2009

Understanding malware autostart techniques with web data extraction

Matthew Gottlieb

Understanding Malware Autostart Techniques with Web Data Extraction

By

Matthew Gottlieb

Thesis submitted in partial fulfillment of the requirements for the
degree of Master of Science in
Networking and Systems Administration

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Department of Networking, Security, and Systems Administration

August 21, 2009

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Networking and Systems Administration

Thesis Approval Form

Student Name: Matthew Gottlieb

Thesis Title: Understanding Malware Autostart Techniques with Web Data Extraction

Thesis Committee

Name	Signature	Date

Bo Yuan
Chair

Sumita Mishra
Committee Member

Yin Pan
Committee Member

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in
Networking and Systems Administration

Understanding Malware Autostart Techniques with Web Data Extraction

I, Matthew Gottlieb, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: _____ Signature of Author: _____

Abstract

The purpose of this study was to investigate automatic execution methods in Windows operating systems, as used and abused by malware. Using data extracted from the Web, information on over 10,000 malware specimens was collected and analyzed, and trends were discovered and presented. Correlations were found between these records and a list of known autostart locations for various versions of Windows. All programming was written in PHP, which proved very effective. A full breakdown of the popularity of each method per year was constructed. It was found that the popularity of many methods has varied greatly over the last decade, mostly following operating system releases and security improvements, but with some frightening exceptions.

Table of Contents

Table of Figures

1 Introduction

The Internet is home to an enormous collection of knowledge. This knowledge is spread across millions of servers, and made available in countless different formats. While this information can itself be very useful, even more value can be found in the analysis of large amounts of this information, to discover patterns and trends that may not be immediately obvious. The process of extracting patterns and correlations from preexisting information is known as data extraction.

One field that is certainly well represented on the Internet is computer security, and information technology at large. With data extraction techniques, this abundance of computer security-related information can be analyzed, furthering the understanding of important issues, such as the constant fight against malicious software.

Malicious software, commonly referred to as malware, is a serious concern in the field of information technology. Developments in Internet technologies, such as email and the World Wide Web, expose millions of computer systems to the dangerous threat of malware. An entire industry has been created to prevent and protect against malware, with major corporations like Symantec investigating the ongoing problem. Understanding the ways pieces of malware function is a critical step in combating this epidemic.

In previous decades, it was common for malware to make its presence obvious, either by catastrophically interrupting a system's normal operation, or displaying a characteristic message to its victims. Programmers created these pieces of malware with simple intentions, as a prank or a way to gain notoriety among their peers. Today, malware authors have motives

that are more serious: money, politics, espionage, and possibly even terrorism. For these types of malware, it is advantageous for the software to run secretly in the background at all times, to remain undetected by end users. When the malware is running, it can gather private information, display advertisements, transmit spam messages, or even launch a targeted attack against a remote system. Clearly, the end user will not intentionally execute these programs, so they must be launched automatically and invisibly. This research will help understand these "autostart" methods, and discover trends in their use, to assist in the fight against malware.

By collecting and analyzing data from a malware research organization, usage of these autostart methods can be measured, discovering the popularity, and predicting future usage, of each method. This research will use a series of PHP scripts to automatically catalog, download, and analyze the information contained in the Symantec Threat Explorer, a collection of information on malware behavior. As the information was not designed to be used in this way, certain challenges, such as the nonuniformity of data contained within the Threat Explorer, must be surmounted. The mythology of this research successfully overcomes these challenges to produce accurate and reliable results on the usage and popularity trends of malware autostart techniques.

2 Literature Review

The topic of malware has generated numerous studies and discussions in recent years. In addition, data extraction is a widely discussed and sometimes contested method research method in both educational and commercial circles.

2.1 The Malware Epidemic

It is hard to deny that Malware is a problem. Massive virus outbreaks have been reported to bring down computing systems of major corporations. Spyware has been blamed for cases of identity theft. Anti-malware companies such as Symantec and F-Secure publish periodic reports on the malware epidemic.

One very difficult concept in malware research is the overwhelming number of terms, each with many possible definitions. Some of these definitions overlap or even conflict with others. In his postgraduate thesis, "Taxonomy of Spyware and Empirical Study of Network Drive-By-Downloads", Barwinski analyzed many different types of malware and their common behaviors. He created multiple VMware virtual machines with varying configurations and exposed them to a number of malware threats by visiting various web sites with an automated script. Barwinski then used system-level tools within the virtual environment, both "advanced" Sysinternals applications and common end-user anti-malware software, to discover the effects of each piece of malware. His conclusions show the many unauthorized system modifications performed by malware.

In her study "Avoiding the Cyber Pandemic", Zelonis equated the damage caused by malware to medical issues such as HIV/AIDS. She qualitatively analyzed malware and its effects on computer systems over the years, finding the malware issue to be increasingly critical. Zelonis

studied the methods used by pieces of malware to infect machines, as well as the vulnerabilities and end-user behaviors they exploit. She offers advice to prevent the future spread of malware, following the analogy of a medical pandemic.

2.2 Malware in the Windows Boot Sequence

One of the most important steps in combating malware is to trace its source. For system administrators and PC technicians tasked with removing malware from an affected machine, it is necessary to locate how the malware is called by the operating system for automatic execution. There are many ways for the malware to join the boot process, from simple startup folders to complex registry keys.

In their study "Deficiencies in Current Software Protection Mechanisms", Qattan & Thernelius observed numerous well-known Trojan horse malware specimens and documented their autostart techniques. In the process of their research, they used a qualitative method, equipped with numerous tools, to observe how malware injects itself into the boot processes of its victim machines.

Barwinski, in "Taxonomy of Spyware", utilized the freeware Autoruns for Windows tool, currently available for download from Microsoft (formerly Sysinternals). This tool automatically searches all known[1] autostart locations, including the file system, registry, shell extensions, driver packages, and many others. This tool is extremely valuable to monitor the goal of virtually malware, to have its code executed without the user's consent.

[1] According to Barwinski, even Microsoft does not know all possible autostart capabilities.

2.3 Investigating Malware

One major difficulty in understanding malware is its inherent lack of documentation. Since this software is typically installed without the user's consent or even knowledge, the author is not likely to include any information about what the software does, and especially not how it goes about doing it. Therefore, investigative steps must be taken in order to understand the behavior of a piece or entire class of malware.

One method of malware investigation is observation. This can be done by comparing the state of a system before and after malware activity. In his doctoral dissertation, "Enabling Internet Worms and Malware Investigation and Defense using Virtualization", Jiang, after intentionally making virtualized "honeypot" systems vulnerable to attack, performed forensic analyses on the systems. In different cases, this was done either by simply observing a machine for clues (e.g. Windows desktop wallpaper, which is sometimes changed by malware activity), browsing a directory (e.g. discovering the presence of *enbiei.exe*, evidence of Blaster worm activity), or perusing tool-assisted log data of the virtual machine.

In "Reverse Code Engineering", Konstantin Rozinov of Bell Labs did a complete study on reverse engineering a virus to better understand its behavior. He explained various types of virus infection techniques, and chose a simple virus, W32/Bagle, for analysis and reverse code engineering. The virus was not reported to have been executed in any test environment; its effects were only explained through annotated code. In this case, the researcher was proficient in code disassembly, and was able to fully understand and explain all aspects of the virus's code. In effect, this method results in a perfect analysis, with every piece of the virus meticulously explained, but in reality, it is inaccessible to many people affected by malware.

Since the focus of this study was to explore the usefulness of reverse code engineering in the battle against malware, this approach was very appropriate.

In "Measurement and Analysis of Autonomous Spreading Malware in a University Environment", Goebel, et al. analyzed malware to discover its spread across networks. They used a number of techniques and tools to monitor malware activity, including its effects on the local system. Using the CWSandbox tool for automatic behavior analysis, they were able to log the malware specimen's activity, such as changes to the file system and registry, which can be possible autostart targets. This is a valuable approach to malware analysis, but it fails to show the actual, tangible effects that malware can have on a production system. To better demonstrate the effects of malware on a machine, a complete simulation of a production system can be utilized.

The most complete malware analysis reports reside in the databases of major antivirus vendors. These companies, like Symantec, Kaspersky, McAfee, etc. are able to dedicate substantial resources to the discovery and understanding of all forms of malware, as it is an enormous part of their product offerings. The information these companies make available to the public is extremely valuable for malware research, as it describes numerous malware specimens in great detail.

2.4 Data Extraction

With the amount of information available from the Internet and related technologies, it is sometimes difficult to make any valuable conclusions; the amount of data is just overwhelming. To make this mass of information understandable, automated computer systems can process

this data and present its findings. Not surprisingly, many data extraction studies focus on computing-related data, as it is abundant on the Internet. In “Mining Web Logs to Debug Distant Connectivity Problems”, Kıcıman, et al. described algorithms to extract usable information from HTTP server logs, with the goal of identifying intermediate connectivity problems. This study was met with various challenges, but being that the data was all machine-written, data uniformity was not one of them.

Another study, “Detecting Mass-Mailing Worm Infected Hosts by Mining DNS Traffic Data”, actually applied data mining to the malware problem. In this study, Ishibashi et al. mined DNS data to discover evidence of mass-mailing worms, a type of malware that spreads by email. Like the above-mentioned study, Ishibashi et al. worked with machine-produced data, which was relatively consistent and easy to work with. In addition, they were clearly given access to this data by working with a major ISP, so automated collection of data was not required.

One paper that does focus on human-readable text as a target for data mining is “Untangling Text Data Mining” by Marti A. Hearst. In this paper, Hearst explains that text can be a rich source of information, but one that is difficult to be understood by a computer. She mentions the value of data mining being beyond “making things easier to find on the web”, the ability to extract new information from existing data. While this paper is not very technically detailed, it does describe multiple techniques for mining usable information from text, a concept very similar to this study.

3 Research Goal

This thesis provides insight into the automatic launch of malware on Windows operating systems. There are various ways for a piece of malware, once it has initially been executed on a machine, to inject itself into that machine's boot process, ensuring it will be executed each time the system is powered on. In addition to their malicious agenda, these startup processes can waste valuable system resources, decreasing end-user productivity and requiring administrator action for removal.

The method of this research also explores the feasibility and challenges of data extraction on a human-readable collection of information, the Symantec Threat Explorer. This database catalogs thousands of malware specimens, describing their behaviors: infection mechanisms, system modifications (including autostart methods), payloads, and removal instructions. The information is downloaded, searched, and processed with command-line PHP scripts, as an additional exercise in PHP's flexibility as a scripting language.

The Windows operating system is built to support a large range of hardware, software, and system configurations. To enable this flexibility, Microsoft created multiple methods for an application to execute automatically, a desirable feature in many situations, but one that is easily exploited for malicious purposes. These methods range from the easily viewable and user-modifiable, such as the Start Menu Startup folder, to the more obscure and difficult to pinpoint, those located deep in the registry. Each of these methods has certain properties to be exploited by a piece of malware. While simple malware might only insert itself into the Startup folder or the basic "Run" registry key (HKLM\Software\Microsoft\Windows\ CurrentVersion\Run), where it is executed as an application, more complicated specimens may

infect other areas of the registry. They may run a login script (HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon), replace the Windows shell (HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell), appear as a system service/device driver (HKLM\System\CurrentControlSet\Services), or exploit one of many other uncommon features, many not understood by even advanced users.

This research applies the aforementioned data extraction process to find trends among known pieces of malware, regarding their use and exploitation of the autostart capabilities of Microsoft Windows. These trends will explain the past and current state of malware startup techniques, as malicious programmers discover increasingly covert methods of launching their code, and help predict the future of these exploits, ultimately providing assistance in the seemingly endless war against malicious software.

4 Source of Data

The data extraction target, or source of data, for this study is the Symantec Threat Explorer. This website is described as "a comprehensive resource for daily, accurate and up-to-date information on the latest threats, risks and vulnerabilities." As the world's most popular security software vendor (by market share and revenue) (Gartner, Inc., 2009), Symantec has a responsibility to understand all types of security threats, including malware. When a piece of malware is discovered, it will be analyzed to discover how it functions, and how to protect against it. This information is utilized in Symantec's antivirus products, such as Norton Antivirus and Symantec Endpoint Security, and is additionally made publically available on the Threat Explorer website.

The Threat Explorer is organized as a human-readable database. It consists of an alphabetic index of malware specimens (Appendix L), a quick view of recently discovered malware, and the ability to search the entire content of the database. Each malware specimen is given its own page, linked from the index. This page is identified by a proprietary Symantec "docid" ID number, in the format <http://www.symantec.com/business/security_response/writeup.jsp?docid=YYYY-MMDD??-????-99>, where 'YYYY' is a 4-digit year[2], 'MM' is a month, 'DD' is a day, and '?' are seemingly arbitrary 0-9 digits.

The information on each malware specimen's page is broken down into three tabs, each accessible through a variable ("tabid") appended to the URL querystring. The first tab, "Summary" (tabid=1) contains a basic overview of the malware, with its discovery date, date

[2] While the first 4 digits of the "docid" correlate with discovery date of the malware in over 90% of cases, it is sometimes misleading. Therefore, this value is not used to find trends; the actual year of discovery is used instead.

the report was last updated, malware type, vulnerable operating systems, and a brief description of the malware. This tab also describes which Symantec virus definitions (used in the company's antivirus products) include information on this piece of malware. Finally, in more recent articles, a basic threat assessment is provided, with information on the malware's status in the wild, level of damage, and methods of distribution.

The second tab, "Technical Details" (tabid=2), is the primary focus of this data mining exercise. It contains some of the same information as the first tab, such as the discovery date, type of malware, and operating systems affected, but it also explains the malware's behavior in detail. Of particular interest to this study, the information on this tab typically describes file system and registry modifications, often explaining the autostart techniques used by the malware. This information is written by numerous different authors, each with their own style and format. While easy for a knowledgeable human to understand, these differences make automated data mining a challenge. Special processing must be performed to normalize the data into a format that can be easily analyzed.

The third tab, "Removal", (tabid=3) is of no interest to this study. It contains end-user instructions to eliminate a piece of malware from a compromised machine.

5 Challenges

This study is not without challenges. Most of these stem from the nature of the Symantec Threat Explorer database, and the methods of this research to automatically gather and analyze the data contained within.

The data is presented as a Web site, with each piece of malware on its own page. Therefore, the server must be queried thousands of times to gather all information presented. This amount of activity in a short amount of time could be viewed as an attack on their servers, and Symantec, being a computer security company, may block access as a security measure. To prevent this, it is important to limit server query density as much as possible, by observing a brief wait period between subsequent queries, and by caching as much data as possible.

Another challenge is the style of presentation of the technical details page. This data is intended to be read by humans to understand the behavior of a specific piece of malware, not to be automatically analyzed by a computer. Therefore, most information is presented in narrative prose, and, since there are multiple authors[3] working on these pages, there are significant variances in style and syntax. Because of this variance, it is impossible to simply search for patterns in the downloaded text; the data must first be normalized, taken from a range of possible formats and collected together in a common, easily searchable format. This adds substantial complexity to the data extraction process, but is necessary to ensure accurate results that are not affected by the article author's style.

[3] A separate data extraction script finds about 125 distinct authors. (Appendix H)

Yet another result of a human-authored information source is the propensity for errors. Symantec's process of analyzing malware, documenting its behavior, and presenting the information is performed primarily by employees, introducing the factor of human error. Many simple spelling and typographical errors have been observed in the Threat Explorer (see Appendix N for an example, there are three 'R's where there should only be two. While these errors do not affect human readability, (most go completely unnoticed) it creates a challenge for computer-based searching. It is important to mention that some "errors" could be intentional, such as in cases where the malware author uses a similar-looking name to disguise a file or registry key, or even an error by the malware author. This makes it impossible to implement an automatic spell check algorithm. Instead, common errors are mitigated at search time (e.g. forward slash instead of backslash, "Current Version" instead of "CurrentVersion") and the regular expressions used for pattern matching are written to be flexible. This implementation compensates for many errors without creating false positives.

To address errors, a post-process error checking script (Appendix G) was written, that compares previously matched strings with unmatched strings, and outputs those that are very similar (1-3 characters different). Many of these "errors" are intentional, as mentioned above, but some true errors were found. When common errors were found (e.g. "Current Version" instead of "CurrentVersion") the search script and/or regular expressions were adjusted to compensate. A few uncommon errors (within an acceptable margin) were left unaddressed. The output of this script can be found in Appendix O.

One final challenge is the difficulty in compiling a complete list of autostart methods. Methods have been added, removed, and modified with each release of Windows, and complete documentation does not exist. Numerous tools and references were utilized to compile a robust list of 101 autostart locations (Appendix K), but this list may be incomplete, especially in respect to older versions of Windows.

6 Methodology Overview

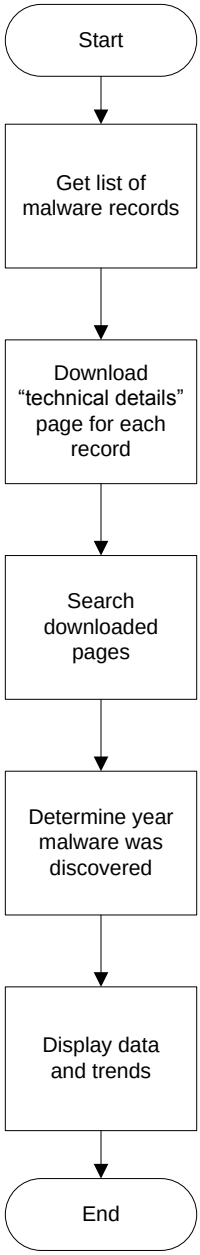


Figure 1: Methodology Overview Flowchart

Originally, this research was to consist of a hands-on, real-world analysis of numerous malware specimens, observing how they act on a machine, creating the files, registry keys, and other modifications necessary to ensure its automatic launch. After discussions with faculty, it was determined that this information already exists, in abundance, within malware description

databases provided by the major antivirus companies. These companies have considerable resources and experience in malware analysis; there would be little benefit to reproducing this information.

To best meet the purpose of this research, existing malware descriptions will be gathered and statistically analyzed. This study is focused on Symantec's Threat Explorer, a robust encyclopedia of various types of computer security threats. This database is freely available on the web, with built-in search and browsing functionality.

To analyze this data, it must first be automatically gathered. This is accomplished with a collection of PHP scripts. PHP is chosen for its vast set of features, particularly its built-in HTTP support, necessary for reading the pages presented by Symantec. In addition to simple regular expression pattern matching, which can be difficult to code and understand, these scripts utilize the Document Object Model (DOM) extension for PHP, which allows the parsing and manipulation of XML data, including HTML. This approach results in easily human-readable code that can remain functional even through minor changes to Symantec's format.

The first script simply compiles a list of all threats in the database, correlating each title with its respective "docid" number and risk type. This data is easily obtained from an HTML table on the "A-Z Threats and Risks" browse feature. The script stores the gathered data in a MySQL database (Appendix I).

Once a list of entries and "docid"s has been created, a second script queries the server for technical information on each entry. Records with certain risk types (see Script Details and

Appendix C) will be ignored. In order to reduce future queries to the Symantec server, this script stores the complete HTML content of each entry to a unique file for later analysis. To prevent an incident that could potentially result in being blocked from the server, this script will perform only one request, chosen at random from the list of "docid" numbers, at a time, pausing for a random time between subsequent queries.

A third script performs the processing and data locating from the gathered information. This script normalizes the data and utilizes PHP's pattern-matching search algorithms to locate key strings in each stored entry. If an autostart location is referenced in the entry, a record will be added to the 'findings' database table.

A simple supporting script is run to determine the year each malware record was discovered by Symantec. While this has no effect on the data extraction, it is necessary in order to display time-based trends in the presentation script.

Once this massive quantity of data is collected in the MySQL database, a final PHP script presents the data in a concise form, returning the results as HTML code to be viewed in a web browser. The script presents this data in HTML tables, which are easily imported into Microsoft Excel to create graphical charts.

7 Script Details

7.1 getids.php

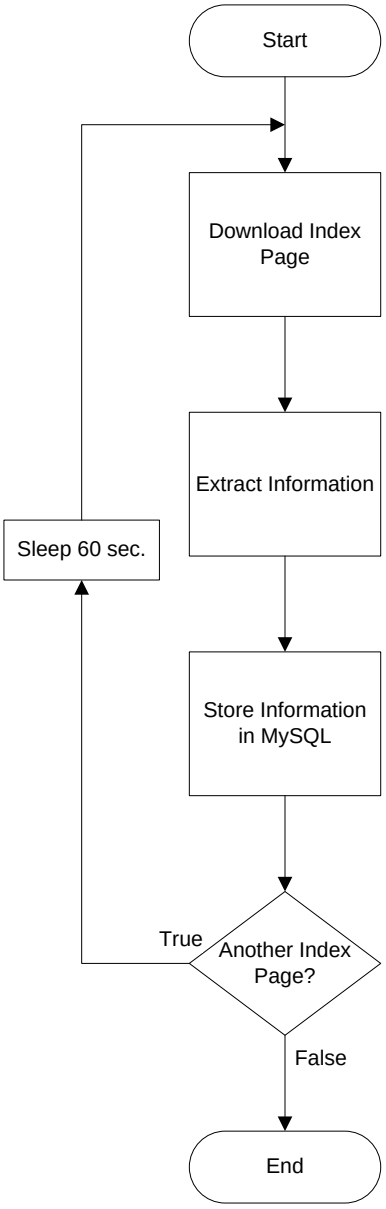


Figure 2: Program Flowchart of getids.php

This script queries the Symantec Web server for index pages, and gathers data on each malware entry. The URL *$url* for each index page is derived from a hard-coded URL combined with an 'azid' from an array of these IDs *$azids* (manually gathered and coded). The script loops through each *$azid*, and for each page, queries the server and stores its response in both a

runtime variable and a file (for debugging purposes). It then reads the page into a PHP DOMDocument object, gathers all HTML tables, and selects the third table, which is the actual listing of malware page links. The script then iterates through each row in the table, assigning variables to each table field. It gets the name of the threat *$name* and destination URL *$href* from column two, and extracts the 'docid' value *$docid* from that URL. It stores the risk type, if set, as *$risktype*. The script prints the 'docid', risk name, and risk type to the console, inserts them into the MySQL table *list*, and then repeats for the next line. Once all lines in the table have been operated on, the script sleeps for 60 seconds (to prevent hammering the server) and goes to work on the next index page. The PHP Document Object Model extension allows this script to be very short and efficient.

7.2 pulldetails.php

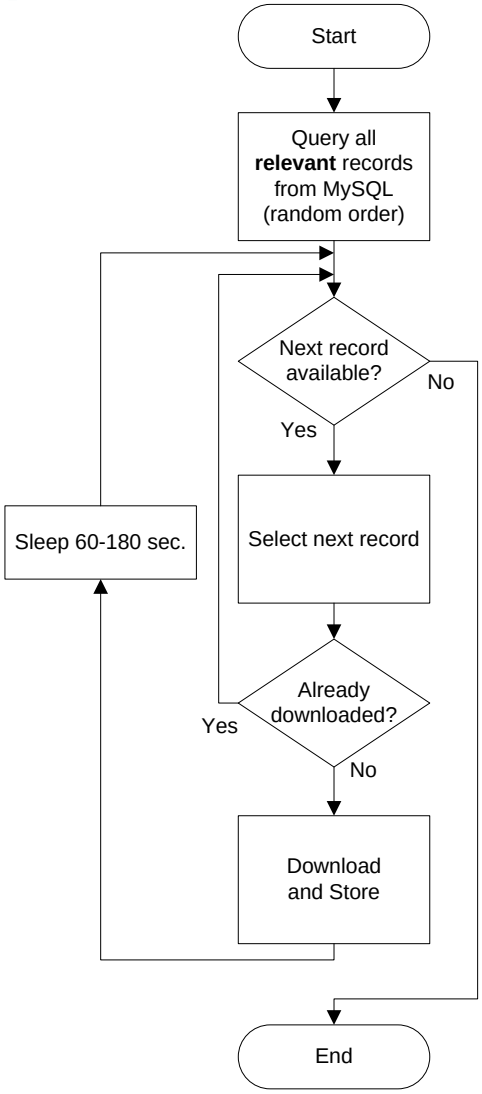


Figure 3: Program Flowchart for pulldetails.php

This script downloads the "Technical Details" page for each malware included in the MySQL table *list*. It starts by querying the MySQL server for *docid* entries in table *list*, excluding certain *risktype*s that are not relevant to this research ('Hoax', 'Parental Control', 'Security Assessment Tool', 'Hack Tool', 'Joke', 'Removal Tool'), in a random order. It iterates through each returned row and then checks if the file has already been downloaded and stored. If it has, the next row is checked. If the file has not yet been downloaded and stored, the script downloads the file from the Symantec server, with a URL consisting of a hard-coded portion and the *docid* from

the MySQL database, and saves it to disk. The script then sleeps for a random time between 60 and 180 seconds. Once all records have been downloaded, the script finishes.

7.3 fixyear.php

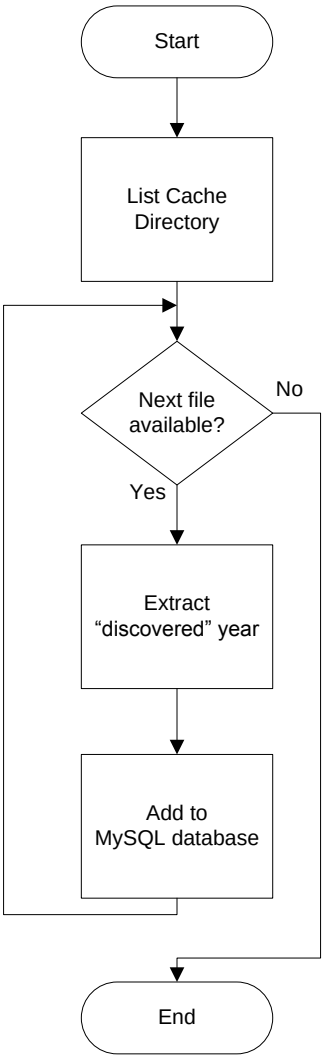


Figure 4: Program Flowchart for fixyear.php

In order to find trends in the malware records, it is necessary to know when each was created. While it is impossible to know precisely when most pieces of malware are written, it is safe to say that most are discovered quickly after being released. Therefore, we can use the "discovered" date from the technical details page. This script loops through every page saved by the previous script by listing the directory where the files are stored. It extracts the "docid"

from the filename for identification, and then sets up a DOMDocument object similar to getids.php. Using the DOM extension, the script selects the "tabModBdy" HTML element, where the textual malware description resides. It then loops through all child nodes of that element, searching for the string "Discovered: ". When this string is found, the script stores the value of that node as *$discovered_line*, then extracts the year (last 4 digits of the string) as *$discovered_year* and stops searching. This value is compared with the first 4 digits of the "docid" *$docid_year*. If the "year" values are different, the "discovered" year is stored in the MySQL database entry for this "docid". If they are the same, or if no "discovered" date was found, the "docid" year is stored. The script then repeats for the next file in the directory, until all files have been operated on.

7.4 search.php

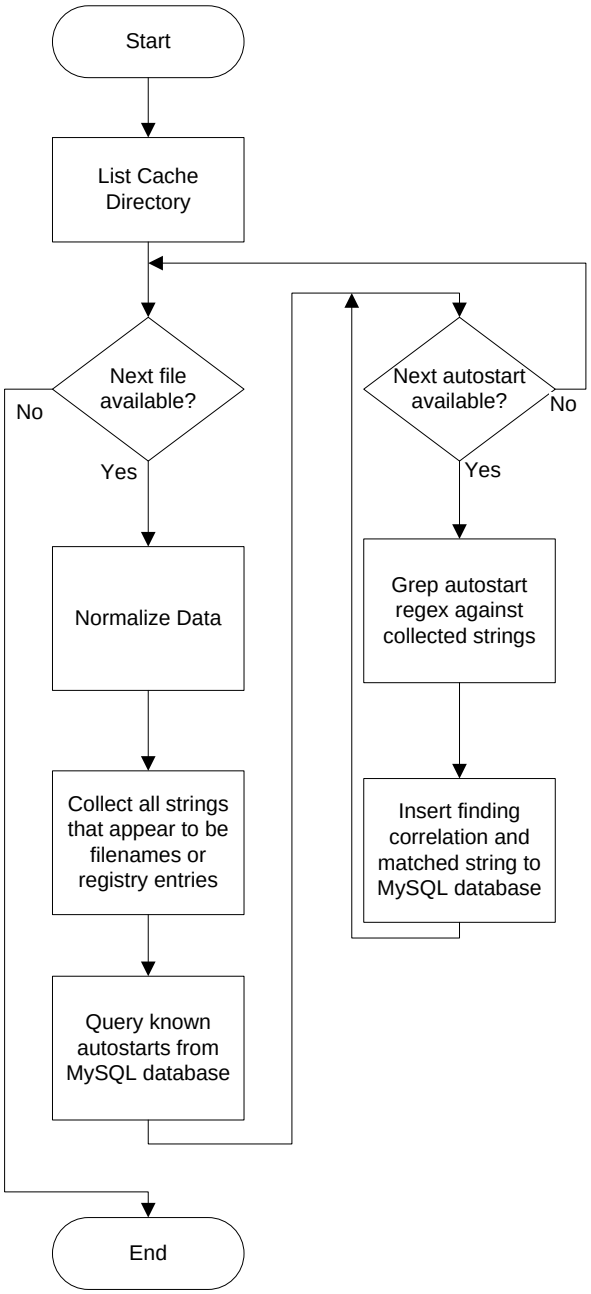


Figure 5: Program Flowchart for search.php

Once all records have been downloaded and stored, they can be analyzed. This script has two main functions for each malware record: to scan for and collect registry keys or file names, and then to pattern-match the findings against known Windows autostart locations. First, the script obtains a listing of the directory containing the cached technical details pages. Much like

fixyear.php, it loops through each filename, and reads the file into a variable *$html*. Unlike getids.php and fixyear.php, this script does not utilize the Document Object Model PHP extension, instead using string searches and pattern matching. This is done to preserve subtle syntax hints that are lost in DOM object handling. To extract the appropriate content from the page[4], the script locates the "tabModBdy" element by its HTML tag, and stores it as *$important_html*.

Once the appropriate HTML code has been extracted, it is normalized. First, the script removes extraneous HTML tags and line breaks. This makes the file paths and registry entries easily locatable. The next step is to reconstruct all registry entries into a common format for pattern matching. Many articles list a registry value name being placed into multiple keys (see Appendix O). The script appends the value name to the end of the paths, and collects these full paths. Other registry paths and file paths are also collected. Once these strings are collected, they are cleaned up (replacing incorrect usage of slashes/backslashes, stripping extraneous characters, etc.) and matched against the regular expressions stored in MySQL (Appendix K). If a match is found, a correlation between "docid" and "autorunid", as well as the complete matched string, are inserted into MySQL.

[4] There is approximately 30 KB of extraneous HTML in each downloaded page.

8 Results

The data extraction PHP scripts gathered a list of 10,349 unique records from the Symantec Threat Explorer database. Of these, 310 were deemed irrelevant to this research, for having risk types that imply something other than a malware description, such as jokes, hoaxes, or removal information. Figure 6 shows the remaining records by their year of discovery. There is a clear increase in the number of malware records reported by Symantec starting around 1999.

This trend is consistent with expectations. As usage of computers and the Internet increased, so did the amount of malware. The stabilization and later decrease can possibly be attributed to improvements in security measures, making malware development more difficult. At the time of this study, the year 2009 is still in progress, explaining the very small number of records for that year. Regardless, the amount of malware seems to be generally decreasing since 2005, certainly a positive trend.

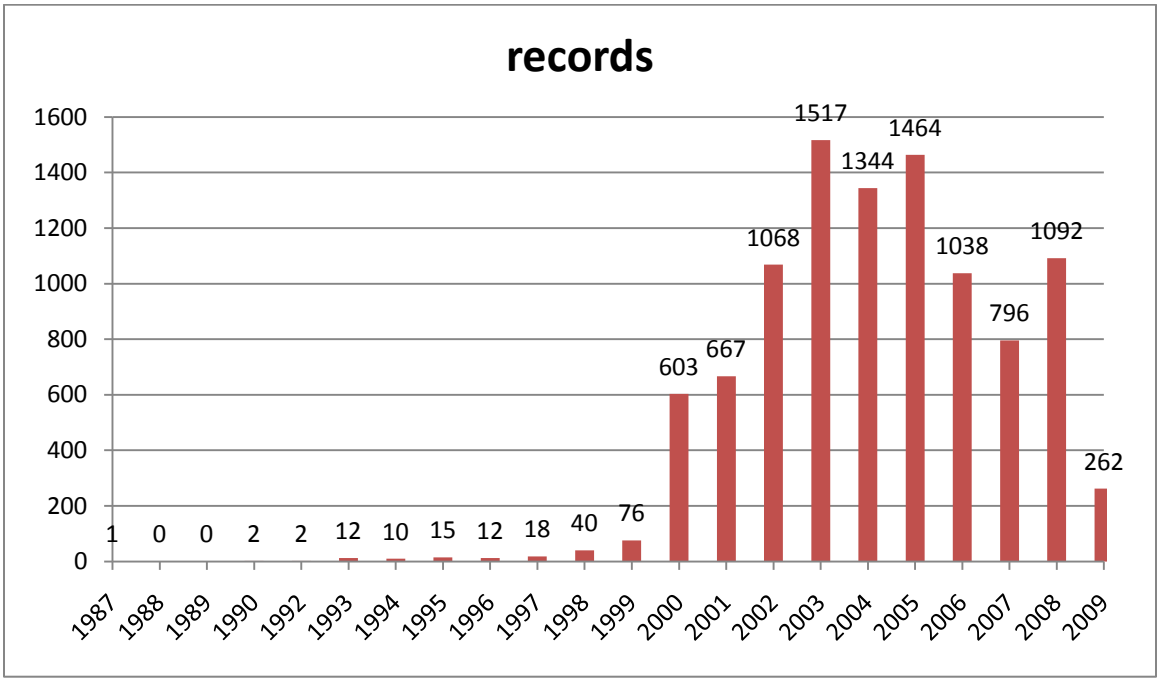


Figure 6: Threat Explorer Records per Year

The 10,039 relevant files were downloaded files and searched for known autostart locations, and 8,212 correlations were found. Figure 7 shows the number of correlations per year. It is important to note that some records contained multiple autostart methods, and some contained none at all. This explains why there are more findings than records in some years.

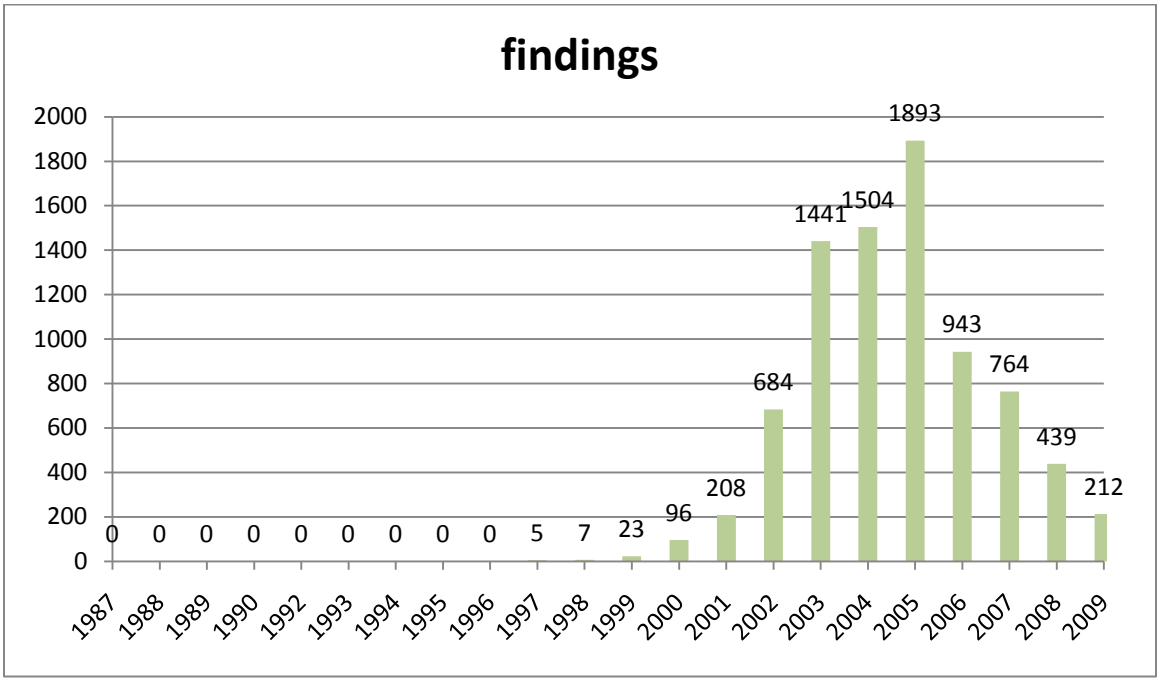


Figure 7: Autostart Location Findings per Year

While the number of findings per year is mostly similar to the number of records found in that given year, the year 2008 is a notable exception. Symantec included a large number of malware records without any technical details during this year. The file sizes of downloaded records are shown in Appendix I. There is a noticeable flat area in 2008 where all records were approximately 34 KB, the size of a page without any technical details. This explains the relatively low number of findings for that year.

8.1 Most Common Methods

Over 100 autostart locations were searched for, and 56 were located at least once. The complete data can be seen in Appendix A. The most common locations are described here.

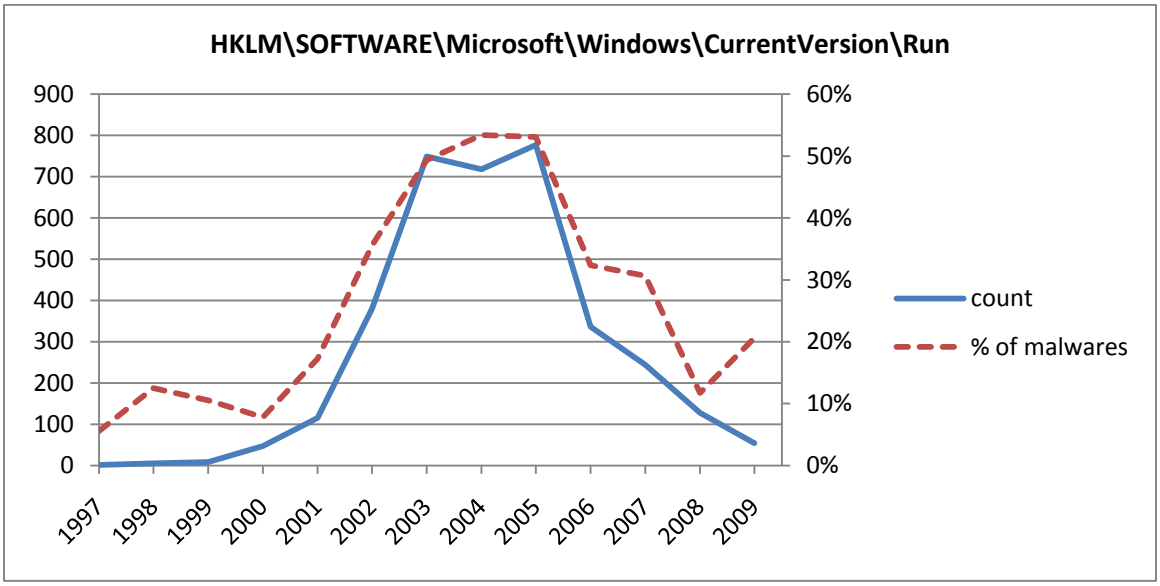


Figure 8: Yearly Findings of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

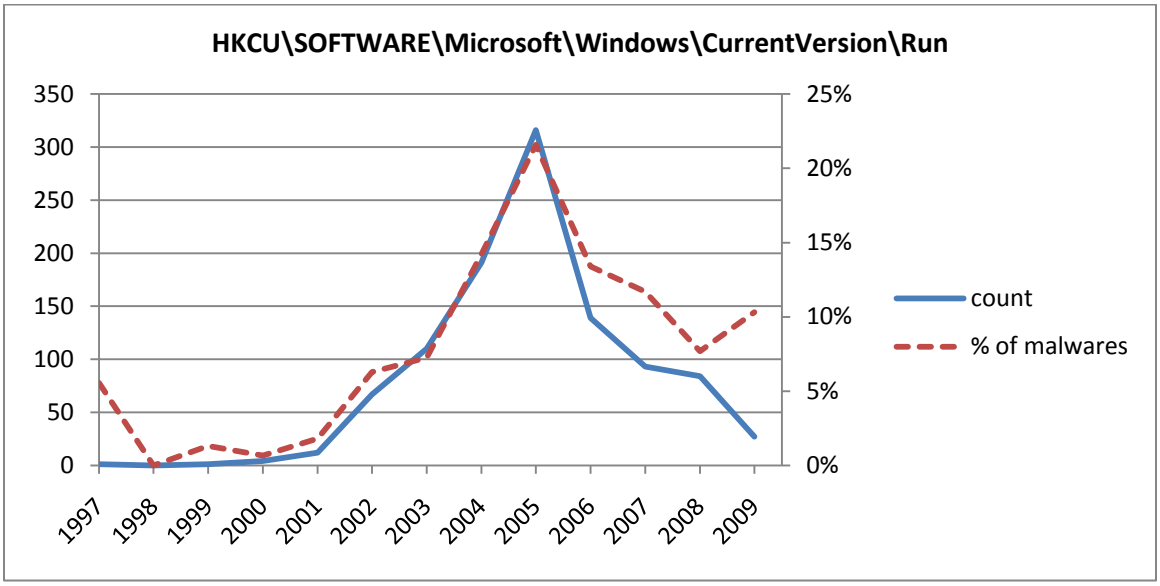


Figure 9: Yearly Findings of HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The two most common autostart locations found in the Symantec Threat Explorer are shown in Figure 8 and Figure 9. These two registry locations are very simple; any filename under this registry key is started, by Windows, during the boot up process. This method is used by many

legitimate applications to start automatically, such as messaging programs. Because of its relatively simplicity, and compatibility with all Windows operating systems, it is commonly used by malware as well. Fortunately, this is one of the most visible autostart locations for a knowledgeable user; the list of programs using this method can be seen with the 'msconfig' tool built in to all recent versions of Windows (Windows 2000 excepted). This allows users to enable or disable the automatic launch of programs that use this method through a simple checkbox user interface.

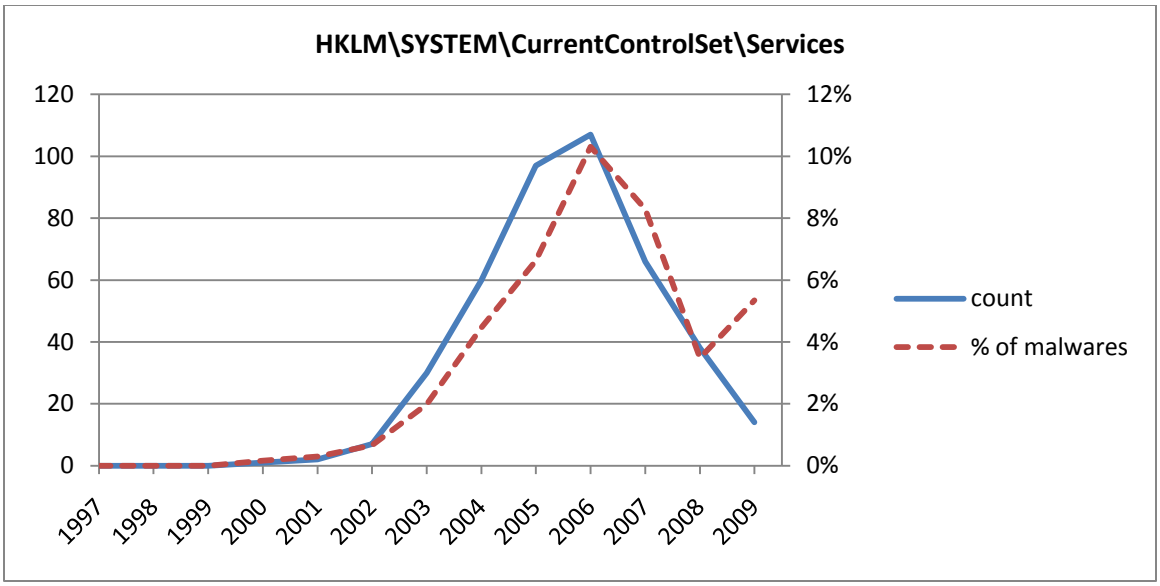


Figure 10: Yearly Findings of HKLM\SYSTEM\CurrentControlSet\Services

The fourth most common autostart location used by malwares reported in the Symantec Threat Explorer (the third can be seen under Mostly Obsolete Methods, below) is shown in Figure 10. This registry key is used for system service registrations, including drivers. Malware authors use this key to register their code as a system service, which are typically started automatically and maintained by the system. This can make it hard for an unknowledgeable user to locate and remove the malware. This form of system service is only supported on "NT-based" versions of Windows, the traditional "consumer-level" versions (95-Me) are not affected. This explains the rarity of this autostart method prior to the release of Windows XP in late 2001, when the "NT-based" kernel began to gain substantial market share. When this autostart method is utilized, it can be difficult to determine how the malware process starts. While the 'msconfig' tool can enable and disable system services, it is in a lesser-used area of the application, and the interface is more crowded and complex.

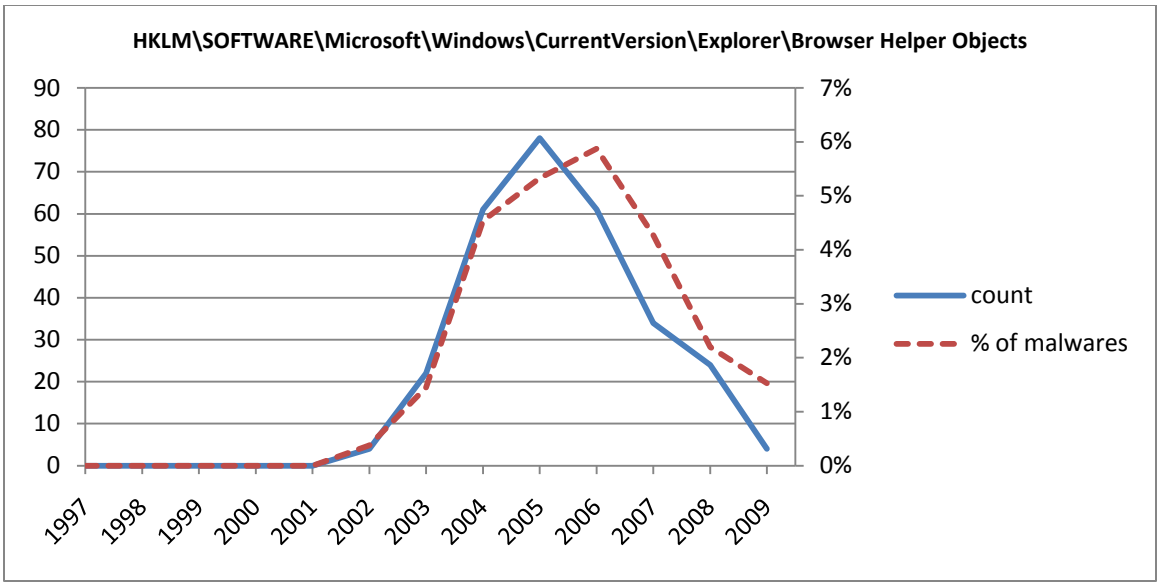


Figure 11: Yearly Findings of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

The fifth most common autostart location identified by this research does not actually invoke execution with the operating system, but instead Internet Explorer. Supported since the release of Internet Explorer 4.0 in 1997, a Browser Helper Object (BHO) is attached to every instance of the browser when it is opened. It can be used legitimately for browser add-ons such as toolbars and file viewer plugins, but malware may attach itself as a BHO to generate pop-up advertisements or record browsing activity. This method gained popularity among malware authors starting in 2002, and was present in 6% of malware discovered in 2006. As it runs within the iexplore.exe process, it is difficult for an end user to pinpoint. Internet Explorer 7, released in October 2006, includes a BHO management tool, allowing the user to easily view and disable unwanted add-ons without having to edit the registry. This feature, along with other browser security improvements, may have had an effect on the popularity of this method; its usage has steadily decreased since Internet Explorer 7 was released.

8.2 Mostly Obsolete Methods

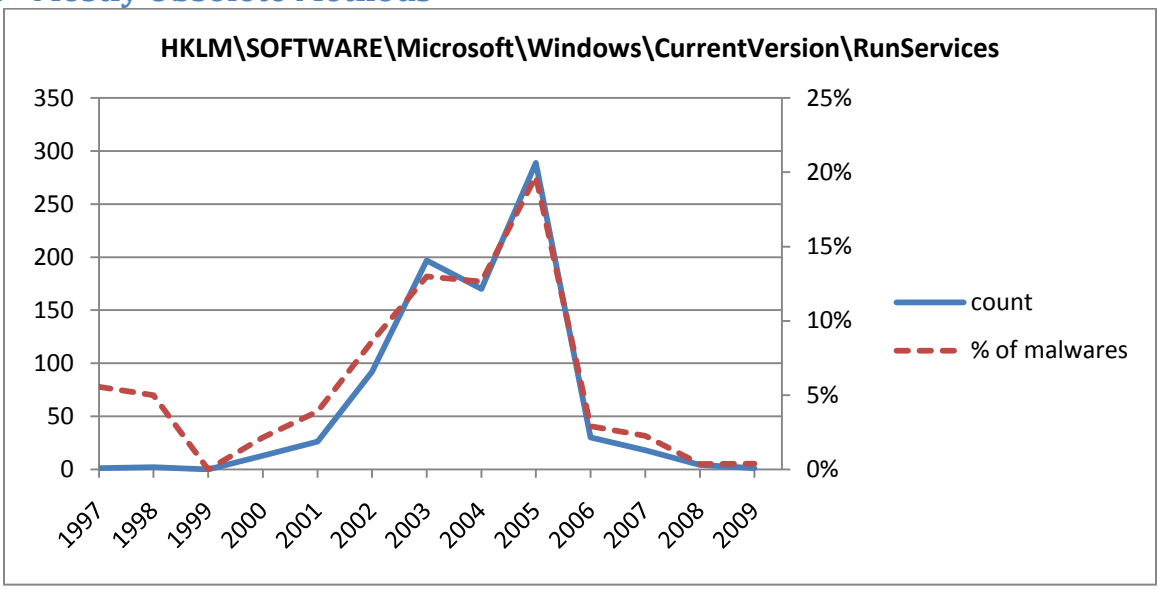


Figure 12: Yearly Findings of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

The third most common autostart location, as shown in Figure 12, displays an interesting trend. While this method was used by approximately 12% of all malware reported by Symantec between 1997 and 2005, its use decreased sharply in 2006, and is almost nonexistent since then. According to Microsoft Knowledge Base article 137367, this key, and a related 'RunServicesOnce' key, apply only to Windows 95, Windows 98, and Windows Millennium Edition (Me). This explains the substantial decrease in usage of this method around 2006, as Windows 98/Me lost market share to Windows XP, and later Windows Vista. Therefore, this autostart method can be considered deprecated and no longer a concern on modern systems.

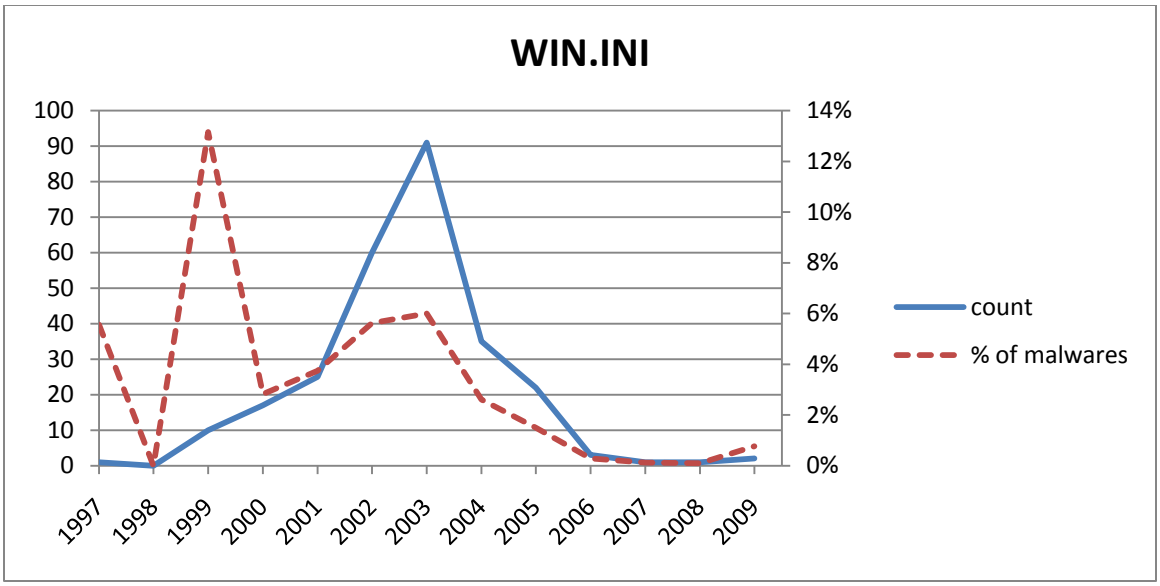


Figure 13: Yearly Findings of WIN.INI

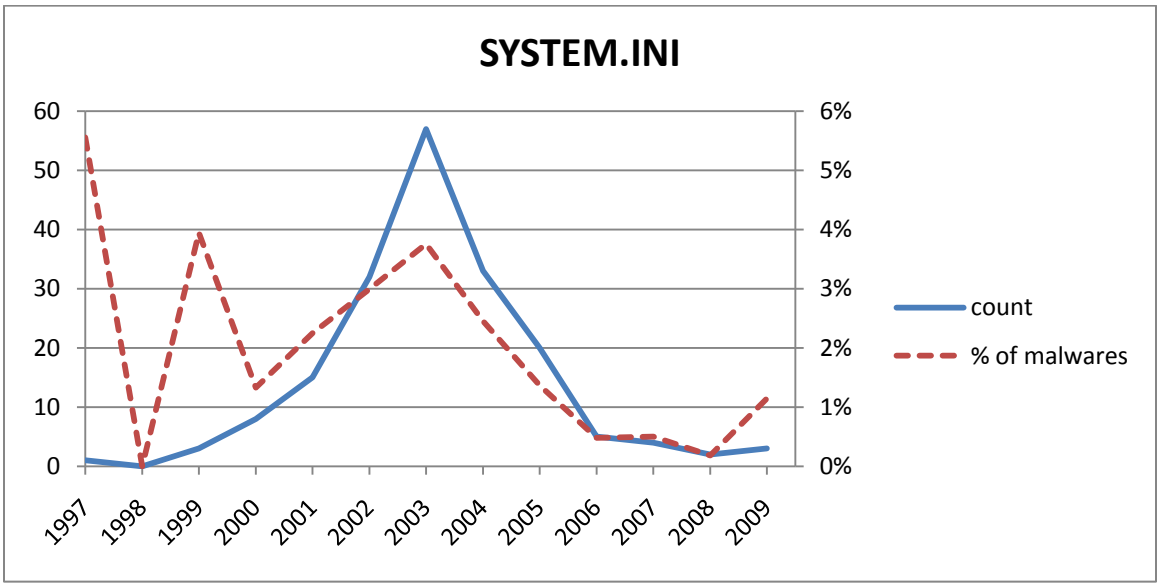


Figure 14: Yearly Findings of SYSTEM.INI

Two other mostly obsolete autostart methods are the WIN.INI and SYSTEM.INI files. These files were used in early versions of Windows for a wide range of configuration options, including automatic program execution. They were, in many ways, precursors to the Windows registry. While these files accounted for a substantial portion of malware autostarts in the 1990s and early 2000s, their use sharply decreased after 2003. This trend is presumably due to the increased popularity of Windows XP, which does not support these files as autostart methods.

8.3 Up-and-Coming Techniques

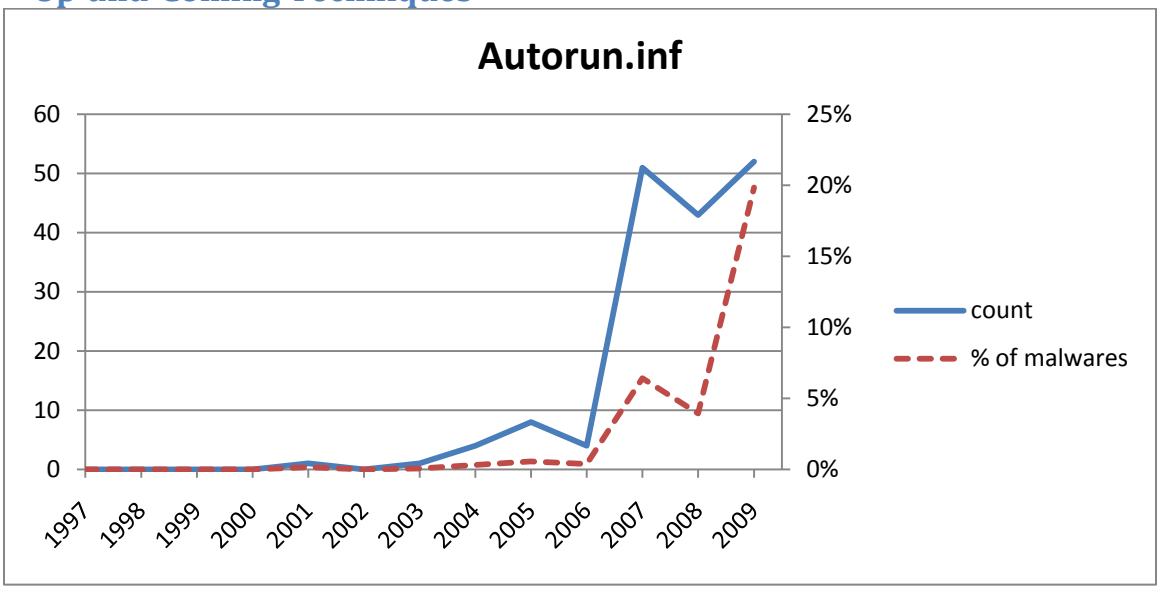


Figure 15: Yearly Findings of Autorun.inf

One relatively new malware autostart method takes advantage of the Windows AutoRun component, a feature intended to facilitate software installation and enhance the user experience by automatically running a command when a disk is mounted or a drive is "double-clicked". While this is a genuinely useful feature, malware authors have exploited this functionality not only to spread malware, but also for repeated execution on an infected machine. By simply creating an Autorun.inf file in the root of a volume, malicious code can be run any time a user inserts a disk or even attempts to browse a hard drive. Even when AutoRun is disabled on certain systems[5], the risk remains (Dormann, 2009). While Windows XP and earlier operating systems automatically run any application specified in the file, Windows Vista adds a layer of protection with a mandatory popup many before any application is launched. Measures such as this, combined with up-to-date security patches, may protect users from malware infection and prevent this autostart method from gaining much more popularity.

[5] A patch for this vulnerability was released in June 2008.

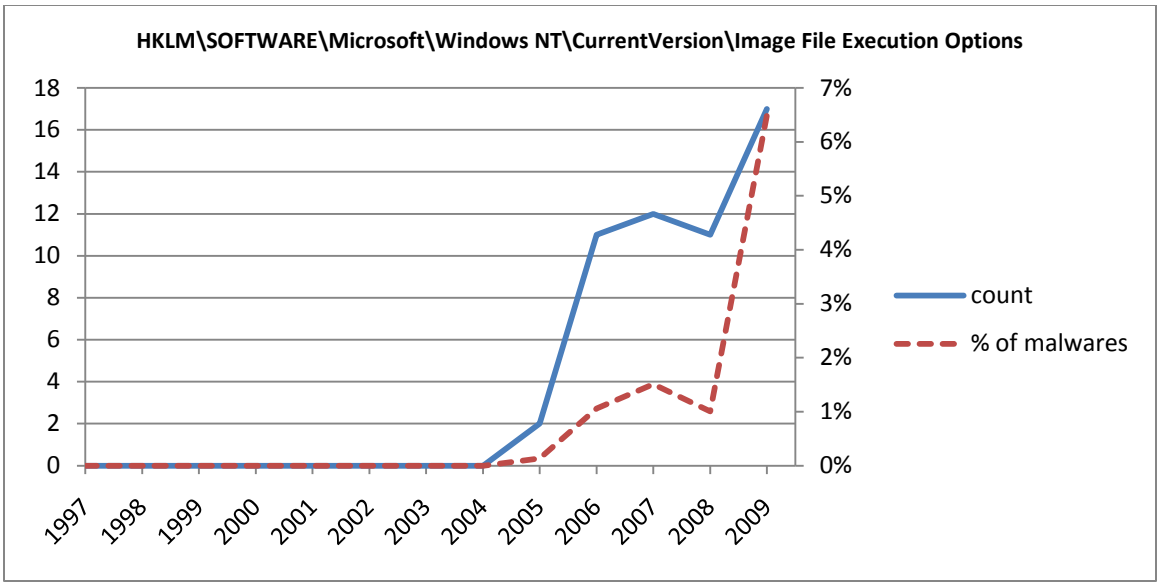


Figure 16: Yearly Findings for HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image Files Execution Options

Another dangerous autostart method, virtually unknown to most I.T. professionals, is the Image File Execution Options registry key. This key is part of a feature built into the Windows NT family of operating systems, legitimately used for software debugging. If a subkey exists for a given executable, the operating system will run the specified "debugger" instead of that executable. The debugger then runs the executable.

However, if a malicious executable is listed as a "debugger", it will be executed in place of the original application, no matter the context. To an end user, it will appear as though the original application has been overwritten with a malicious file, but replacing the application with a known clean version will not resolve the problem. Beyond the obvious capability of executing malicious files without the user's knowledge, this capability could potentially be very dangerous; critical security applications could be disabled with a simple registry key. (Zdrnja, 2008) Many tools that monitor startup entries, such as msconfig.exe, do not handle this registry key, making it invisible and unknown to all but the most knowledgeable experts.

This key was not utilized as a malware execution method until 2005. It has rapidly increased in popularity since then, and was present in over 6% of malwares discovered by Symantec in 2009. As this is an intended feature, it is not easy to disable this vulnerability, and it remains unpatched. A possible solution would be a forced confirmation window before starting the "debugger"; similar to what has been implemented for AutoRun in Windows Vista (above).

9 Future Work

There are possibilities for future research into this subject. This thesis is focused on a single primary source for malware analysis, the Symantec Threat Explorer. As malware is a significant problem in the computing world, multiple other firms provide details on the behavior of specific pieces of malware. While the Symantec Threat Explorer is very accurate, and possibly the most complete collection of technical information on malware, errors were observed throughout the course of this research. More accurate results could be obtained by cross-referencing data from multiple malware analysis sources.

Another possible area of future study would be to correlate the authors of the technical details pages to their individual styles. While this study uses code to "normalize" the data found in these pages, developing an understanding of each author's style, and having code that differentiates based on the author, could produce more accurate results.

Finally, there is a significant opportunity to increase program efficiency. For the purposes of this research, these scripts were written to be executed only once each, not as a continuous operation. Therefore, performance and efficiency were not much of a consideration. Not counting file download, which was made intentionally slow, the process of listing, searching, analyzing, and error checking the data contained in the Symantec Threat Explorer takes multiple hours, even on a high-end machine[6]. This could likely be reduced to a fraction of that time with proper optimization of the program code.

[6] System specifications: Intel Core 2 Duo E8400, 4 GB DDR2-1066 Memory, 4x 640 GB RAID 5 Array

10 Conclusion

This research met its goal to discover accurate and reliable trends on the usage of malware autostart techniques on Windows operating systems. While some of the results were expected, some curious trends were discovered that demonstrate both success in combating malware, as well as increasing popularity of dangerous upcoming threats.

Overcoming the many challenges of this research was not a superficial task. The variances in writing style and formatting were more substantial than expected, and the planned-simple code quickly became complex and inefficient. Data extraction from a human-readable source can be quite difficult, and this was no exception.

Regardless, the methodology of this study was very effective in meeting its goal. PHP is certainly a powerful language that has usage far beyond Web page preprocessing. Its flexibility and immense built-in features, especially combined with the equally impressive MySQL database solution, proved invaluable in the course of this research.

While this research only covers a very small portion of the massive malware epidemic, it is hoped that these findings will enhance professional understanding of these autostart techniques, especially the more obscure, to assist the battle against malware and improve computer security at large.

11 Works Cited

Barwinski, M. A. (2005). *Taxonomy of Spyware and Empirical Study of Network Drive-By-Downloads.* Masters Thesis, Naval Postgraduate School.

Dormann, W. (2009, April 14). *Vulnerability Note VU#889747.* Retrieved July 21, 2009, from US-CERT: http://www.kb.cert.org/vuls/id/889747

Esposito, D. (1999, January). *Browser Helper Objects: The Browser the Way You Want It.* Retrieved July 19, 2009, from MSDN: http://msdn.microsoft.com/en-us/library/bb250436(VS.85).aspx

Gartner, Inc. (2009, June 22). *Gartner Says Worldwide Security Software Revenue Grew 18.6 Per Cent in 2008.* Retrieved June 30, 2009, from Gartner Newsroom: http://www.gartner.com/it/page.jsp?id=1031712

Goebel, J., Holz, T., & Willems, C. (2007). *Measurement and Analsys of Autonomous Spreading Malware in a University Environment.* RWTH Aachen University, Center for Computing and Communication.

Hearst, M. A. (1999). *Untangling Text Data Mining.* Association for Computational Linguistics.

Ishibashi, K., Toyono, T., Toyama, K., Ishino, M., Ohshima, H., & Mizukoshi, I. (2005). *Detecting Mass-Mailing Worm Infected Hosts by Mining DNS Traffic Data.* NTT Corporation, NTT Information Sharing Platform Labs. Philadelphia: ACM.

Jiang, X. (2006). *Enabling Internet Worms and Malware Investigation and Defense using Virtualization.* PhD Thesis, Purdue University, Center for Education and Research in Information Assurance and Security.

Kıcıman, E., Maltz, D. A., Goldszmidt, M., & Platt, J. C. (2006). *Mining Web Logs to Debug Distant Connectivity Problems.* Microsoft Research. Pisa: ACM.

Microsoft Corporation. (2007, January 19). *Definition of the RunOnce Keys in the Registry.* Retrieved July 16, 2009, from Microsoft Help and Support: http://support.microsoft.com/kb/137367/EN-US/

Qattan, F., & Thernelius, F. (2004). *Deficiencies in Current Software Protection Mechanisms and Alternatives for Securing Computing Integrity.* Masters Thesis, Stockholm University - Royal Institute of Technology, Department of Computer and Systems Sciences.

Rozinov, K. (2004). *Reverse Code Engineering: An In-Depth Analysis of the Bagle Virus.* Bell Labs.

Russinovich, M., & Cogswell, B. (2009, April 6). *Autoruns for Windows v9.41.* Retrieved April 30, 2009, from Microsoft TechNet: http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx

Symantec Corporation. (2009, May 12). *Threat Explorer*. Retrieved May 17, 2009, from Symantec: http://www.symantec.com/business/security_response/threatexplorer/index.jsp

Symantec. (2008, April). *Symantec Internet Security Threat Report.* Retrieved April 12, 2009, from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf

The PHP Group. (2009, May 22). *Document Object Model.* Retrieved May 28, 2009, from PHP: Hypertext Preprocessor: http://us3.php.net/manual/en/book.dom.php

Wang, Y.-M., Roussev, R., Verbowski, C., Johnson, A., Wu, M.-W., Huang, Y., et al. (2004). Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management. *Large Installation System Administration , XVIII*, 33-46.

Wikipedia contributors. (2009, April 17). *Malware.* Retrieved April 20, 2009, from http://en.wikipedia.org/w/index.php?title=Malware&oldid=284374181

Zdrnja, B. (2008, February 28). *Abusing Image File Execution Options.* Retrieved July 25, 2009, from Internet Storm Center: http://isc.sans.org/diary.html?storyid=4039

Zelonis, K. (2004). *Avoiding the Cyber Pandemic: A Public Health Approach to Preventing Malware Propagation.* Masters Thesis, Carnegie Mellon University, Heinz School.

12 Appendix

location	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	total
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	4	6	10	40	115	380	750	719	776	333	247	125	55	**3562**
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	1	1	1	4	12	67	110	191	316	138	93	85	26	**1045**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices	2	3	1	9	26	92	197	170	289	30	18	4	1	**843**
HKLM\SYSTEM\CurrentControlSet\Services	0	0	0	1	2	7	32	59	97	106	66	38	14	**422**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	1	0	0	0	0	4	22	61	78	59	35	24	4	**288**
WIN.INI	1	1	11	12	25	60	91	35	22	3	1	1	2	**268**
SYSTEM.INI	1	0	4	7	15	32	57	33	20	5	4	2	3	**183**
Autorun.inf	0	0	0	0	1	0	1	4	8	4	51	43	52	**164**
C:\%windir%\All Users\Start Menu\Programs\Startup (All Users Startup)	0	0	1	2	5	11	45	28	13	10	24	9	4	**152**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	0	0	0	0	0	2	6	10	29	23	42	15	3	**130**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	0	0	1	2	3	14	21	31	23	6	10	5	2	**118**
HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar	0	0	0	0	0	0	11	26	35	13	7	1	0	**93**
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	0	0	0	0	1	3	17	6	15	13	18	6	11	**90**
C:\Documents and Settings\username\Start Menu\Programs\Startup (per user startup)	0	0	0	0	0	0	3	15	19	18	17	9	3	**84**
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	0	0	0	1	1	2	20	23	20	3	4	4	0	**78**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	0	0	0	0	0	0	3	1	7	18	27	13	3	**72**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	0	0	0	0	0	0	7	5	13	17	16	10	1	**69**
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Run	0	0	0	0	1	2	13	21	13	3	6	0	0	**59**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify	0	0	0	0	0	0	3	4	8	32	4	7	0	**58**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0	0	0	0	0	0	0	0	2	11	12	11	17	**53**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	0	0	0	0	0	0	5	18	11	7	9	0	0	**50**
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Load	0	0	0	0	0	0	5	7	14	13	8	0	0	**47**
HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions	0	0	0	0	1	0	2	6	13	12	3	0	0	**37**
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	0	0	0	0	0	1	0	3	4	8	4	3	5	**28**
HKCU\SOFTWARE\Microsoft\Internet Explorer\UrlSearchHooks	0	0	0	0	0	0	3	7	7	3	1	0	0	**21**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\System	0	0	0	0	0	0	2	0	3	6	7	2	0	**20**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx	0	0	0	0	0	0	5	4	5	3	1	1	0	**19**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce	0	0	0	0	1	5	4	2	2	1	1	1	0	**17**
HKCU\Control Panel\Desktop\Scrnsave.exe	0	0	0	0	0	0	2	2	3	2	3	3	1	**16**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	0	0	0	0	0	0	0	2	4	0	5	3	0	**14**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved	0	0	0	0	0	0	1	2	1	3	4	2	0	**13**
HKCU\SOFTWARE\Microsoft\Internet Explorer\Extensions	0	0	0	0	0	0	1	1	6	5	0	0	0	**13**
HKLM\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars	0	0	0	0	0	0	1	4	1	4	1	0	0	**11**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls	0	0	0	0	0	0	0	0	0	2	6	2	1	**11**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	0	0	0	0	0	0	0	4	2	1	0	0	0	**7**
HKLM\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries	0	0	0	0	0	0	1	0	3	0	1	1	1	**7**
HKLM\SOFTWARE\Classes\Protocols\Filter	0	0	0	0	0	0	1	1	2	2	1	0	0	**7**
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	0	0	0	0	0	0	0	0	0	1	2	2	2	**7**
HKCU\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars	0	0	0	0	0	0	0	2	2	1	0	1	0	**6**
HKCU\SOFTWARE\Microsoft\Command Processor\Autorun	0	0	0	0	0	0	0	1	0	2	2	0	0	**5**
HKCU\SOFTWARE\Microsoft\Active Setup\Installed Components	0	0	0	0	0	0	1	0	2	0	0	1	0	**4**
HKCU\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components	0	0	0	0	0	0	0	0	2	1	0	0	0	**3**
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers	0	0	0	0	0	0	0	0	0	0	3	0	0	**3**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	0	0	0	0	0	1	0	1	0	0	1	0	0	**3**
HKLM\SOFTWARE\Classes\Directory\ShellEx\ContextMenuHandlers	0	0	0	0	0	0	0	0	0	2	1	0	0	**3**
HKLM\SOFTWARE\Microsoft\Command Processor\Autorun	0	0	0	0	0	0	0	0	0	1	1	0	0	**2**
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved	0	0	0	0	0	0	0	0	0	1	0	1	0	**2**
HKLM\SOFTWARE\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance	0	0	0	0	0	0	0	0	0	2	0	0	0	**2**
HKLM\SOFTWARE\Classes\Protocols\Handler	0	0	0	0	0	0	0	2	0	0	0	0	0	**2**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32	0	0	0	0	0	0	0	0	0	0	1	0	1	**2**
HKLM\SOFTWARE\Classes\Folder\ShellEx\ContextMenuHandlers	0	0	0	0	0	0	0	0	0	1	0	0	0	**1**
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UIHost	0	0	0	0	0	0	0	0	0	0	0	1	0	**1**
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages	0	0	0	0	0	0	0	0	0	0	1	0	0	**1**
HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors	0	0	0	0	0	0	0	0	1	0	0	0	0	**1**
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute	0	0	0	0	0	0	0	0	0	0	0	1	0	**1**
HKLM\SOFTWARE\Classes\Exefile\Shell\Open\Command\(Default)	0	0	0	0	0	1	0	0	0	0	0	0	0	**1**

Appendix B: getids.php

```
<?php

// include mysql connect information
include "mysql.inc.php";


// array of page 'azid's
$azids =
Array('A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','_12345678
90');

// loop for each azid
foreach ($azids as $azid)
{
  // load page from symantec server
  $url = "http://www.symantec.com/business/security_response/threatexplorer/azlisting.jsp?azid=$azid";
  $response = file_get_contents($url ,"r");

  // cache page (for debug)
  file_put_contents("cache/$azid.txt", $response);

  // load page from cache (for debug)
  //$response = file_get_contents("cache/$azid.txt");



  // create new DOM object
  $dom = new domDocument;

  // load html from $response
  @$dom->loadHTML($response);

  // get all html tables in document
  $tables = $dom->getElementsByTagName('table');

  // select the third table (zero-indexed)
  $table = $tables->item(2);

  // get rows
  $rows = $table->getElementsByTagName('tr');

  // work on each row
  foreach ($rows as $row)
  {
    // assign variables to each table field
    $col1 = $row->firstChild;
    $col2 = $row->firstChild->nextSibling;
    $col3 = $row->firstChild->nextSibling->nextSibling;
    $col4 = $row->firstChild->nextSibling->nextSibling->nextSibling;
```

```
    // get threat name (value between <a> anchors)
    $name = $col2->firstChild->nodeValue;

    // get href value from <a> attribute
    $href = $col2->firstChild->attributes->getNamedItem('href')->value;

    // retrieve docid from href string
    // substr returns part of the string, specified by the location of "docid="
    // the "docid=" string itself is excluded with the +6
    $docid = substr($href, strpos($href, "docid=") + 6);

    // get risk type (if set)
    $risktype = isset($col3->firstChild) ? $col3->firstChild->nodeValue : "";

    // print results
    echo $docid;
    echo ": ";
    echo $name;
    echo ": ";
    echo $risktype;
    echo "\n";

    // escape special characters for SQL query
    $docid = mysql_real_escape_string($docid);
    $name = mysql_real_escape_string($name);
    $risktype = mysql_real_escape_string($risktype);

    // insert into mysql database
    mysql_query("INSERT INTO list (docid, name, risktype) VALUES ('$docid', '$name', '$risktype')");
  }// end row loop

  // delay execution 60 seconds (to prevent hammering web server)
  sleep(60);

}// end azid loop

?>
```

Appendix C: pulldetails.php

```
<?php

// include mysql connect information
include "mysql.inc.php";

////////////////////
//  LOOP THREATS  //
////////////////////

// risktypes to exclude (PHP Array format)
$excludes = Array('Hoax', 'Parental Control', 'Security Assessment Tool', 'Hack Tool', 'Joke', 'Removal Tool');

// put in format for sql query
$excludes_sql = "'" . implode("', '", $excludes) . "'";

// select threats from mysql list in random order, excluding risktypes above
$response = mysql_query("SELECT docid FROM list WHERE risktype NOT IN ($excludes_sql) ORDER BY RAND()");

// loop through response
while ($row = mysql_fetch_row($response))
{
  // get docid from mysql response
  $docid = $row[0];

  // if threat is not already cached
  if (!file_exists("cache/details/$docid.html"))
  {
    // print out docid
    echo $docid;
    echo "\n";

    // HTTP GET technical details for threat
    $url = "http://www.symantec.com/business/security_response/writeup.jsp?docid=$docid&tabid=2";
    if (($html = file_get_contents($url, "r")) !== FALSE)
    {
      // save html to disk
      file_put_contents("cache/details/$docid.html", $html);
    }

    // sleep between 60 and 180 seconds
    sleep(mt_rand(60,180));
  }
}

?>
```

Appendix D: fixyear.php

```
<?php

// include mysql connect information
include "mysql.inc.php";

// directory of cached details
$path = "cache/details";

// open directory handle
$dir = opendir($path);

// count current file
$file_count = 0;

// total number of files in directory
$num_files = count(glob("$path/*.*"));

// loop through each file
while (($file = readdir($dir)) !== false)
{
  // ignore . and ..
  if ($file != "." && $file != "..")
  {
    // increment file count
    $file_count++;

    // progress line
    echo $progress = sprintf("%.1f%% complete (%u/%u files scanned)", $file_count / $num_files * 100, $file_count,
$num_files);

    // backspace progress line
    echo str_repeat("\010", strlen($progress));

    // get docid from filename
    $docid = substr($file, 0, 19);

    // read file
    $html = file_get_contents($path . "/" . $file);

    // new domdocument
    $dom = new domDocument;

    // load html from $response
    @$dom->loadHTML($html);

    // get tabModBdy html element
    $tabmodbdy = $dom->getElementById("tabModBdy");

    // get children of tabModBdy
    $children = $tabmodbdy->childNodes;
```

```
    // look for 'discovered' line
    $discovered_line = "";
    $discovered_year = "";
    for ($index = 0; $index < $children->length; $index++)
    {
      // check if value contains "Discovered: "
      if (strpos($children->item($index)->nodeValue, "Discovered: ") !== FALSE)
      {
        // set discovered_line variable
        $discovered_line = $children->item($index)->nodeValue;

        // extract year (last 4 digits)
        $discovered_year = substr($discovered_line, -4);

        // stop looking, it has been found
        break;
      }
    }

    // get docid year from docid
    $docid_year = substr($docid, 0, 4);


    // compare discovered year (if not empty) to docid year
    if (!empty($discovered_year) && $discovered_year != $docid_year)
    {
      $fixed_year = $discovered_year;
    }
    else
    {
      $fixed_year = $docid_year;
    }

    // update list mysql table
    mysql_query("UPDATE list SET year='$fixed_year' WHERE docid='$docid'");

  }
}


?>
```

Appendix E: search.php

```
<?php

// count variables
$file_count = 0;

// start variable for running total of html analyzed
$totalimportant = "";

// include mysql connect information
include "mysql.inc.php";

// fetch mysql autoruns
// this is static throughout execution of this script
$autoruns_result = mysql_query("SELECT id, location, regex FROM autoruns");

// directory of cached details
$path = "cache/details";

// open directory handle
$dir = opendir($path);

// total number of files in directory
$num_files = count(glob("$path/*.*"));

// loop through each file
while (($file = readdir($dir)) !== false)
{
  // ignore . and ..
  if ($file != "." && $file != "..")
  {
    // increment file count
    $file_count++;

    // progress line
    echo $progress = sprintf("%.1f%% complete (%u/%u files scanned)", $file_count / $num_files * 100, $file_count,
$num_files);

    // backspace progress line
    echo str_repeat("\010", strlen($progress));


    // read file
    $html = file_get_contents($path . "/" . $file);

    //
    // select important part of html (where the actual details are listed)
    // cannot use DOM because no consistent pattern, and html "hints" are needed for regex matching
    //

    // strings to begin and end "important html"
```

```
    $begin_str = '<div id="tabModBdy">';
    $end_str   = '<div id="tabModFtr">';

    // find position of each
    $begin_pos = strpos($html, $begin_str);
    $end_pos   = strpos($html, $end_str);

    // substring between begin and end
    $important_html = substr($html, $begin_pos, ($end_pos - $begin_pos));

    //
    // normalize formatting
    //

    // combine neighboring tt blocks so long as next line is not new registry key or file path
    $important_html = preg_replace("/<\\/tt>(<br>)?[\r\n]?<tt>(?!(HKLM|HKCU|HKEY)|C:)/", "", $important_html);

    // remove html line breaks between directory portions (formatting)
    $important_html = preg_replace("/\\\\<br>[\r\n]/", "\\", $important_html);


    //
    // reconstruct registry "values" to full path (where listed as "in the registry subkey")
    //

    // create new array for reconstructed findings
    $back_finds = Array();

    // find backwards listings, where name and value are specified before the key
    //preg_match_all('/the values?:.*?((HKCU|HKLM|HKEY)[^<]*)/is', $important_html, $back_listings);
    preg_match_all('/the values?:?<br>.*?(?:((?:HKCU|HKLM|HKEY)[^<]*)(?:<\/tt>|<br>|\s*|<tt>)*)+/is', $important_html,
$back_listings);

    // go through each backwards listing
    foreach ($back_listings[0] as $back_pathkey => $back_listing)
    {
      // find registry entry names and values
      preg_match_all('/(?:>|&quot;)((?:&lt;)?[A-Za-z0-9\ \.\+\[\]\(\)]+(?:&gt;)?)(?:\t|=|&quot;| )[^<]/is',
$back_listing, $back_names);
      // find base paths (could be multiple)
      preg_match_all('/(?:HKCU|HKLM|HKEY)[^<]*/is', $back_listing, $back_reg_paths);

      // go through base paths
      foreach ($back_reg_paths[0] as $back_reg_path)
      {
        // go through names
        foreach ($back_names[1] as $back_name)
        {
          //
          // re-establish order of registry paths and names
          //
```

```
            // full path of registry entry (trim whitespace from both portions)
            $back_reg_fullpath = trim($back_reg_path) . "\\" . trim($back_name);

            // add to $back_finds
            $back_finds[] = $back_reg_fullpath;
          }
        }
      }
      //
      // end reconstruct backwards registry entries

      // combine important html to a file for testing
      $totalimportant .= $important_html;

      // gather all registry text (may have duplicates from "backwards listings", but will not affect final results)
      preg_match_all('/(HKLM|HKCU|HKEY)[^<=]*/is', $important_html, $reg_finds);

      // gather anything that looks like a file path -- this may include extra words at the end, but these will not
affect later searching
      preg_match_all('/[\b>](C:|%.+?%)\\\\[^<]*/is', $important_html, $file_finds);

      // gather ini files (popular in win95-ME era)
      preg_match_all('/\b[A-Z]*?\.ini/is', $important_html, $ini_finds);


      // combine all findings for this file
      $all_findings = Array();

      // go through backwards findings
      foreach ($back_finds as $back_find)
      {
        // add to $all_findings
        $all_findings[] = $back_find;
      }

      // go through other registry findings
      foreach ($reg_finds[0] as $reg_find)
      {
        // trim whitespace
        $reg_find = trim($reg_find);

        // remove extraneous punctuation
        $reg_find = rtrim($reg_find, "().,-:");

        $all_findings[] = $reg_find;
      }
      foreach ($file_finds[0] as $file_find)
      {
        // trim whitespace
        $file_find = trim($file_find);

        // trim first '>' character if exists
```

```
      $file_find = ltrim($file_find, ">");

      // add to $all_findings
      $all_findings[] = $file_find;
    }
    foreach ($ini_finds[0] as $ini_find)
    {
      // add to $all_findings
      $all_findings[] = $ini_find;
    }


    // cleanup all_findings (remove remaining formatting or blatant errors)
    $all_findings = str_replace("\\\\", "\\", $all_findings);
    $all_findings = str_replace("/", "\\", $all_findings);
    $all_findings = array_map("strip_tags", $all_findings);
    $all_findings = str_replace('"', '', $all_findings);
    $all_findings = str_replace('&quot;', '', $all_findings);
    $all_findings = str_replace('HKEY_LOCAL_MACHINE%', 'HKEY_LOCAL_MACHINE', $all_findings);
    $all_findings = str_replace('\\Current Version\\', '\\CurrentVersion\\', $all_findings);


    // reset $autoruns_result pointer
    mysql_data_seek($autoruns_result, 0);

    // array of matches (debug)
    $matches = Array();

    // loop through regexes
    while ($row = mysql_fetch_array($autoruns_result))
    {
      // grep all_findings with current regex
      $matches = preg_grep($row['regex'], $all_findings);

      // if something was found
      if (!empty($matches))
      {
//      echo "FOUND ($file): " . $row['location'];
//      echo "\n";

        mysql_query("INSERT INTO findings (docid, autorunid) VALUES ('" . substr($file, 0, 19) . "', '{$row['id']}')");
      }

      // add matched location strings to mysql table for error-checking comparison (next script)
      foreach ($matches as $match)
      {
        // remove trailing backslash (eliminate functionally identical duplicates)
        $match = rtrim($match, "\\");

        // escape special characters (mostly backslashes)
        $sql_match = mysql_real_escape_string($match);
```

```
        // query mysql
        mysql_query("INSERT INTO matches (location) VALUES ('$sql_match')");
      }
    }
  }
}

file_put_contents("important.html", $totalimportant);

?>
```

Appendix F: results.php

```
<?php

function display_results($mysql_result, $title)
{
  // print out title heading
  echo "<h2>$title</h2>\n";

  // create table
  echo "<table border=\"1\">\n";


  // print headings
  echo "<tr>";

  // iterate through fields for names
  for ($header_field = 0; $header_field < mysql_num_fields($mysql_result); $header_field++)
  {
    echo "<th>";
    echo mysql_field_name($mysql_result, $header_field);
    echo "</th>";
  }

  // finish headings
  echo "</tr>\n";

  // iterate through rows for data
  for ($row = 0; $row < mysql_num_rows($mysql_result); $row++)
  {
    // new row
    echo "<tr>";

    // iterate through fields
    for ($field = 0; $field < mysql_num_fields($mysql_result); $field++)
    {
      echo "<td>";
      echo mysql_result($mysql_result, $row, $field);
      echo "</td>";
    }

    // end row
    echo "</tr>\n";
  }

  // close table
  echo "</table>";
}
?>

<?php
```

```
// include mysql connect information
include "mysql.inc.php";

$result = mysql_query("SELECT year, COUNT(DISTINCT(list.docid)) AS records, COUNT(findings.docid) AS findings,
COUNT(findings.docid)/COUNT(DISTINCT(list.docid)) AS normalized FROM list LEFT OUTER JOIN findings ON
list.docid=findings.docid GROUP BY year");
echo mysql_error();
display_results($result, "Per Year");

//$result = mysql_query("SELECT year, autoruns.location, COUNT(findings.autorunid) AS 'malwares using method',
COUNT(findings.autorunid)/(SELECT COUNT(docid) FROM list WHERE LEFT(list.docid, 4) = LEFT(findings.docid, 4))*100 AS
'normalized with total yearly records' FROM autoruns JOIN findings ON autoruns.id = findings.autorunid GROUP BY id,
year");
//$result = mysql_query("SELECT list.year, autoruns.location, COUNT(findings.autorunid) FROM list LEFT OUTER JOIN
findings ON list.docid=findings.docid JOIN autoruns ON findings.autorunid=autoruns.id GROUP BY year, autorunid");
$result = mysql_query("SELECT autoruns.location, SUM(IF(year = 1997, 1, 0)) AS '1997', SUM(IF(year = 1998, 1, 0)) AS
'1998', SUM(IF(year = 1999, 1, 0)) AS '1999', SUM(IF(year = 2000, 1, 0)) AS '2000', SUM(IF(year = 2001, 1, 0)) AS
'2001', SUM(IF(year = 2002, 1, 0)) AS '2002', SUM(IF(year = 2003, 1, 0)) AS '2003', SUM(IF(year = 2004, 1, 0)) AS
'2004', SUM(IF(year = 2005, 1, 0)) AS '2005', SUM(IF(year = 2006, 1, 0)) AS '2006', SUM(IF(year = 2007, 1, 0)) AS
'2007', SUM(IF(year = 2008, 1, 0)) AS '2008', SUM(IF(year = 2009, 1, 0)) AS '2009', COUNT(findings.autorunid) AS 'total'
FROM list LEFT OUTER JOIN findings ON list.docid=findings.docid JOIN autoruns ON findings.autorunid=autoruns.id GROUP BY
autorunid ORDER BY total DESC");
display_results($result, "Yearly Popularity of Each Autostart Method");
echo mysql_error();

//$result = mysql_query("SELECT autoruns.location,COUNT(findings.autorunid) FROM autoruns LEFT OUTER JOIN findings ON
autoruns.id = findings.autorunid GROUP BY id ORDER BY COUNT(findings.autorunid) DESC");
//display_results($result, "Total Count of Each Autostart Method");
//echo mysql_error();

$result = mysql_query("SELECT * FROM autoruns");
display_results($result, "autoruns and regular expressions");

//$result = mysql_query("SELECT list.year, CASE LEFT(autoruns.location, 2) WHEN 'HK' THEN 'registry' WHEN 'C:' THEN
'file system' ELSE IF(RIGHT(autoruns.location, 4) = '.INI', 'INI file', 'other') END AS type, COUNT(findings.autorunid)
FROM list JOIN findings ON list.docid = findings.docid JOIN autoruns ON autoruns.id = findings.autorunid GROUP BY year,
type ORDER BY type, year");
$result = mysql_query("SELECT list.year, COUNT(IF(LEFT(autoruns.location, 2) = 'HK', 1, NULL)) AS 'registry',
COUNT(IF(LEFT(autoruns.location, 2) = 'C:', 1, NULL)) AS 'start menu', COUNT(IF(RIGHT(autoruns.location, 4) = '.INI', 1,
NULL)) AS 'INI file', COUNT(IF(autoruns.location = 'Autorun.inf', 1, NULL)) AS 'Autorun.inf' FROM list JOIN findings ON
list.docid = findings.docid JOIN autoruns ON autoruns.id = findings.autorunid GROUP BY year ORDER BY year");
display_results($result, "registry vs. filesystem by year");
echo mysql_error();



?>
```

Appendix G: errorcheck.php

```
<?php

// verbose constant - set to true to show more information
define("VERBOSE", true);

// count variables
$file_count = 0;

// open file to save found errors
$error_file = fopen('errors.txt', 'w');

// array of found "errors"
$found_errors = Array();

// include mysql connect information
include "mysql.inc.php";

// fetch mysql autoruns and matches
// these are static throughout execution of this script
$autoruns_result = mysql_query("SELECT id, location, regex FROM autoruns");
$location_result = mysql_query("SELECT DISTINCT(location) FROM matches");


// directory of cached details
$path = "cache/details";

// open directory handle
$dir = opendir($path);

// total number of files in directory
$num_files = count(glob("$path/*.*"));

// loop through each file
while (($file = readdir($dir)) !== false)
{
  // ignore . and ..
  if ($file != "." && $file != "..")
  {
    // increment file count
    $file_count++;

    // progress line
    echo $progress = sprintf("%.1f%% complete (%u/%u files scanned)", $file_count / $num_files * 100, $file_count,
$num_files);

    // backspace progress line
    echo str_repeat("\010", strlen($progress));


    // read file
```

```
    $html = file_get_contents($path . "/" . $file);

    //
    // select important part of html (where the actual details are listed)
    // cannot use DOM because no consistent pattern, and html "hints" are needed for regex matching
    //

    // strings to begin and end "important html"
    $begin_str = '<div id="tabModBdy">';
    $end_str   = '<div id="tabModFtr">';

    // find position of each
    $begin_pos = strpos($html, $begin_str);
    $end_pos   = strpos($html, $end_str);

    // substring between begin and end
    $important_html = substr($html, $begin_pos, ($end_pos - $begin_pos));

    //
    // normalize formatting
    //

    // combine neighboring tt blocks so long as next line is not new registry key or file path
    $important_html = preg_replace("/<\\/tt>(<br>)?[\r\n]?<tt>(?!(HKLM|HKCU|HKEY)|C:)/", "", $important_html);

    // remove html line breaks between directory portions (formatting)
    $important_html = preg_replace("/\\\\<br>[\r\n]/", "\\", $important_html);


    //
    // reconstruct registry "values" to full path (where listed as "in the registry subkey")
    //

    // create new array for reconstructed findings
    $back_finds = Array();

    // find backwards listings, where name and value are specified before the key
    preg_match_all('/the values?:?<br>.*?(?:((?:HKCU|HKLM|HKEY)[^<]*)(?:<\/tt>|<br>|\s*|<tt>)*)+/is', $important_html,
$back_listings);

    // go through each backwards listing
    foreach ($back_listings[0] as $back_pathkey => $back_listing)
    {
      // find registry entry names and values
      preg_match_all('/(?:>|&quot;)((?:&lt;)?[A-Za-z0-9\ \.\+\[\]\(\)]+(?:&gt;)?)(?:\t|=|&quot;| )[^<]/is',
$back_listing, $back_names);
      // find base paths (could be multiple)
      preg_match_all('/(?:HKCU|HKLM|HKEY)[^<]*/is', $back_listing, $back_reg_paths);

      // go through base paths
      foreach ($back_reg_paths[0] as $back_reg_path)
      {
```

```
        // go through names
        foreach ($back_names[1] as $back_name)
        {
          //
          // re-establish order of registry paths and names
          //

          // full path of registry entry (trim whitespace from both portions)
          $back_reg_fullpath = trim($back_reg_path) . "\\" . trim($back_name);

          // add to $back_finds
          $back_finds[] = $back_reg_fullpath;
        }
      }
    }
    //
    // end reconstruct backwards registry entries


    // gather all registry text (may have duplicates from "backwards listings", but will not affect final results)
    preg_match_all('/(HKLM|HKCU|HKEY)[^<=]*/is', $important_html, $reg_finds);

    // gather anything that looks like a file path -- this may include extra words at the end, but these will not
affect later searching
    preg_match_all('/[\b>](C:|%.+?%)\\\\[^<]*/is', $important_html, $file_finds);

    // gather ini files (popular in win95-ME era)
    preg_match_all('/\b[A-Z]*?\.ini/is', $important_html, $ini_finds);


    // combine all findings for this file
    $all_findings = Array();

    // go through backwards findings
    foreach ($back_finds as $back_find)
    {
      // add to $all_findings
      $all_findings[] = $back_find;
    }

    // go through other registry findings
    foreach ($reg_finds[0] as $reg_find)
    {
      // trim whitespace
      $reg_find = trim($reg_find);

      // add to $all_findings
      $all_findings[] = $reg_find;
    }
    foreach ($file_finds[0] as $file_find)
    {
      // trim whitespace
```

```
  $file_find = trim($file_find);

  // trim first '>' character if exists
  $file_find = ltrim($file_find, ">");

  // add to $all_findings
  $all_findings[] = $file_find;
}
foreach ($ini_finds[0] as $ini_find)
{
  // add to $all_findings
  $all_findings[] = $ini_find;
}


// cleanup all_findings (remove remaining formatting or blatant errors)
$all_findings = str_replace("\\\\", "\\", $all_findings);
$all_findings = str_replace("/", "\\", $all_findings);
$all_findings = array_map("strip_tags", $all_findings);
$all_findings = str_replace('"', '', $all_findings);
$all_findings = str_replace('&quot;', '', $all_findings);
$all_findings = str_replace('HKEY_LOCAL_MACHINE%', 'HKEY_LOCAL_MACHINE', $all_findings);
$all_findings = str_replace('\\Current Version\\', '\\CurrentVersion\\', $all_findings);

//
// find matches just as search.php does
//
// reset $autoruns_result pointer
mysql_data_seek($autoruns_result, 0);

// array of matches
$matches = Array();

// array of unmatched findings
// findings are removed as they are matched
$unmatched_findings = $all_findings;

// loop through regexes
while ($row = mysql_fetch_array($autoruns_result))
{
  // grep all_findings with current regex
  $matches = preg_grep($row['regex'], $all_findings);

  $unmatched_findings = array_diff($unmatched_findings, $matches);
}

//
// look for spelling/typographical errors in unmatched findings
// by comparing with matched findings in ALL files
//
```

```
    // compare all findings in this file to all matched locations from MySQL
    foreach ($unmatched_findings as $finding)
    {
      // reset $location_result pointer
      mysql_data_seek($location_result, 0);

      // loop through found locations
      while ($row = mysql_fetch_array($location_result))
      {

        // only check if length <= 255 -- levenshtein cannot work on longer strings
        if (strlen($finding) <= 255)
        {
          // calculate levenshtein distance
          $l_distance = levenshtein(strtoupper($finding), strtoupper($row['location']));

          // set threshold to cubic root of string length
          $l_threshold = pow(strlen($finding), 1/3);

          // set upper limit of threshold to 3 characters
          $l_threshold = min($l_threshold, 3);

          if ($l_distance > 0 && $l_distance < $l_threshold)
          {
            // add "error" finding to array
            $found_errors[] = $finding;

            if (VERBOSE)
            {
                  $output = $finding . " vs " . $row['location'] . "\n";

                  echo $output;
                  fwrite($error_file, $output);
            }

            // prevent comparing same finding multiple times in same file
            break;
          }
        }

      }
    }

  }
}

// sort & summarize
sort($found_errors);
$summarized_errors = array_count_values($found_errors);
arsort($summarized_errors);
```

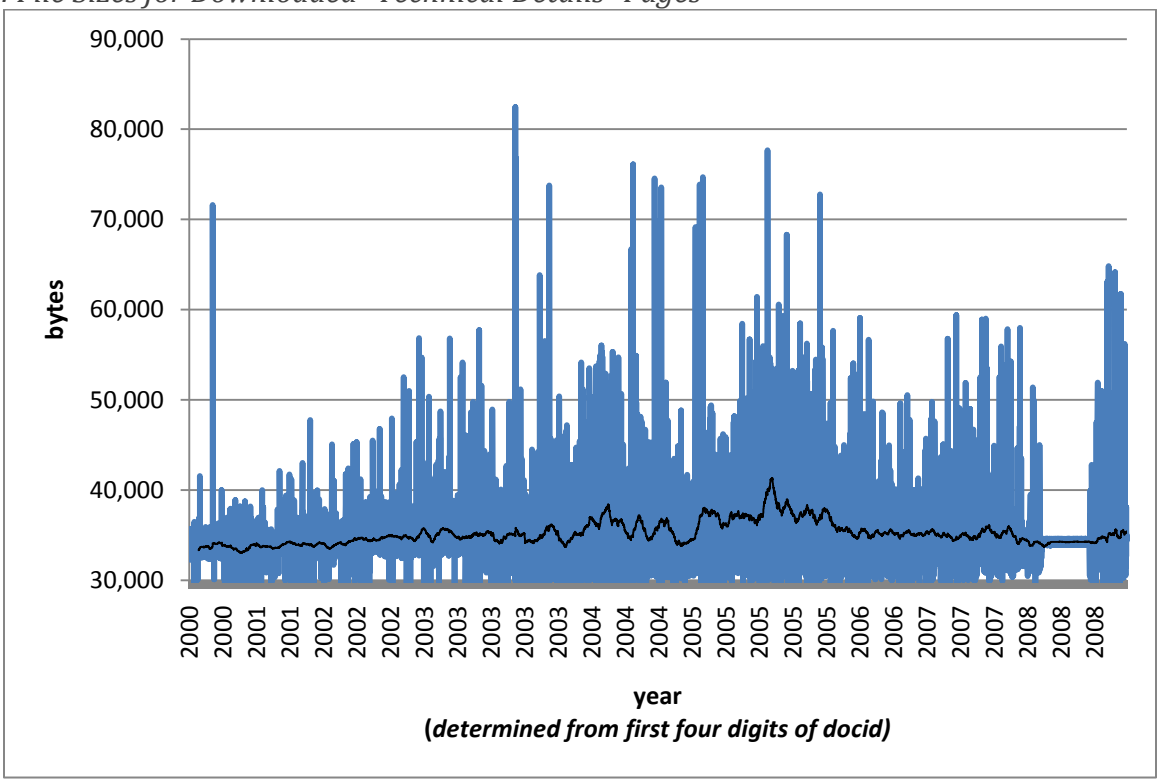
```
// print summary
$summary_heading = "==========================================\n";
$summary_heading .= "          SUMMARY OF ERRORS FOUND          \n";
if (!VERBOSE)
  $summary_heading .= "enable VERBOSE constant for more information\n";
$summary_heading .= "==========================================\n";

echo $summary_heading;
fwrite($error_file, $summary_heading);

// loop summarized
foreach ($summarized_errors as $error => $frequency)
{
  // create output
  $summary_line = "($frequency found) $error\n";

  // print output to console and file
  echo $summary_line;
  fwrite($error_file, $summary_line);
}


// close error output file
fclose($error_file);

?>
```

Appendix H: authors.php

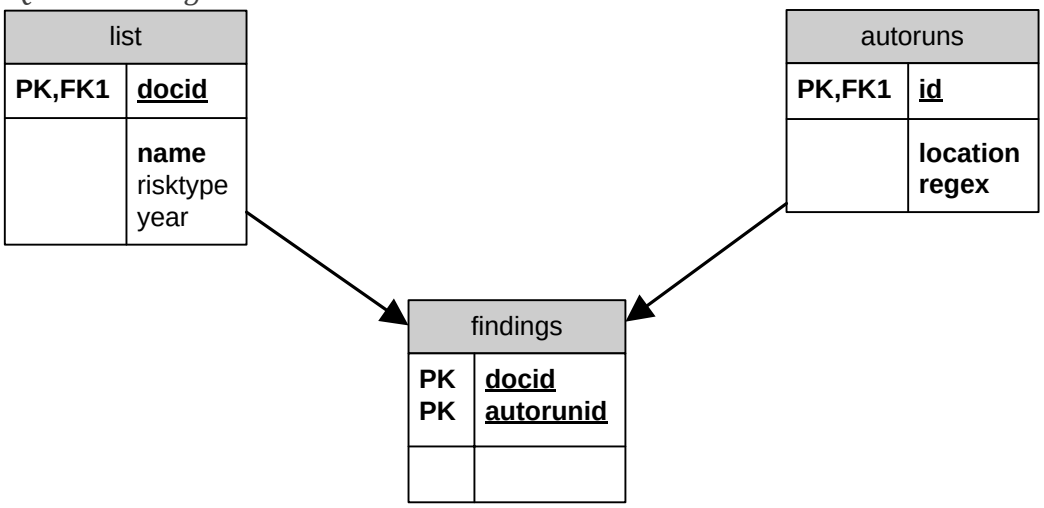
```
<?php

////////////////////
//  LOOP THREATS  //
////////////////////

// directory of cached details
$path = "cache/details";

// open directory handle
$dir = opendir($path);

// array of authors
$authors = Array();

// loop through each file
while (($file = readdir($dir)) !== false)
{
  // ignore . and ..
  if ($file != "." && $file != "..")
  {
    // read file
    $html = file_get_contents($path . "/" . $file);

    // new domdocument
    $dom = new domDocument;

    // load html from $response
    @$dom->loadHTML($html);

    // get tabModBdy html element
    $tabmodbdy = $dom->getElementById("tabModBdy");

    // get children of tabModBdy
    $children = $tabmodbdy->childNodes;

    // look for 'writeup by' line
    $author_line = "";
    for ($index = 0; $index < $children->length; $index++)
    {
      // check if value contains "Discovered: "
      if (strpos($children->item($index)->nodeValue, "Writeup By: ") !== FALSE)
      {
        // set discovered_line variable
        $writeup_line = $children->item($index)->nodeValue;

        $author_line = substr($writeup_line, strpos($writeup_line, "Writeup By: ") + 12);

        // break up multiple authors
        $author_line = preg_replace("/( and|\\&|\\;)/", ",", $author_line);
```

```
        $author_line = str_replace(", ", ",", $author_line);
        $author_line = str_replace(",,", ",", $author_line);

        $these_authors = explode(",", $author_line);

        // add author to array
        $authors = array_merge($authors, $these_authors);

        // stop looking, it has been found
        break;
      }
    }
  }
}

//
// done searching files, process array
//

// remove duplicates
$authors = array_unique($authors);
sort($authors);

// calculate soundex for each author entry in array
$soundexes = array_map("soundex", $authors);

$combined = (array_combine($soundexes, $authors));

foreach ($combined as $author)
{
  echo $author;
  echo ": ";
  echo soundex($author);
  echo "\n";
}

echo "\n";
echo count($authors) . " \"unique\" authors";
echo "\n";
echo count($combined) . " corrected for errors";

?>
```

Appendix I: File Sizes for Downloaded "Technical Details" Pages



Appendix J: MySQL Table Diagram



Appendix K: 'autoruns' MySQL Table

id	location	regex
1	Autorun.inf	/Autorun\.inf/i
2	WIN.INI	/WIN\.INI/i
3	SYSTEM.INI	/SYSTEM\.INI/i
4	C:\%windir%\All Users\Start Menu\Programs\Startup (All Users Startup)	/(C:\\)?(%?Windows%?|%Windir%|Documents and Settings|WINNT\\Profiles)(\\(All Users|%AllUsers(Profile)?%))?\\Start Menu\\Programs\\Start ?up/i
5	C:\Documents and Settings\username\Start Menu\Programs\Startup (per user startup)	/(C:\\)?((Documents and Settings|(%?Windows%?|%windir%|winnt)\\Profiles)\\.*?(profile|current user|user ?name).*?|%user ?profile%)\\Start Menu\\Programs\\Start ?up/i
6	HKCU\Control Panel\Desktop\Scrnsave.exe	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\Control Panel\\Desktop\\Scrnsave\.exe/i
7	HKCU\SOFTWARE\Classes*\ShellEx\ContextMenuHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\.*?\\ShellEx\\ContextMenuHandlers/i
8	HKCU\SOFTWARE\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\AllFileSystemObjects\\ShellEx\\ContextMenuHandlers/i
9	HKCU\SOFTWARE\Classes\Directory\Background\ShellEx\ContextMenuHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Directory\\Background\\ShellEx\\ContextMenuHandlers/i
10	HKCU\SOFTWARE\Classes\Directory\ShellEx\ContextMenuHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Directory\\ShellEx\\ContextMenuHandlers/i
11	HKCU\SOFTWARE\Classes\Directory\Shellex\CopyHookHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Directory\\Shellex\\CopyHookHandlers/i
12	HKCU\SOFTWARE\Classes\Directory\Shellex\DragDropHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Directory\\Shellex\\DragDropHandlers/i
13	HKCU\SOFTWARE\Classes\Directory\Shellex\PropertySheetHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Directory\\Shellex\\PropertySheetHandlers/i
14	HKCU\SOFTWARE\Classes\Exefile\Shell\Open\Command\(Default)	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Exefile\\Shell\\Open\\Command\\(Default)/i
15	HKCU\SOFTWARE\Classes\Folder\Shellex\ColumnHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Folder\\Shellex\\ColumnHandlers/i
16	HKCU\SOFTWARE\Classes\Folder\ShellEx\ContextMenuHandlers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Classes\\Folder\\ShellEx\\ContextMenuHandlers/i
17	HKCU\SOFTWARE\Microsoft\Active Setup\Installed Components	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Active Setup\\Installed Components/i

18	HKCU\SOFTWARE\Microsoft\Command Processor\Autorun	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Command Processor\\Autorun/i
19	HKCU\SOFTWARE\Microsoft\Ctf\LangBarAddin	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Ctf\\LangBarAddin/i
20	HKCU\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Internet Explorer\\Desktop\\Components/i
21	HKCU\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Internet Explorer\\Explorer Bars/i
22	HKCU\SOFTWARE\Microsoft\Internet Explorer\Extensions	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Internet Explorer\\Extensions/i
23	HKCU\SOFTWARE\Microsoft\Internet Explorer\UrlSearchHooks	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Internet Explorer\\UrlSearchHooks/i
24	HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Load	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\Load/i
25	HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Run	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\Run/i
26	HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Shell/i
27	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ShellIconOverlayIdentifiers/i
28	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run/i
29	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Shell	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\Shell/i
30	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\Software\\Microsoft\\Windows\\CurrentVersion\\Run(?!Once)/i
31	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce/i
32	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Shell Extensions\\Approved/i
33	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ShellServiceObjectDelayLoad/i
34	HKCU\SOFTWARE\Policies\Microsoft\Windows\SYSTEM\Scripts\Logoff	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Policies\\Microsoft\\Windows\\SYSTEM\\Scripts\\Logoff/i
35	HKCU\SOFTWARE\Policies\Microsoft\Windows\SYSTEM\Scripts\Logon	/(HKEY_CURRENT_USER|HKCU|HKEY_USERS?\\\.DEFAULT)\\SOFTWARE\\Policies\\Microsoft\\Windows\\SYSTEM\\Scripts\\Logon/i

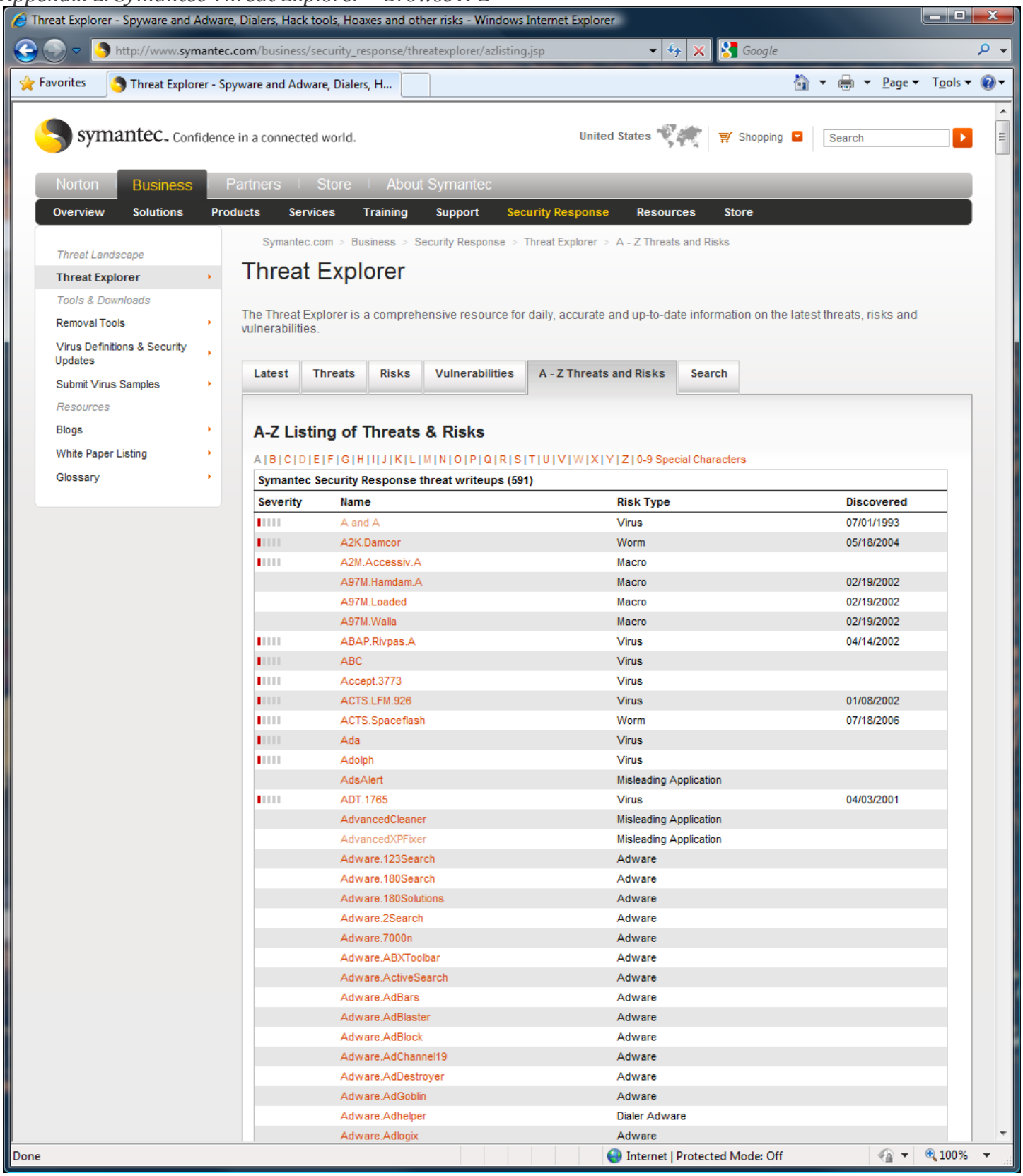
36	HKLM\SOFTWARE\Classes\AllFileSystemObjects\ShellEx\ ContextMenuHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\AllFileSystemObjects\\ShellEx\\ ContextMenuHandlers/i
37	HKLM\SOFTWARE\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\CLSID\\{083863F1-70DE-11d0-BD40-00A0C911CE86}\\Instance/i
38	HKLM\SOFTWARE\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\CLSID\\{7ED96837-96F0-4812-B211-F13C24117ED3}\\Instance/i
39	HKLM\SOFTWARE\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\CLSID\\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\\Instance/i
40	HKLM\SOFTWARE\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\CLSID\\{AC757296-3522-4E11-9862-C17BE5A1767E}\\Instance/i
41	HKLM\SOFTWARE\Classes\Directory\Background\ShellEx\ ContextMenuHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Directory\\Background\\ShellEx\\ ContextMenuHandlers/i
42	HKLM\SOFTWARE\Classes\Directory\ShellEx\ ContextMenuHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Directory\\ShellEx\\ ContextMenuHandlers/i
43	HKLM\SOFTWARE\Classes\Directory\Shellex\ CopyHookHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Directory\\Shellex\\ CopyHookHandlers/i
44	HKLM\SOFTWARE\Classes\Directory\Shellex\ DragDropHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Directory\\Shellex\\ DragDropHandlers/i
45	HKLM\SOFTWARE\Classes\Directory\Shellex\ PropertySheetHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Directory\\Shellex\\ PropertySheetHandlers/i
46	HKLM\SOFTWARE\Classes\Exefile\Shell\Open\Command\ (Default)	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Exefile\\Shell\\Open\\Command\\ (Default)/i
47	HKLM\SOFTWARE\Classes\Filter	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Filter/i
48	HKLM\SOFTWARE\Classes\Folder\Shellex\ColumnHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Folder\\Shellex\\ColumnHandlers/i
49	HKLM\SOFTWARE\Classes\Folder\ShellEx\ ContextMenuHandlers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Folder\\ShellEx\\ ContextMenuHandlers/i
50	HKLM\SOFTWARE\Classes\Protocols\Filter	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Protocols\\Filter/i
51	HKLM\SOFTWARE\Classes\Protocols\Handler	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Classes\\Protocols\\Handler/i
52	HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Active Setup\\ Installed Components/i
53	HKLM\SOFTWARE\Microsoft\Command Processor\Autorun	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Command Processor\\Autorun/i
54	HKLM\SOFTWARE\Microsoft\Ctf\LangBarAddin	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Ctf\\LangBarAddin/i
55	HKLM\SOFTWARE\Microsoft\Internet Explorer\Explorer Bars	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Internet Explorer\\ Explorer Bars/i
56	HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Internet Explorer\\Extensions/i

57	HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Internet Explorer\\Toolbar/i
58	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Drivers32	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Drivers32/i
59	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Image File Execution Options/i
60	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Windows\Appinit_Dlls	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Windows\\Appinit_Dlls/i
61	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\GinaDLL	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\GinaDLL/i
62	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\Notify	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\Notify/i
63	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\SaveDumpStart	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\SaveDumpStart/i
64	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\Shell	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\Shell/i
65	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\System	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\System/i
66	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\Taskman	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\Taskman/i
67	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\UIHost	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\UIHost/i
68	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon\Userinit	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ Winlogon\\Userinit/i
69	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Authentication\Credential Provider Filters	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Authentication\\Credential Provider Filters/i
70	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Authentication\Credential Providers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Authentication\\Credential Providers/i
71	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Authentication\PLAP Providers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Authentication\\PLAP Providers/i
72	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Browser Helper Objects	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Explorer\\Browser Helper Objects/i
73	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\SharedTaskScheduler	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Explorer\\SharedTaskScheduler/i
74	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\ShellExecuteHooks	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Explorer\\ShellExecuteHooks/i

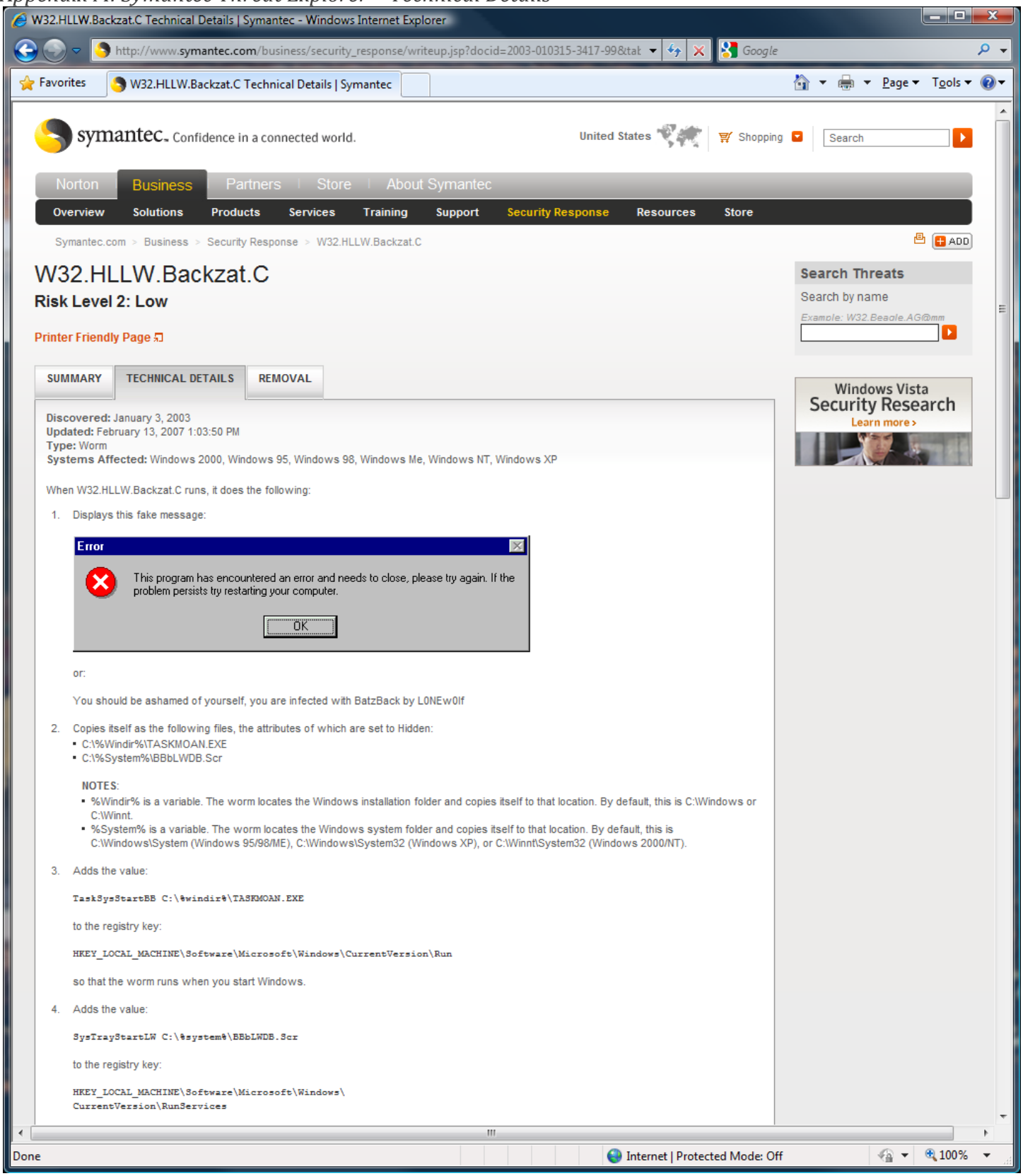
75	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ShellIconOverlayIdentifiers/i
76	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run/i
77	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Shell	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\Shell/i
78	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run(?!(Once|Services))/i
79	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce(?!Ex)/i
80	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnceEx/i
81	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunServices(?!Once)/i
82	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunServicesOnce/i
83	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Shell Extensions\\Approved/i
84	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ShellServiceObjectDelayLoad/i
85	HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logon	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Policies\\Microsoft\\Windows\\System\\Scripts\\Logon/i
86	HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Shutdown	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Policies\\Microsoft\\Windows\\System\\Scripts\\Shutdown/i
87	HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup	/(HKEY_LOCAL_MACHINE|HKLM)\\SOFTWARE\\Policies\\Microsoft\\Windows\\System\\Scripts\\Startup/i
88	HKLM\SYSTEM\CurrentControlSet\Control\BootVerificationProgram\ImagePath	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\BootVerificationProgram\\ImagePath/i
89	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\Authentication Packages/i
90	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\Notification Packages/i
91	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\Security Packages/i
92	HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\NetworkProvider\\\Order/i

93	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Print\\Monitors/i
94	HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\SecurityProviders\\SecurityProviders/i
95	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\BootExecute/i
96	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Execute	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\Execute/i
97	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDlls	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\KnownDlls/i
98	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\S0InitialCommand	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\S0InitialCommand/i
99	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SetupExecute	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\SetupExecute/i
100	HKLM\SYSTEM\CurrentControlSet\Services	/(HKEY_LOCAL_MACHINE|HKLM)\\System\\CurrentControlSet\\Services(?!\\(Alerter|ALG|AppMgmt|wuauserv|BITS|ClipSrv|EventSystem|COMSysApp|Browser|CryptSvc|DcomLaunch|Dhcp|TrkWks|MSDTC|Dnscache|ERSvc|Eventlog|EapHost|FastUserSwitchingCompatibility|Fax|MSFtpsvc|hkmsvc|helpsvc|HTTPFilter|HidServ|IISADMIN|ImapiService|cisvc|PolicyAgent|6to4|dmserver|dmadmin|ehRecvr|ehSched|MSMQ|MSMQTriggers|Messenger|MHN|SwPrv|Netlogon|mnmsrvc|napagent|Netman|NetDDE|NetDDEdsdm|Nla|xmlprov|NtLmSsp|PNRPSvc|p2psvc|p2pgasvc|p2pimsvc|SysmonLog|PlugPlay|WmdmPmSN|Spooler|ProtectedStorage|RSVP|RasAuto|RasMan|RDSessMgr|RpcSs|RpcLocator|RemoteRegistry|NtmsSvc|Iprip|RemoteAccess|seclogon|SamSs|wscsvc|lanmanserver|ShellHWDetection|SMTPSVC|SimpTcp|SCardSvr|SNMP|SNMPTRAP|SSDPSRV|SENS|srservice|Schedule|LmHosts|LPDSVC|TapiSrv|TlntSvr|TermService|Themes|UPS|upnphost|VSS|WebClient|AudioSrv|Shared?Access|stisvc|MSIServer|winmgmt|Wmi|W32Time|Dot3svc|WZCSVC|WmiApSrv|lanmanworkstation|w3svc|WinSock2|Tcpip))/i
101	HKLM\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries	/(HKEY_LOCAL_MACHINE|HKLM)\\SYSTEM\\CurrentControlSet\\Services\\WinSock2\\Parameters\\NameSpace_Catalog5\\Catalog_Entries/i

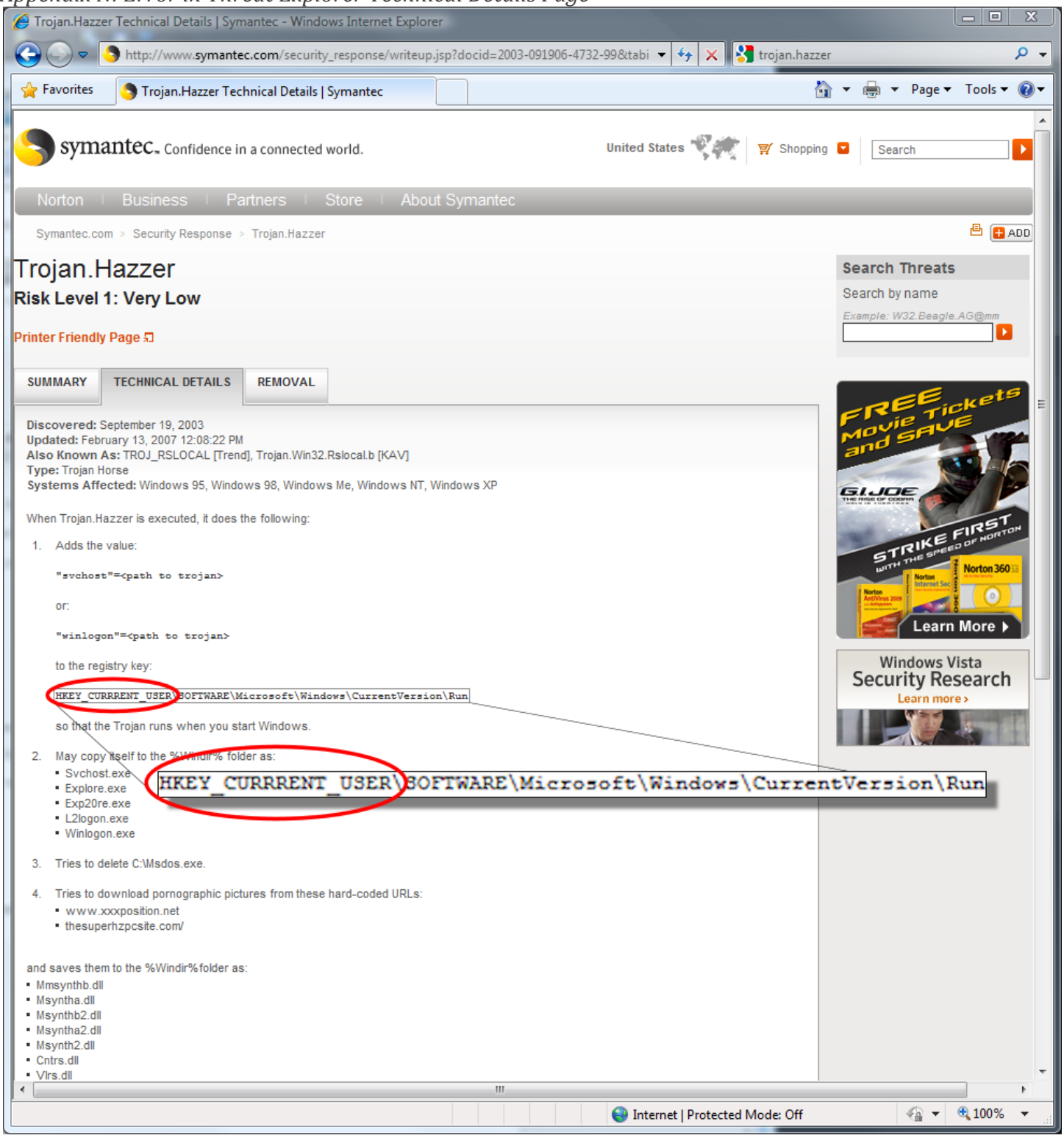
Appendix L: Symantec Threat Explorer – Browse A-Z



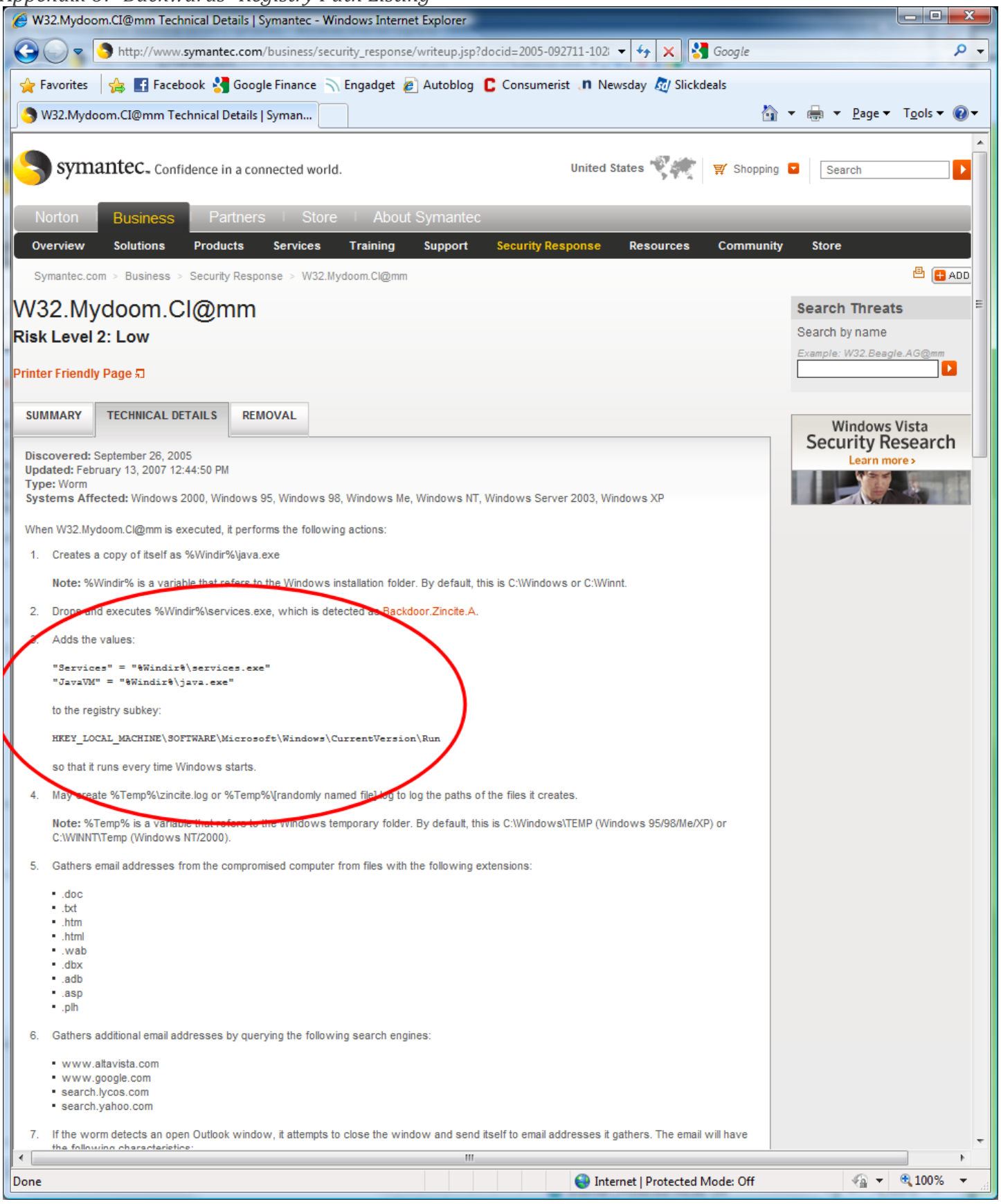
Appendix M: Symantec Threat Explorer – Technical Details



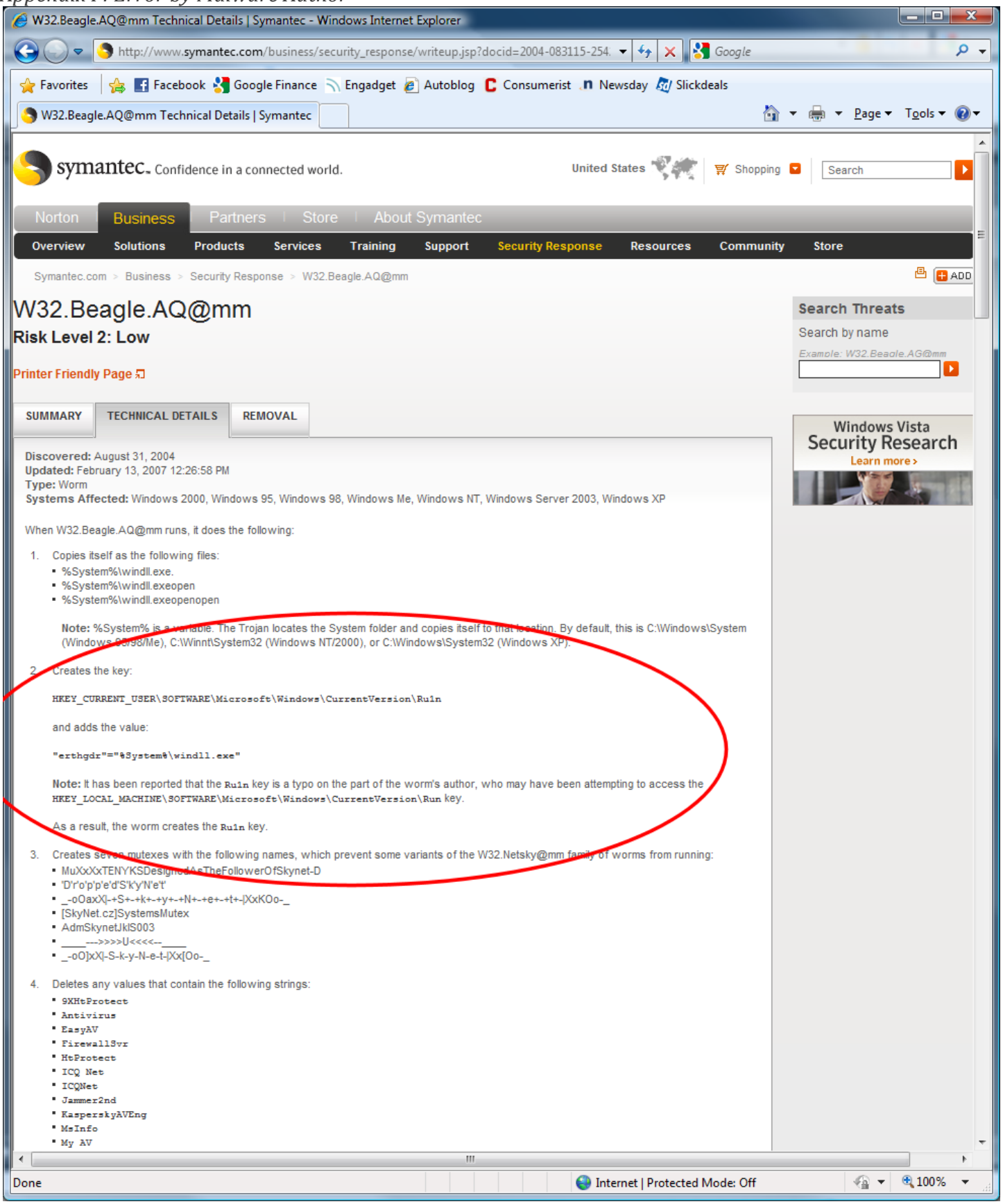
Appendix N: Error in Threat Explorer Technical Details Page



Appendix O: "Backwards" Registry Path Listing



Appendix P: Error by Malware Author



Appendix Q: Output of errorcheck.php

```
==========================================
          SUMMARY OF ERRORS FOUND
==========================================
(55 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n
(45 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun
(44 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n
(18 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc
(13 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\erthgdr
(12 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\My AV
(12 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\ICQNet
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\SkynetsRevenge
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\NetDy
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\service
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\SysMonXP
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Tiny AV
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\HtProtect
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\9XHtProtect
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\MsInfo
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\ICQ Net
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\FirewallSvr
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\KasperskyAVEng
(11 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Jammer2nd
(10 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Special Firewall Service
(10 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\My AV
(10 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Norton Antivirus AV
(10 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Zone Labs Client Ex
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\HtProtect
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\ICQ Net
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\FirewallSvr
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\EasyAV
(9 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objecta
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\ICQNet
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\9XHtProtect
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Tiny AV
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\service
(9 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Antivirus
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\SysMonXP
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\NetDy
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\KasperskyAVEng
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\MsInfo
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Jammer2nd
(9 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\PandaAVEngine
(8 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Special Firewall Service
(8 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Antivirus
(8 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Norton Antivirus AV
(8 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\PandaAVEngine
(8 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Zone Labs Client Ex
(7 found) %System%\autorun.ini
(6 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n
(6 found) HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run
(6 found) Wini.ini
(6 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip
(6 found) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\(Default)
(6 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\EasyAV
(5 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\erthegdr
(5 found) wint.ini
```

```
(5 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Ru1n
(4 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ERSvc
(3 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\srservice
(3 found) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\(default)
(3 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\ICQ Net
(3 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\erthgdr
(3 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\srservice\Start
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\[default]
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Antivirus
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\HtProtect
(2 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\NoRun
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\erthgdr
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsfot\Windows NT\CurrentVersion\Winlogon\Userinit
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\EasyAV
(2 found) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\wscsvc
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\9XHtProtect
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\erthegdr
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\FirewallSvr
(2 found) HKEY_CURRENT_USER\Software\Microsoft\WindowsCurrentVersion\Run
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoRun
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsfot\Windows NT\CurrentVersion\Winlogon\Shell
(2 found) sysdeb.ini
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Norton Antivirus AV
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\NetDy
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\My AV
(2 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ ShellServiceObjectDelayLoad
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\PandaAVEngine
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Special Firewall Service
(2 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Zone Labs Client Ex
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Tiny AV
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\SysMonXP
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\service
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\MsInfo
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Jammer2nd
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\ICQNet
(2 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\KasperskyAVEng
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\ccSvcHst.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\kvol.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Run\[random worm filename]
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\zwpInit_Dlls
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\avp.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVerion\RunOnce
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\kernelwind32.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\kabaload.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Shell
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\avp.com\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\iparmo.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsCurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\isPwdSvc.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curre\ntVersion\Explorer\Browser Helper Objects{27150F81-0877-42E9-AF13-
55E5A3439A26}
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVerion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\guangd.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\cross.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\shcfg32.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\nod32kui.exe\Debugger
```

```
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\nod32krn.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\kvupload.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\regedit.Exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\regedit32.Exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\kvwsc.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\mmsk.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\loaddll.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\logogo.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\mcconsol.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\mmqczj.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\rfwProxy.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\rfwcfg.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\taskmgr.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\symlcsvc.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\zxsweep.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\pjpInit_Dlls
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ztpInit_Dlls
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\sos.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\servet.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\rfwsrv.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\runiep.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\safelive.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\scan32.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\kvolself.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winsock2\ParametersProtocol_Catalog9\Catalog_Entries\000000[Two random
digits]
(1 found) HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Run subkey
(1 found) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip
(1 found) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\UPS
(1 found) HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog\Catalog_Entries
(1 found) HKEY_LOCAL_MACHINE\Sofware\Microsoft\Windows\CurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ExplorerNoRun
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ruins
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\wrn
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurretVersion\Run\Systems Restart
(1 found) HKEY_LOCAL_MAHINE\Software\Microsoft\Windows\CurrentVersion\Run
(1 found) HKey_Local_Machine\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell
(1 found) Wkkin.ini
(1 found) twain.ini
(1 found) wins.ini
(1 found) winsl.ini
(1 found) Wins.ini
(1 found) Winq.ini
(1 found) Systems.ini
(1 found) Wina.ini
(1 found) Winl.ini
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrenVersion\Run
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Rn
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\erthgdr2
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\dwn
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objecta\{edbf1bc8-39ab-48eb-a0a9-
c75078eb7c8e}
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objecta\{7caf96a2-c556-460a-988e-
76fc7895d284}
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ ShellServiceObjectDelayLoad\[FILE NAME OF DLL WORM COMPONENT]
```

```
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objecta\{27150F81-0877-42E9-AF13-
55E5A3439A26}
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objecta\{5f4c3d09-b3b9-4f88-aa82-
31332fee1c08}
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\explorer\NoRun
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ruins
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Shell
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsCurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\RunServices
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell
(1 found) HKEY_LOCAL_MACHINE\Software\Microsoft\ActiveSetup\Installed Components
(1 found) HKEY_LOCAL_MACHINE\Software\Micorsoft\Windows\CurrentVersion\Run\Agent
(1 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RSVP
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\avgrssvc.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winsock2\ParametersProtocol_Catalog9\Catalog_Entries\000000[Two random
digits]\PackedCatalogItem
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ ShellServiceObjectDelayLoad\Web Event Logger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RfwMain.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsfot\Windows\CurrentVersion\RunServices
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsfot\Windows\CurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windo ws\CurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windo ws\CurrentVersion\Run\Task Manager
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\360rpt.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\360Safe.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command\[DEFAULT]
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\exefile\shell\open\command\(Default)
(1 found) HKEY_CURRRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load
(1 found) HKEY_CURRRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\winlogon
(1 found) HKEY_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows\CurrentVersion\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTRWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{78364D99-A640-4DDF-B91A-
67EFF8373045}
(1 found) HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows\CurrentVersion\Run\Distributed File System
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\360tray.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\AgentSvr.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\IceSword.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\HijackThis.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Iparmor.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KASMain.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KAV32.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KASTask.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\FileDsty.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\FTCleanerShell.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\AutoRun.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\AppSvc32.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\AvMonitor.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\CCenter.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Discovery.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Debugger
(1 found) HKEY_CURRRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchost
(1 found) HKEY_CURRRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
(1 found) HKEY_CURRENT USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
(1 found) HKEY\LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Svhost Loader
(1 found) HKEY_CURRENT_USERS\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
(1 found) HKEY_CURRENT_USERS\Software\Microsoft\Windows\CurrentVersion\Run\[RANDOM NAME]
(1 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Antivirus
(1 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Rn
(1 found) HKEY\LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Svhost Loader
```

```
(1 found) HKEY\LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
(1 found) %Windir%\winsl.ini
(1 found) %SystemDrive%\autorun.ini
(1 found) C:\Document and Settings\All Users\Start Menu\Programs\Startup\Empty.pif
(1 found) C:\Windows\Winl.ini
(1 found) HKEY\LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
(1 found) C:\Windows\Winq.inia
(1 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\Antivirus
(1 found) HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru1n\directs.exe
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\Antivirus
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n\erthgdr2
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\NoRun
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurretVersion\Run
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\explorer\NoRun
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\norun
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Norun
(1 found) HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run\
(1 found) HKEY_CURRENT_USER\SoftwareE\Microsoft\Windows\CurrentVersion\Run
(1 found) HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run\Explorer
(1 found) HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run\TaskMon
(1 found) HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ExplorerNoRun
(1 found) HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KAVDX.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KAVPFW.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\SmartUp.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\SREng.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\SysSafe.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\TNT.Exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\TrojanDetector.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\TrojDie.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\SDGames.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Rsaupd.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RavStub.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RavMonD.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RavTask.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RegClean.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RsAgent.exe\Debugger
(1 found) %System%\autorun.ico
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Trojanwall.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\TxoMoU.Exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Wsyscheck.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\WoptiClean.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\XP.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\adam.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\auto.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\appdllman.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UpLive.EXE\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UmxPol.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UIHost.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UFO.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UmxAgent.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UmxAttachment.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UmxFwHlp.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\UmxCfg.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\RavMon.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Rav.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KRepair.COM\Debugger
```

```
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KRegEx.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KVCenter.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KVMonXP.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KVSrvXP.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KVMonXP_1.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KPFWSvc.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KPFW32X.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KAVStart.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KAVSetup.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KISLnchr.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KMFilter.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KPFW32.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KMailMon.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KVStub.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KWatch.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\NAVSetup.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\MagicSet.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\PFW.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\PFWLiveUpdate.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\Ras.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\QHSET.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KvfwMcl.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KvXP.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KWatchX.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KWatch9x.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KaScrScn.SCR\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KsLoader.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KvReport.kxp\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\KvDetect.exe\Debugger
(1 found) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution\Options\autoruns.exe\Debugger
```