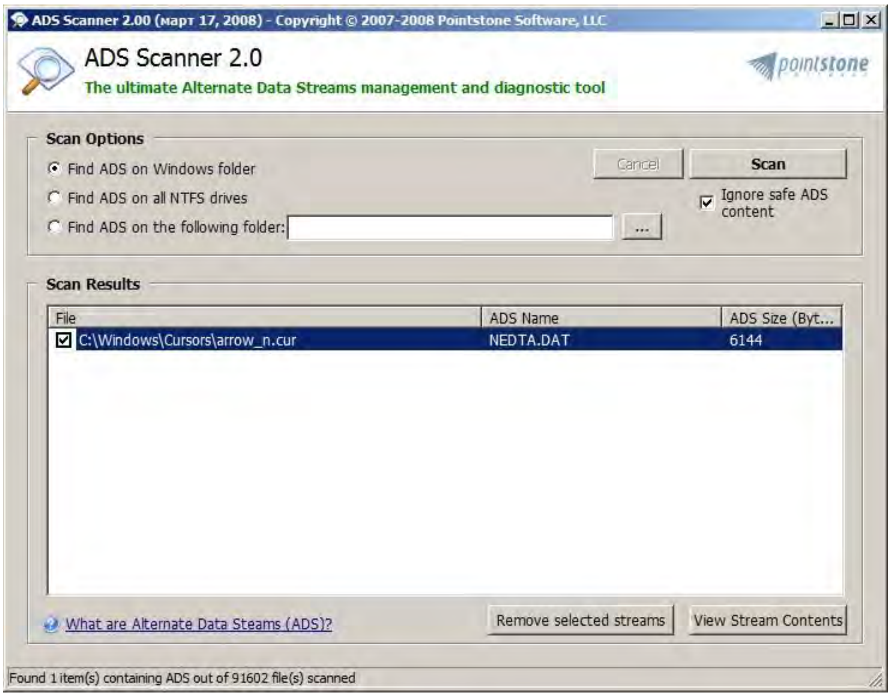
File	ADS Name	ADS Size (Byt...
□ C:\php\ext\php_pgsql.dll	Zone.Identifier	26
□ C:\php\ext\php_shmop.dll	Zone.Identifier	26
□ C:\php\ext\php_snmp.dll	Zone.Identifier	26
□ C:\php\ext\php_soap.dll	Zone.Identifier	26
□ C:\php\ext\php_sockets.dll	Zone.Identifier	26
□ C:\php\ext\php_sqlite3.dll	Zone.Identifier	26
□ C:\php\ext\php_sybase_ct.dll	Zone.Identifier	26
□ C:\php\ext\php_tidy.dll	Zone.Identifier	26
□ C:\php\ext\php_xmlrpc.dll	Zone.Identifier	26
□ C:\php\ext\php_xsl.dll	Zone.Identifier	26
□ C:\php\extras\openssl.cnf	Zone.Identifier	26
□ C:\php\extras\ssl\openssl.cnf	Zone.Identifier	26

C:\Program Files (x86)\Java\jre1.8.0_31\bin\client\

Fig.3. The found Alternate Data Streams (ADS) after the performed scan

4. Results

On fig.4 the number of malicious Alternate Data Streams (ADS) is shown. The selected scan options was connected with the finding ADS on all Windows folder. It was found 1 item that containing Alternate Data Streams (ADS) out of 91602 scanned files.



ADS Scanner 2.00 (март 17, 2008) - Copyright © 2007-2008 Pointstone Software, LLC

ADS Scanner 2.0

The ultimate Alternate Data Streams management and diagnostic tool

Scan Options

● Find ADS on Windows folder

○ Find ADS on all NTFS drives

○ Find ADS on the following folder:

☑ Ignore safe ADS content

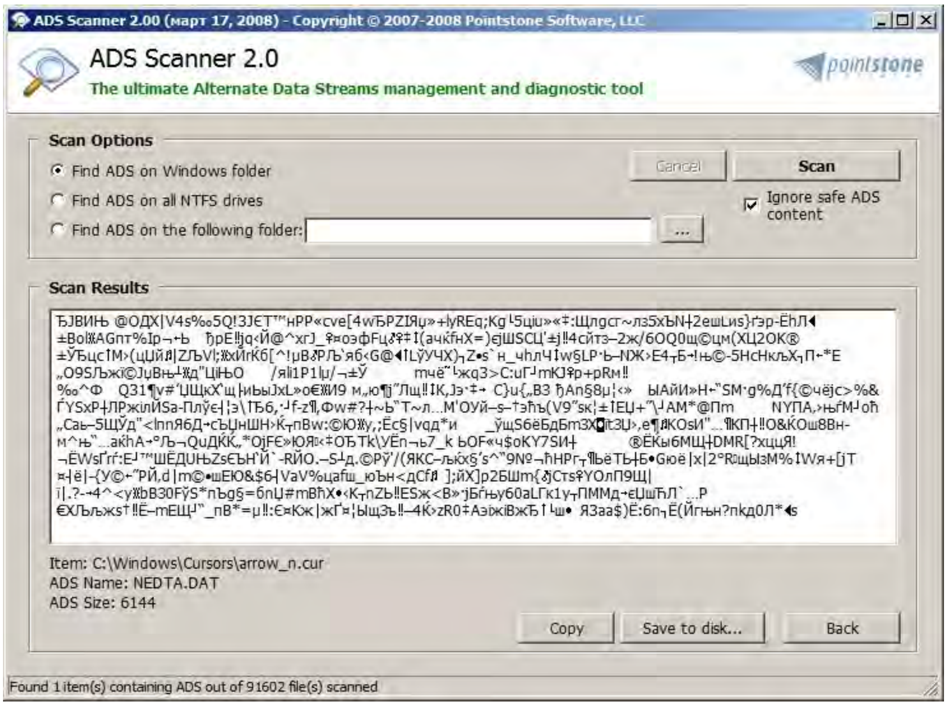
Scan Results

File	ADS Name	ADS Size (Byt...
☑ C:\Windows\Cursors\arrow_n.cur	NEDTA.DAT	6144

Found 1 item(s) containing ADS out of 91602 file(s) scanned

Fig.4. The achieved server availability report

On fig.5 the content of malicious Alternate Data Streams (ADS) is illustrated



ADS Scanner 2.00 (март 17, 2008) - Copyright © 2007-2008 Pointstone Software, LLC

ADS Scanner 2.0

The ultimate Alternate Data Streams management and diagnostic tool

Scan Options

● Find ADS on Windows folder

○ Find ADS on all NTFS drives

○ Find ADS on the following folder:

☑ Ignore safe ADS content

Scan Results

```
ЂJВИЊ @ОДХ|V4s‰5Q!3JЄТ™нPP«cve[4wЂPZIЯџ»+lyREq;Kg└5џiu»«‡:Щлgcг~лз5хЪN╪2ешLиs}ѓэр-ЁhЛ◄
±Bo▒AGпт%Ip¬←Ь   ђpE‼jq‹Й@^xгJ_♀¤оэфFџ♪♀‡↕(ачќfнХ=)єјШSCЦ'±j‼4сйтз–2ж/6OQ0щ©цм(ХЦ2OK®
±ЎЂцс↑M›(цЏйЯ|ZЉV!;▒хЙгЌб[^!µB♪PЉ`яб‹G@◄↑LўУЧХ)┐Z•s` н_чhлЧ↕w§LP·Ь–NЖ›E4┬Б→!њ©-5HcHклъХ┐П←*E
„O9SЉжї©JџВњ┴▒д"ЦіЊО     /яli1P1lџ/¬±Ў         mчё˜└жq3>C:uГ┘mKJ♀p+pRм‼
‰^Ф   Q31¶v#'ЏЩкХ'щ├иЬыJxL»о€▒И9 м„ю¶j"Лщ‼↕K,Jэ·‡→ C}u{„B3 ђAn§8µ¦‹»   ЫАйИ»H←"SM·g%Д'f{©чёjс>%&
ЃYSxP╪ЛPжілИSa-Плўє┤¦э\↑Ђб,·┘f-z¶,Фw#?┼~Ь"Т~л…M'OУй–s–†эћъ(V9"sк¦±↑EЏ+"\┘AM*@Пm       NYПА,›њѓM┘oћ
„Саь–5ЩЎд"<lnnЯбД→сЪЏнШН›Ќ┬пBw:©Ю▒у,;Ёс§|vqд*и       _ўщS6ёБдБm3X◘ї3Џ›,е¶ЯKOsИ"…¶КП╪‼O&ЌОш8Вн-
м^њ"…аќhA→°Љ¬QuДЌЌ„*OjFЄ»ЮЯ▯‹‡OЂTk\УЁn¬ь7_k ЬOF«ч$оKY7SИ╪          ®ЁКы6МЩ╪DMR[?хццЯ!
¬ЁWsЃгѓ:E┘™ШЁДUЊZsЄЪН'Й`-RЙO.–S┴д.©Pў'/(ЯКС–љќх§'s^"9N№¬ћHPг┬¶ЬёТЬ╪Б•Gюё|x|2°R▯щЫзM%↕Wя+[jT
¤┤ё|-{У©←"PЙ,d|m©•шЕЮ&$б┤VaV%цafш_юЪн<дСfЯ ];йХ]p2БШm{♪јСтs♀YOлП9Щ|
ї|.?-→4^<y▒bB30FўS*nЪg§=бnЏ#mBћX•‹K┬nZЬ‼ESж<B»·jБѓњу60aLГк1у┬ПММд→єЏшЋЛ`…P
€ХЉљжs†‼Ё–mЕЩ┘"_nB*=µ‼:Є¤Кж|жЃ¤¦Ыщ3ъ‼–4Ќ›zR0‡Азіжі ВжЂ↑└ш•  Я3аа$)Ё:6п┐Ё(Йгњн?пкд0Л*◄s
```

Item: C:\Windows\Cursors\arrow_n.cur

ADS Name: NEDTA.DAT

ADS Size: 6144

Found 1 item(s) containing ADS out of 91602 file(s) scanned

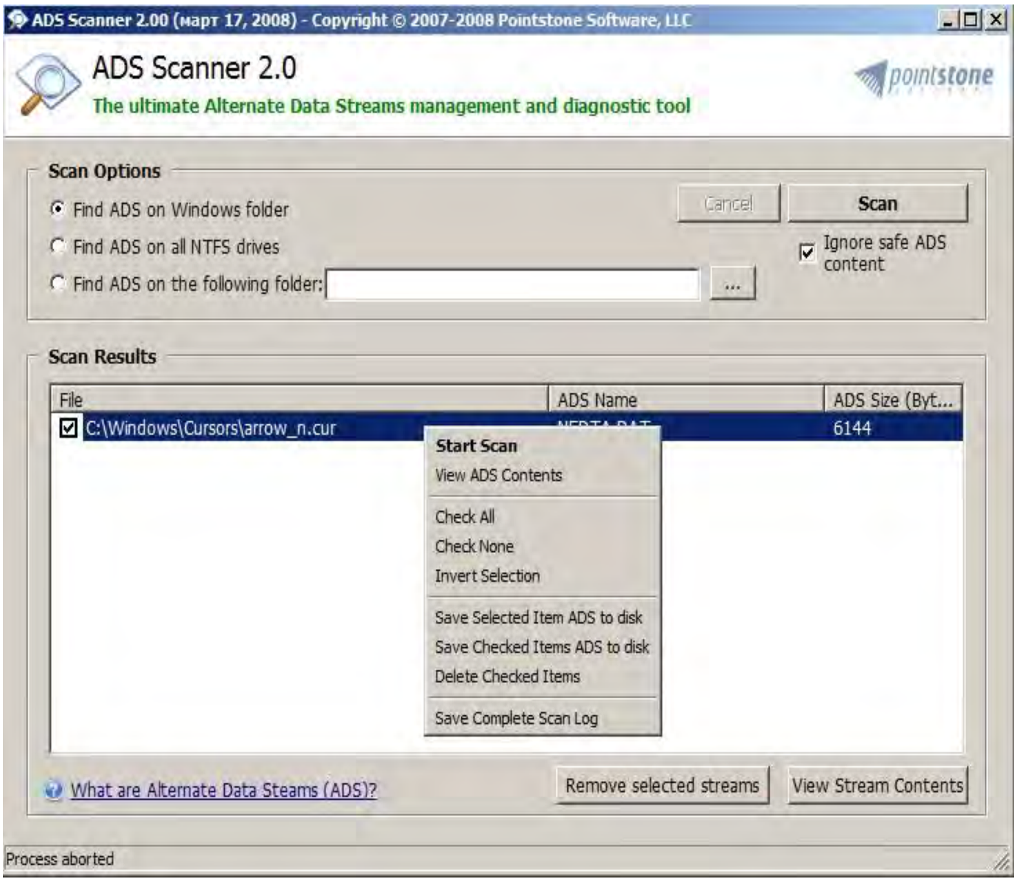
Fig.5. The content of malicious Alternate Data Streams (ADS)

As shown on fig.5 this ADS is consists of the following items:

- Item: C:\Windows\Cursors\arrow_n.cur.
- ADS name: NEDTA.DAT.
- ADS size: 6144 Bytes.

On fig.6 the following action options are shown:

- Start Scan.
- View ADS Content (shown on fig.5).
- Check All.
- Check None.
- Invert Selection.
- Save Selected Item ADS to disk.
- Save Checked Item ADS to disk.
- Delete Checked Items.
- Save Complete Scan Log.



ADS Scanner 2.00 (март 17, 2008) - Copyright © 2007-2008 Pointstone Software, LLC

ADS Scanner 2.0

The ultimate Alternate Data Streams management and diagnostic tool

Scan Options

● Find ADS on Windows folder

○ Find ADS on all NTFS drives

○ Find ADS on the following folder:

☑ Ignore safe ADS content

Scan Results

File	ADS Name	ADS Size (Byt...
☑ C:\Windows\Cursors\arrow_n.cur	NEDTA.DAT	6144

Process aborted

Fig.6. The action options

Thanks to this program each normal user, system and network administrator and security professionals could obtain detailed graphical information about hidden malicious Alternate Data Streams in the target host operation system. [4,6,7,13,17,1819,20,22,25,26,28,29].

5. Conclusion

The alternate data streams are hidden files that could be attached to each normal and visible computer file. Recent cyber criminals, hacker and crackers use these alternate data streams in order to hide their malicious file and unfortunately very small number of antivirus programs and anti-malware and rootkit scanners and analyzers can find them. Therefore, the attackers or cyber-criminals are able to obtain all computers and network resources completely unnoticed by the host. For this reason it is recommended to be made the correct configuration of the computer and network systems and each host file must be detailed and at regular intervals analyzed and scanned with specialized antivirus programs and thereby, the risk of cyber-attacks, viruses, worms, spyware, rootkits and other malicious programs could be totally reduced.

Acknowledgements

This paper is supported by the Project BG051PO00l-3.3.06-0003 “Building and steady development of PhD students, post-PhD and young scientists in the areas of the natural, technical and mathematical sciences”. The Project is realized by the financial support of the Operative Program “Development of the human resources” of the European social found of the European Union.

REFERENCES:

[1]. Altheide, Cory. "Forensic analysis of Windows hosts using UNIX-based tools." Digital Investigation 1, no. 3 (2004): 197-212.

[2]. Anglin, Matthew Joseph, David Maxwell Cannon, Barry Fruchtman, AvishaiHaim Hochberg, and James Patrick Smith. "Separating file data streams to enhance progressive incremental processing." U.S. Patent 7,908,246, issued March 15, 2011.

[3]. Bem, Derek, and Ewa Z. Huebner. "Alternate Data Streams in Forensic Investigations of File Systems Backups." Current Computing Developments in E-Commerce, Security, HCI, DB, Collaborative and Cooperative Systems (2006): 449-460.

[4]. Berghel, Hal, and NatasaBrajkovska. "Wading into alternate data streams." Communications of the ACM 47, no. 4 (2004): 21-27.

[5]. Berghel, Hal. "Wireless infidelity I: War driving." Communications of the ACM 47, no. 9 (2004): 21-26.

[6]. Berghel, Hal, David Hoelzer, and Michael Sthultz. "Data hiding tactics for Windows and Unix file systems." Advances in Computers 74 (2008): 1-17.

[7]. Broomfield, Mike. "Ntfs alternate data streams: focused hacking." *Network Security* 2006, no. 8 (2006): 7-9.

[8]. Cogswell, Bryce, and Mark Russinovich. "Rootkitrevealer v1. 71." Rootkit detection tool by Microsoft (2006).

[9]. Davis, Jeremy, Joe MacLean, and David Dampier. "Methods of information hiding and detection in file systems." In Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on, pp. 66-69. IEEE, 2010.

[10]. French, Steven Michael, David John Kleikamp, and Theodore YueTakTso. "Method and apparatus for emulating alternate data streams across heterogeneous file systems." U.S. Patent Application 11/467,424, filed August 25, 2006.

[11]. Gardner, Patrick A., Spencer D. Smith, and Alexander Danileiko. "Method and apparatus for detecting executable software in an alternate data stream." U.S. Patent 8,141,153, issued March 20, 2012.

[12]. Hristov Hr., "A passive strategy for management of counteraction toencroachments on business organization, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, Vol.6, 2014, pp. 187-194

[13]. Huebner, Ewa, Derek Bem, and Cheong Kai Wee. "Data hiding in the NTFS file system." digital investigation 3, no. 4 (2006): 211-226.

[14]. Hurlbut, Dustin. "Thumbs DB Files Forensic Issues." AccessData Training Document (2005).

[15]. Kankanhalli, Mohan S., Jun Wang, and Ramesh Jain. "Experiential sampling on multiple data streams." Multimedia, IEEE Transactions on 8, no. 5 (2006): 947-955.

[16]. Kent, Karen, Suzanne Chevalier, Tim Grance, and Hung Dang. "Guide to integrating forensic techniques into incident response." NIST Special Publication (2006): 800-86.

[17]. Knierim, Daniel G., and John A. Martin. "Memory system for storing data from variable numbers of input data streams." U.S. Patent 4,975,880, issued December 4, 1990.

[18]. Lee, Jaejin, Chungyong Lee, and Douglas B. Williams. "Secure communication using chaos." In Global Telecommunications Conference, 1995. GLOBECOM'95., IEEE, vol. 2, pp. 1183-1187. IEEE, 1995.

[19]. Means, Ryan L. "Alternate data streams: out of the shadows and into the light." Retrieved September 20 (2003): 2005.

[20]. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Информационныетехнологии и безопасность, ЖурналАкад. наукУкраины., Спец. выпуск, Киев, 2013, Стр. 79-86

[21]. Olston, Chris, Jing Jiang, and Jennifer Widom. "Adaptive filters for continuous queries over distributed data streams." In Proceedings of the 2003 ACM SIGMOD international conference on Management of data, pp. 563-574. ACM, 2003.

[22]. Parker, Don. "Windows ntfs alternate data streams." *Security Focus* 16 (2005).

[23]. Rogers, M., and M. Lockheed. "Anti-forensics." Center for Education and Research in Information Assurance & Security (CERIAS), Department of Information and Computer Technology, Purdue University (2005).

[24]. Stokes, Randall K. "Method for creation, management, and use of files containing multiple virtual data streams using standard file system APIs." U.S. Patent 6,466,944, issued October 15, 2002.

[25]. Tasheva, Z. N., Tasheva, A. T. Combining cryptography and steganography in software system for hiding confidential information, International Journal of Science, Education and Innovation, Volume 1, 2013. ISSN 1314-9784, Association Scientific and Applied Research, pp. 84-92.

[26]. Thomas, McGee, and AgnihotriLalitha. "Method and system for information alerts." U.S. Patent Application 10/053,451, filed November 9, 2001.

[27]. Wee, Cheong Kai. "Analysis of hidden data in NTFS file system." Edith Cowan University (2006).

[28]. Zadjmool, Ray. "Hidden threat: Alternate data streams." *Retrieved September* 20 (2004): 2005.

[29]. Zeadally, Sherali, EceYaprak, and Y. Li. "A SURVEY OF NETWORK PERFORMANCE TOOLS." (2002).