



Heaventools PE Explorer

Codeanalyse der Malware

Reverse-Engineering-Spezialisten von Antivirus- und Forensik-Unternehmen stehen vor einer Herausforderung, viele schädliche Software zu analysieren, die im hohen Maße auftritt. Software-Entwickler suchen nach einer effektiven Möglichkeit, potentiell schädliche ausführbare Windows-Dateien sicher zu überprüfen und zu analysieren. Um diese Bedürfnisse zu erfüllen, bietet Heaventools PE Explorer, eine integrierte Sammlung verschiedener Tools, die einen Framework für die Arbeit mit EXE-, DLL-, ActiveX-Controls- und anderen ausführbaren Dateiformaten, die unter MS Windows 32-Bit-Plattformen laufen, bildet.

Obwohl Antivirus-Software ständig verbessert wird, schafft es ein erheblicher Teil der Malware, dem automatischen Schutz zu entkommen. PE Explorer erlaubt es Ihnen, sich direkt in das Innere des Programms zu stürzen, und hilft Software-Firmen dabei, festzustellen, ob die Binärdateien schädlich sind, indem diese manuell untersucht werden, ohne dabei auf die automatischen Scan-Engines angewiesen zu sein.

Syntax Description Editor for adding custom comments, altering values or creating new library description

Export Properties display the details for the currently selected function

The screenshot shows the PE Explorer interface for 'C:\Test\firefox.exe'. The 'EXPORT VIEWER' section displays a table of export entries:

Entry Point	Ord	Export Name
008C080Fh	11	
008C101Bh	12	
004D9C11h	13	
008C0C75h	14	
008C30EBh	15	
008C2E98h	16	
0065FAACh	17	??UnsRect@@QAE@ABUU@@Z
004D94C2h	18	??0nsRect@@QAE@ABUnsPoint@@ABUnsSize@@@Z
004D94F4h	19	??0nsRect@@QAE@HHHH@Z

The 'Syntax Details' window shows the following C++ function signature:

```
public: __thiscall nsRect::nsRect(struct nsPoint const &,struct nsSize const &)
```

The 'Log Window' displays the following messages:

```
14.03.2006 02:21:41 : EOF Extra Data From: 00605800h (7165952)
14.03.2006 02:21:41 : Length of EOF Extra Data: 00000065h (101) bytes.
14.03.2006 02:21:41 : EOF Position: 00605865h (7166053)
14.03.2006 02:21:41 : Precompiling Resources...
14.03.2006 02:21:41 : Done.
```

Log Window displays notes, messages, errors, warnings, or status of each task

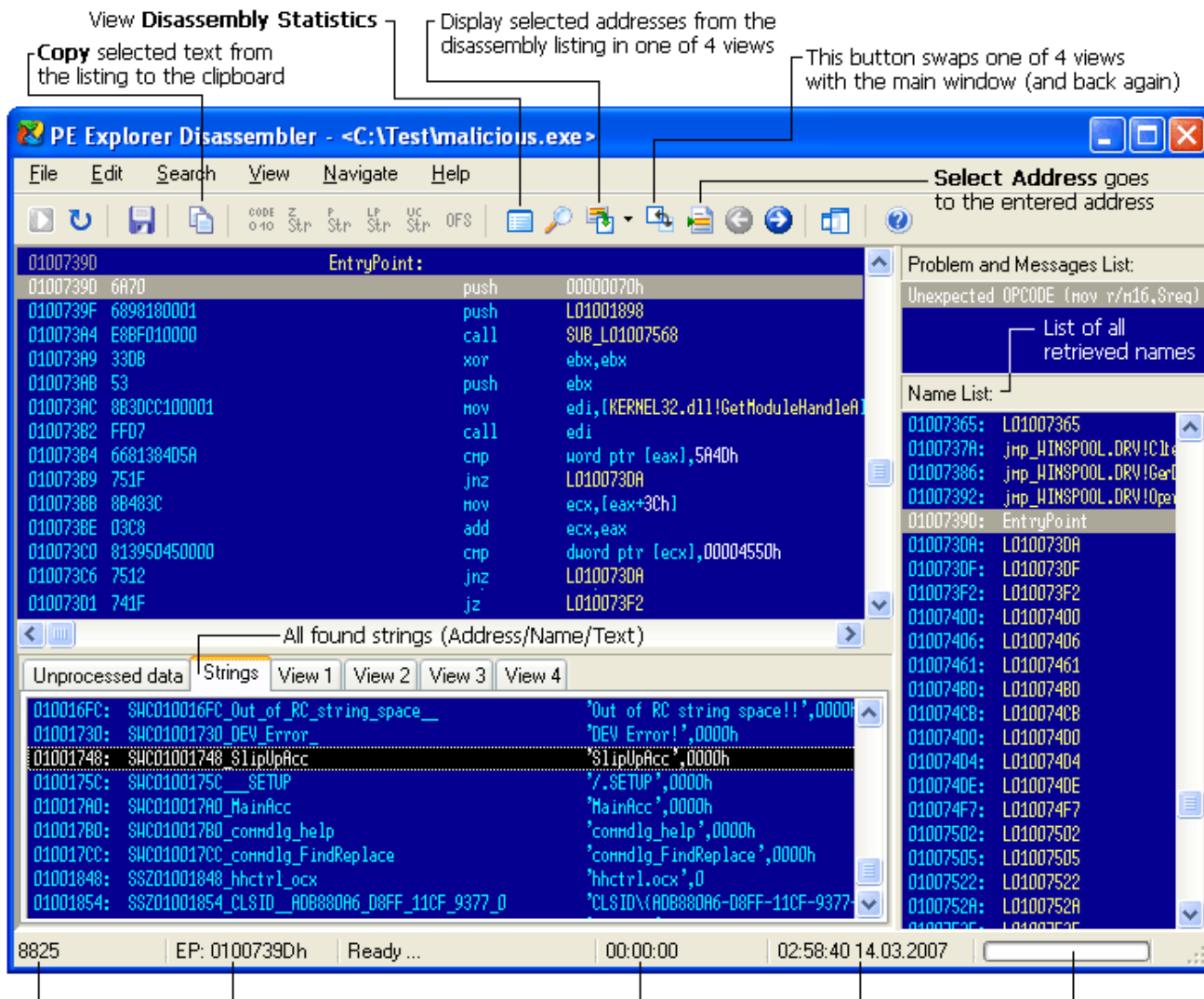
Parameters, return values, calling conventions are conveniently displayed for you in the **Syntax Details** window

PE Explorer reduziert die Zeit erheblich, die man braucht, um die Struktur der komplexen Malware zu verstehen. Diese Anwendung listet jede Kopfzeile, jeden Funktionsabschnitt und jede Tabelle

einer ausführbaren Datei, um die zur Laufzeit gespeicherten Werte offen zu legen und stellt die zahlreichen internen Informationen der Binärdatei in einem besser verständlichen Format dar. Dabei erhält der Anwender einfach lesbare Informationen über die Funktion der ausführbaren Datei. PE Explorer deckt die gesamte Struktur und alle Ressourcen der verdächtigen Datei auf, um diese zu untersuchen und Reverse-Engineering zu betreiben. Mit PE Explorer können Sie rasch die Prozeduren und Bibliotheken, die die Malware benutzt, analysieren, ohne dabei die ausführbaren Dateien zu aktivieren – ein großer Vorteil gegenüber Diagnose-Programmen, bei denen der verdächtige Code ausgeführt werden muss, um analysiert zu werden.

Disassembler

Eine Disassemblierung des Codes ermöglicht eine Untersuchung, wie das Programm exakt funktioniert sowie die Identifizierung potentieller Sicherheitslücken. Wenn Sie Reverse-Engineering auf Spyware anwenden, können Sie feststellen, nach welchen Informationen das Spionageprogramm suchte, bekommen aber auch viele andere Funktionen. Reverse-Engineering kann auch dafür benutzt werden, undokumentierte APIs oder Porttreiber zu entdecken, sowohl Software-Patches zu analysieren.



The status line displays the current position of the cursor, the address corresponding to the cursor position, the current status, the time spent by the last operation, the current time and date, and the progress indicator for writing the listing to a file.

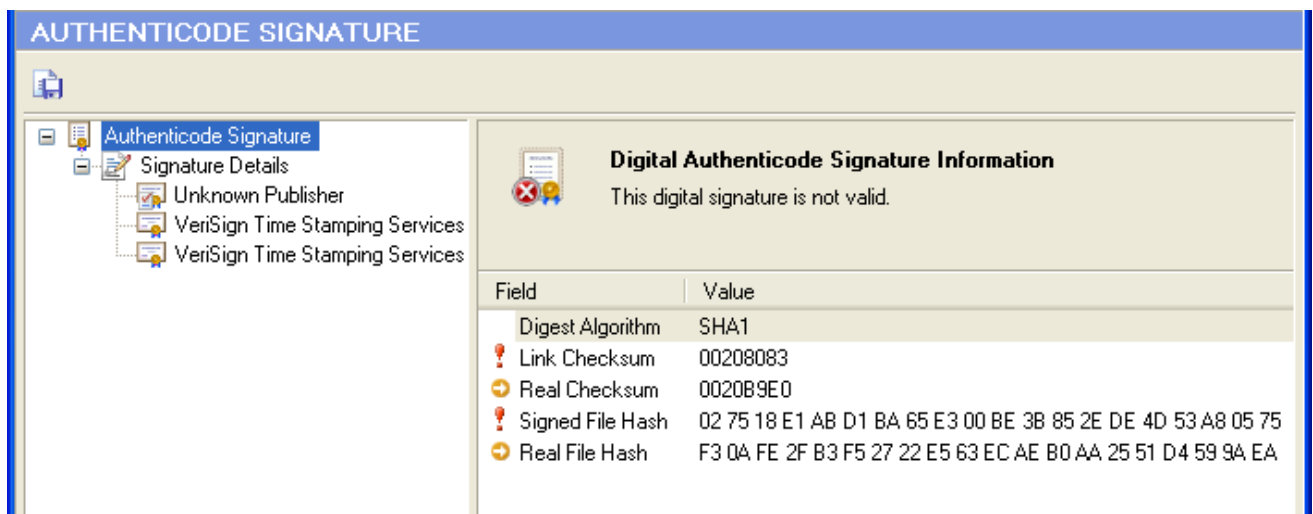
PE Explorer wurde als leicht zu bedienende Alternative zu anderen Disassembler- programmen gestaltet. Leistungsstark, wie die anderen, teureren Disassemblerprogramme, konzentriert sich PE Explorer sowohl auf die Benutzerfreundlichkeit, als auch auf Navigationsleichtigkeit. Es unterstützt

die meisten allgemeinen Intel x86-Befehlsätze und Erweiterungen (MMX, 3DNow!, SSE, SSE2 und SSE3), und verwendet einen hochwertigen Algorithmus, speziell entwickelt, um den Quellcode der Zielfeile so exakt wie möglich in Assemblersprache zu rekonstruieren.

Der Disassembler zieht den ASCII- und Unicode-Text aus dem Datenteil heraus. Im Unterschied zu den verschiedenen Zeilen-Tools, die nach Textzeilen in der Datei suchen, bzw. sie extrahieren, ist PE Explorer durchs Extrahieren dieser Zeilen aus bestimmten Speicherplätzen anstatt durch Suchen viel präziser und detaillierter. Die Ausgabe der in binären Dateien gefundenen Zeilen gibt Ihnen ein gutes Wissen über die Funktionen und Unterprogramme, die vom Programm aufgerufen werden.

Überprüfen der Identität des Software-Herstellers

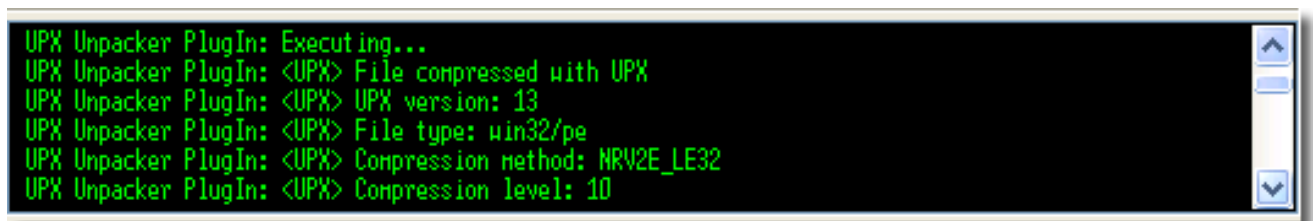
Mit dem Digital Signature Viewer der Anwendung steht Ihnen ein hervorragendes Tool zum Erkennen von Viren, Malwareprogrammen und anderen schädlichen ausführbaren Dateien zur Verfügung, mit dem Sie die in der geladenen ausführbaren Datei enthaltene digitale Microsoft Authenticode-Signatur (sofern vorhanden) anzeigen und überprüfen können.



Dies ist eine leistungsfähige Methode, um den Herausgeber und die Integrität der ausführbaren Datei zu überprüfen.

Komprimierte Würmer und Trojaner entpacken

PE Explorer kann eine breite Palette von Dateitypen öffnen, angefangen bei häufig vorkommenden Dateitypen wie beispielsweise EXE- und DLL-Dateien bis hin zu selteneren Dateitypen wie etwa DPL- und CPL-Dateien. Jedoch werden Viren, Würmer und Trojaner im echten Leben oft gegen Reverse-Engineering geschützt, komprimiert und getarnt.



PE Explorer kann sogar mit ausführbaren Schadprogrammen umgehen und diese sicher entpacken. Selbst dann, wenn ein Schadprogramm gepackt und manuell modifiziert wurde, so dass standardmäßige Entkomprimiermethoden nicht direkt verwendet werden können, um die Datei zu dekomprimieren ohne sie auszuführen. PE Explorer unterstützt Dateien, die mit Upack und vielen

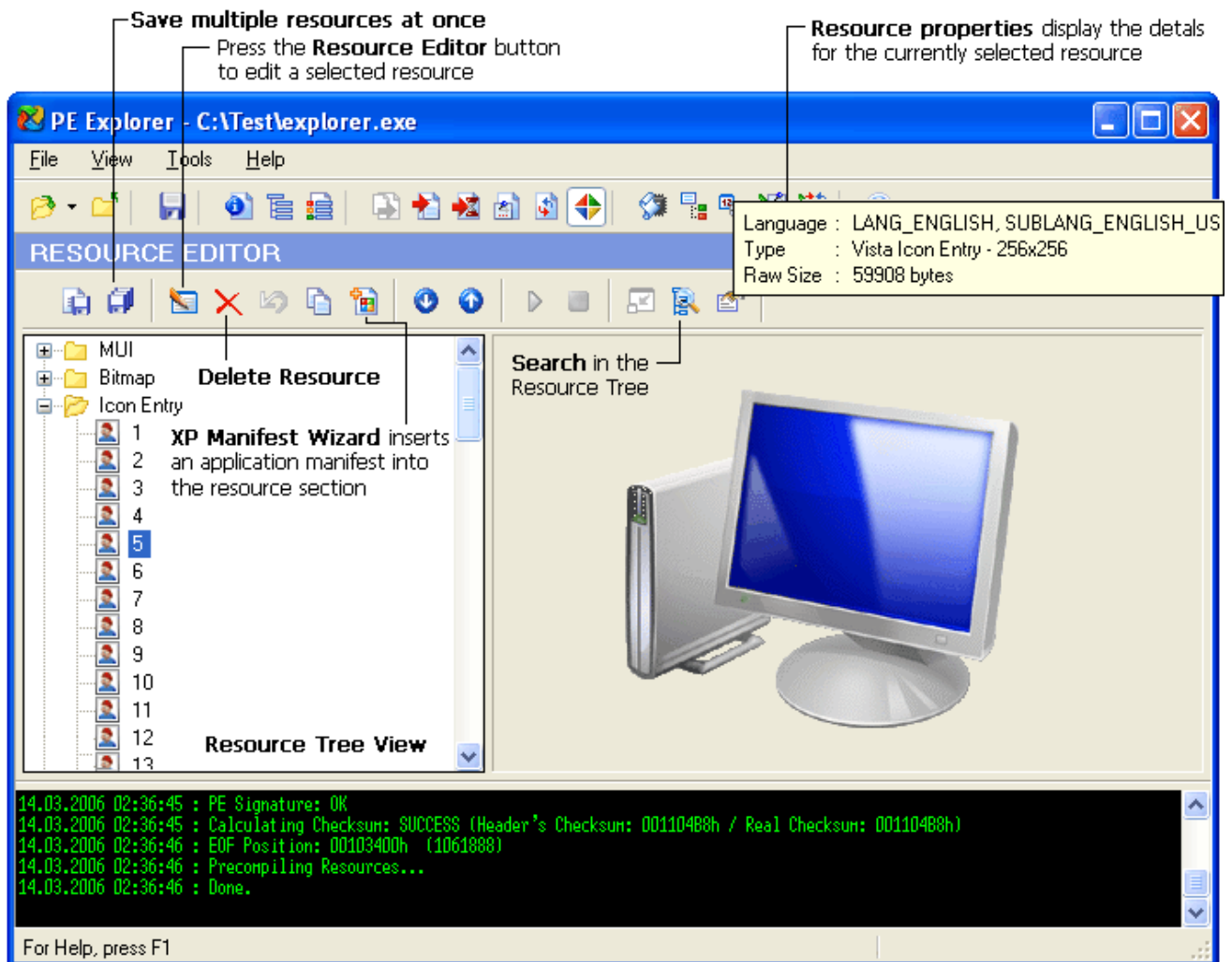
anderen UPX-Scramblern verändert wurden. Nun können Sie diese verschleierte Dateien mit PE Explorer öffnen, sogar ohne zu wissen, dass die Dateien automatisch entpackt werden.

Das Produkt bietet zudem eine offene Schnittstelle zur Einbindung von benutzerdefinierten Startup-Modulen zum Bearbeiten von verschlüsselten Dateien.

Visueller Ressourcen-Editor

PE Explorer vereint einen Ressourcenbetrachter, Extrahierer sowie einen Ressourcen-Editor. Nachdem die Datei geöffnet wird, sehen Sie eine verzeichnisartige Struktur, die ähnlich der vom Windows Explorer ist. Jeder Ordner stellt einen anderen Ressourcentyp dar, der durch die Ziellanwendung genutzt wird (Icons, Grafiken, Menü, Text, Dialogfenster, XML, HTML).

Mit PE Explorer können Sie die Ressourcen eigener Software ansehen, extrahieren, ersetzen, bearbeiten oder löschen. Noch wichtiger, ermöglicht diese Anwendung den Rebranding von Drittanwendungen und -Bibliotheken, für die Sie keinen Code haben, mit neuen Icons, Zeilen und Versionsnummern.



Um immer auf dem neuesten Stand mit dem Windows-Betriebssystem zu bleiben, hilft PE Explorer Ihren älteren Anwendungen, die Vorzüge der neuen Control-Styles und Designs von Windows XP und Vista zu nutzen, und markiert Nicht-Vista Anwendungen mit dem angeforderten Ausführungslevel. Dies ermöglicht es, dieselbe Version der Anwendung für Windows Vista und Windows XP zu vertreiben.

Dependency Scanner

Ein weiteres Feature ist der Dependency Scanner, der alle Module, die mit Ihrer PE-Datei statisch verlinkt sind, sowie alle nachträglich in den Speicher geladenen Module überprüft und sie anschließend in einer hierarchischen Baumstruktur anzeigt, die sichtbar macht, worauf die PE-Datei zugreift. PE Explorer hilft Ihnen beim Herausfinden der minimal notwendigen DLL-Dateien, die zum Laden und Ausführen einer EXE-Datei notwendig sind, und gibt den vollständigen Pfad zu Modulen, die mit der EXE-Datei geladen werden, an. Es hilft beim Entdecken von fehlenden oder ungültigen Modulen, Import-/Export-Fehlanpassungen, zyklischen Abhängigkeiten und anderen modulbezogenen Problemen, und bei der Behebung von Systemfehlern, die durch Laden oder Ausführen der Module hervorgerufen werden.

Industrie-Feedback

“Ich benutze PE Explorer für .SYS-Dateien, da ich Systemarchitekt für NT/XP-Gerätetreiber bin. Es hat mich interessiert, wie die .SYS-Dateien miteinander agieren, und dieses Tool hat mir dabei geholfen, dieses Zusammenspiel besser zu verstehen.” – *Dominick Cafarelli, Sniffer Technologies, Network Associates*

“Ich benutze PE Explorer schon seit einer Weile, und ich bin von den neuesten Funktionen sehr beeindruckt – besonders vom Disassembler.” – *Conrad Herrmann, Zone Labs, Inc.*

Minimalen System-Anforderungen

PE Explorer läuft unter allen Windows-Versionen, von 95/98/XP bis Server 2003 und Vista.

- Intel Pentium® oder AMD K5 processor mit 166 MHz
- 16 MB RAM
- 15 MB freie Festplattenkapazität

Nutzer, die mit großen Dateien arbeiten, würden profitieren, wenn ihre Systemkonfiguration über die oben genannten Systemanforderungen hinausgehen. Dadurch kann eine schnellere Disassemblierung sichergestellt werden.

Produktwartung

Beim Kauf von PE Explorer bekommen Sie Wartung und Support für 18 Monate ab Kaufdatum.

Kaufinfos

Wir bieten eine kostenlose Testversion, so dass Sie die Software risikofrei testen können. Sie können PE Explorer und technischen Basissupport kostenlos 30 Tage ausprobieren, bevor Sie eine Kaufentscheidung treffen. Sollten Sie sich dafür entscheiden, besuchen Sie bitte unsere Webseite www.heaventools.de, um direkt von uns zu bestellen.



Heaventools Software

<http://www.heaventools.de>
101-1001 West Broadway Dept. 381
Vancouver, BC, V6H4E4, Canada

Email: sales@heaventools.com
Fax: +1 (206) 984-3919