GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Monitoring Malware

Coover Chinoy

GSEC Practical Assignment
Version 1.4c - Option A
February, 2005

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

ABSTRACT

With the exponential growth rates and frequency of attacks on the rise, malware has become a paramount concern for electronic computing environments worldwide. These attacks have resulted in significant productivity and financial loss for both commercial and residential environments of all sizes.

Maintaining a secure, sustainable and efficient infrastructure is the one of the many goals of a Chief Information Officer (CIO) and is a primary goal of every Information Technology (IT) Director. While the CIO and the IT Director have dedicated team(s) to manage their corporate infrastructure, maintaining a home personal computer usually rests solely upon the knowledge of the home user.

Unfortunately, when corporate users go home and begin to use their home computers, they often neglect to realize that their computing activities must be more cautious because they are no longer protected by their corporations actively monitored and managed network infrastructures. The ability to propagate via uncheck public E-mail, susceptible web browser, non-patched systems and unprotected network shares all increase the success probability for malware infections which at times can be detrimental to the end user's computer and possibly to their corporation.

This paper will focus on answering the questions:

- What is malware?
- What are the impacts of malware?
- What are some built-in and free Windows based monitoring tools that can be used to potentially identify malicious activity?

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Introduction:

To begin, we should first understand what is malware.

Malware (**Mal**icious soft**ware**) is a general term that refers to software that was written with malicious intent and performs its actions without the user's permission[1]. The variety of malware examples can usually be placed into one of the following categories. As defined by Ed Skoudis in Malware – Fighting Malicious Code[2]:

- A ***virus*** is a self-replicating piece of code that attaches itself to other programs and usually requires human interaction to propagate.
- A ***worm*** is a self-replicating piece of code that spreads via networks and usually doesn't require human interaction to propagate.
- A ***trojan horse*** is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality.
- ***Spyware*** is the categorical name for any application that may track your online and/or offline PC activity and is capable of locally saving or transmitting those findings for third parties sometimes but usually more often without your knowledge or consent[3].

Malware Impacts:

To gain a better understanding of malware it is important to understand the impacts that it may cause for computer users working in companies and those using them in their homes. The impacts of malware vary in both variety and severity. For an individual, malware impacts may range from minor annoyances of windows opening unexpectedly and frequently and can extend to failures of individual computer systems. For companies, depending on their thoroughness of preparation and execution of a sound security policy and strategy, impacts can range from trivial occurrences to major network impacts to extreme catastrophic and long term concerns.

For companies large and small alike, negative media attention and financial loss seem to be the cause for the most severe business impacts. Though capable independently, both negative media attention and financial loss could directly lead to a sequence of catastrophic events which could bring into question a company's long term reputation of brand recognition, customer loyalty, profitability, stability and even its viability in their industry.

As stated in the 2004 CSI/FBI Computer Crime and Security Survey[CSI/FBI-4], "…total (dollar) losses for 2004 were $141,496,560, down from $201,767,340 in 2003.". However, the survey also indicated that, "… respondents are generally either unable or unwilling to estimate the dollar losses. In this year's survey, (only) 269 respondents out of a total of 494 provided dollar loss estimates." When reviewing why the losses seemed relatively low for a problem that appears to be growing exponentially worldwide, it was noted that, "… these 494 computer security respondents were from U.S. corporations, government agencies, financial, medical institutions and universities."

© SANS Institute 2005 Author retains full rights.

From a more global view, InformationWeek reported on the financial impacts from the major malware attacks in 2004:

> "None of the attacks this year top the dollar losses attributed to the LoveBug attack four years ago, according to Computer Economics. But the four largest attacks of the year have proven a wicked and costly combination. Damages worldwide attributed to MyDoom are estimated at $4.75 billion; Sasser, $3.5 billion; NetSky, $2.7 billion; and Bagle, $1.5 billion. Total combined losses are estimated at $12.45 billion."[5]

Losses like these can be significantly devastating for any company. Internal effects by financial losses could pave the way for decreases in internal corporate spending, internal fund re-allocations and agency and/or employment cutbacks just to name a few repercussions. Additionally, malware attacks can result in significant and unexpected costs due to time and effort spent on reactive and investigative action to eliminate the present threat as well as preventative actions to guard against future attacks.

From a company's perspective, concerns on when the attack occurred, how the malware breached defenses, what are the present risks to the infrastructure and what information may have been altered or even exposed outside the company must be assessed and resolved expeditiously. Early efforts by computer incident response teams and/or other active groups within security organizations continue to remain on 7x24 readiness to hopefully identify a potential threat and take the necessary course of action to contain it, eradicate it, and learn from it in order that the thread of future attacks may be proactively avoided. Information Technology (IT) organizations must also develop and communicate a well established security policy within their organization. Properly communicated guidelines can help reduce the possibility of such attacks.

Another serious impact of malware attacks could possibly be the inadvertent leakage of sensitive information. The possibility of sensitive data like personal financial data (e.g. social security numbers, patient medical records, etc…) being disclosed to outside entities could be major infringements of personal privacy against recent U.S. laws like HIPPA[6] and the Gramm Leach Bliley act[7]. Such instances could lead down the road to painstaking litigation and possibly additional financial penalties or worse. Again, negative media attention generated from such an event could be hazardous to a company and to any of its existing and future customer base. Severe skepticism by customers on the company's abilities to safeguard their data and its integrity can lead to horrific thoughts of who has their personal data. Amusing but very discerning television advertisements regarding identity theft make consumers aware of this increasing and costly threat.

© SANS Institute 2005 Author retains full rights.

Malware attacks can also result in a company's productivity loss. Individuals using computers that have been infected with malware may experience windows that open up unexpectedly (also known as popups), may observe excessive and unexpected use of computer resources (e.g. hard drive disk access, hard drive space, memory, network traffic, etc…) which often result in a degradation of overall computer performance. In extreme cases, malware like the SQL Slammer worm corrupted data on hard drives. All these effects of system degradation many times result in severe lockups and rebooting which reduce a user's productivity.

If let loose into an environment full of computers that are susceptible to a particular exploit, fast moving worms like SoBig.F and Code Red could monopolize network bandwidth sufficiently as they propagated themselves to nearby computers and in some cases have caused near "network meltdowns".

By becoming a victim of malware, your computer could become one of a large number of computer "zombies" which is able to be controlled by another individual to participate in a distributed denial of service (DDoS) attack upon an unsuspecting target. One such famous incident was the DDoS attack on Yahoo on 8 February 2000[8].

Unfortunately, there is a wide variety of malware that always seems to be traversing about on the internet from computer to computer. One day a computer may be malware free, and the very next it may be infected with any one of a number of existing or possibly new malware variants. This ferocity of present day malware continues to keep many individuals busy with both reactive and proactive tasks.

On a daily basis, corporate employees concentrate on performing their business related job functions. They use their computers regularly to send emails, transfer files, and utilize the company's intranet and Public Internet to review information.

Employees working in small companies usually have some individual(s) responsible for handling their computer networking and security related business needs for their companies on a part time basis. In the case of medium to large size companies, large operations teams or even entire organizations are dedicated to actively monitoring and managing their enterprise. These organizations establish, educate and enforce corporate (security) policies to their workforce. Within the confines of their corporate intranets, corporate employees are often protected from the ever present risks of malware infection that exist on the Public Internet by their corporate firewalls, virus scanning E-mail servers and intrusion detection systems (IDS). However, the same sense of security is retained as this corporate user connects to the Internet when they use their personal computers at home. While a "defense in depth" methodology protects corporate users when in the office, a more cautious approach must be taken when accessing the Internet from a home network.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

High speed access to the Internet from residential locations has progressed through a variety of technologies over the years. A plethora of transport services offering a wide spectrum of upload and download speeds are available for homes from ISPs. Such services include: dialup, Integrated Services Digital Network (ISDN), satellite, Digital Subscriber Loop (DSL), cable modem and even T-1's. High speed access is available to the majority of home owners in populated residential areas. Though outlying areas may still only have dialup offerings, users in those areas look to alternatives like satellite and other means for higher speed access. Why do you ask?

As per an October 1996 study by Juniper Communications, more people have begun performing financial transactions from their home computers.

> In October 1996, Jupiter Communications and Find/SVP released their study, 'The American Home Financial Services Survey.' The survey showed that 55 percent of all PC-owning households are doing some financial management on their computers, representing 9,200,000 households.[Lee-9]

With high speed capabilities, home users are now able to download large computer games, applications, music, streaming video and a plethora of other items and information ubiquitously available on the Internet. Unfortunately, just as the high speeds allow more rapid access to the Internet, the ability for malware to make its way to and possibly into home computers also increases from not only one, but possibly many potential sources and vectors.

Given this, people should be much more cautious about protecting their home computers and home networks from malware attacks.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Monitoring Tools:

What Windows based monitoring tools can be used to potentially identify malicious activity?

The age old adage that, "An ounce of prevention is worth a pound of cure" is very applicable when used in a discussion related of personal computing. It is especially vital with our present day environment where malware still appears to run freely. Before we being to proactively (rather than reactively) monitor for malware on a home computer system, we must first perform some preliminary tasks.

The first and most important task is to establish a regular and well maintained backup strategy to recover from any unplanned computer failure. As more and more individuals continue to utilize their computers for personal, financial and business needs, backups become more critical for the restoration of data in the unfortunate event of any data compromise, data corruption or loss. This is especially true in the incident of an unexpected malware infestation. Additionally, it is recommended to keep your original operating systems and application licenses and installation CDs/DVDs together with your backups in a safe place in the disastrous event that a complete software re-installation is required on the computer. Given the reduction in availability of free time in our daily lives, and with the alarming malware growth statistic, do you think your computer would be a good target for hackers? The last concern for backups is to ensure that the data being backed up is virus-free. To protect against viruses, we continue onto our second task.

The second task is to ensure that an active anti-virus application is installed and has been updated with latest virus signatures. These applications will aide users in the detection of known viruses and aid in the prevention of infected files from being propagated via email, internet downloads or system transfers via the network or removable media.

The third task involves the creation of a system baseline. A system baseline will help to provide a clearer understanding of exactly what programs, process, services and ports are functioning under normal computer operations. A baseline is a know frame of reference to which you would compare each computer resource that you want to monitor. It is best to create a baseline, immediately after a computer has been initially loaded using the original installation media and all mandatory and recommended patches and updates have been applied. The tools we review below can assist you with the creation of a baseline just as they can assist you in the detection of anomalies from that baseline caused by entities like malware.

Given that backups are safely stored, your anti-virus software is operational and a system baseline has been created and understood, we can now look at using some of the following tools to investigate and examine changes and anomalies to our computer system.

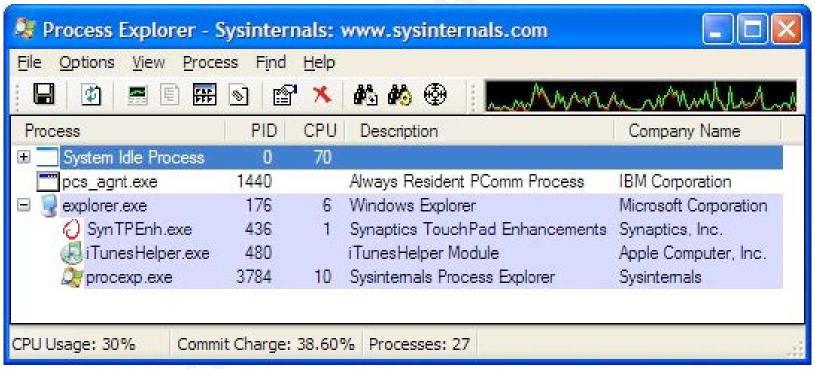
© SANS Institute 2005 Author retains full rights.

There are many tools available from to perform monitoring of each system resource defined below. For the purposes of this paper, I selected tools that will execute on Microsoft Windows NT4, 2000, XP and 2003 operating systems. I also elected to minimize costs by maximizing the use of the built-in capabilities and easily attainable free tools that could easily be downloaded.

1. Program and Process Monitors:
   - Tools: Windows Task Manager[10], Process Explorer[11]

   Microsoft's Windows Task Manager and Process Explorer from Winternals Software are both good GUI based tools that provide details about active programs and processes that are actively operating on a computer. Using either tool will allow your to review processes and services running by the SYSTEM as well as those run under the user's context. While the understanding of processes can be difficult for the novice user, I believe process explorer provides a better organizational representation of the information.

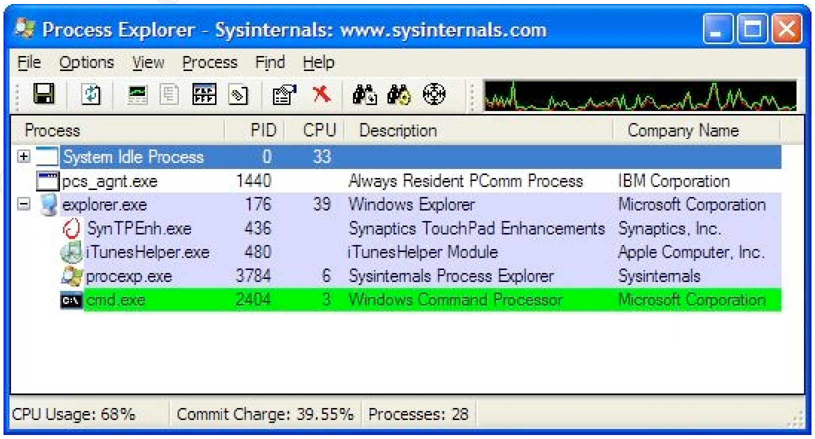
   In Figure #1 below, a baseline was created identifying all of the active processes. Then later in Figure #2, a new process was created, cmd.exe, which has been highlighted in green as it is a newly introduced process.



Process	PID	CPU	Description	Company Name
System Idle Process	0	70		
pcs_agnt.exe	1440		Always Resident PComm Process	IBM Corporation
explorer.exe	176	6	Windows Explorer	Microsoft Corporation
SynTPEnh.exe	436	1	Synaptics TouchPad Enhancements	Synaptics, Inc.
iTunesHelper.exe	480		iTunesHelper Module	Apple Computer, Inc.
procexp.exe	3784	10	Sysinternals Process Explorer	Sysinternals

CPU Usage: 30% | Commit Charge: 38.60% | Processes: 27

Figure #1: Created baseline of active processes



Process	PID	CPU	Description	Company Name
System Idle Process	0	33		
pcs_agnt.exe	1440		Always Resident PComm Process	IBM Corporation
explorer.exe	176	39	Windows Explorer	Microsoft Corporation
SynTPEnh.exe	436		Synaptics TouchPad Enhancements	Synaptics, Inc.
iTunesHelper.exe	480		iTunesHelper Module	Apple Computer, Inc.
procexp.exe	3784	6	Sysinternals Process Explorer	Sysinternals
cmd.exe	2404	3	Windows Command Processor	Microsoft Corporation

CPU Usage: 68% | Commit Charge: 39.55% | Processes: 28

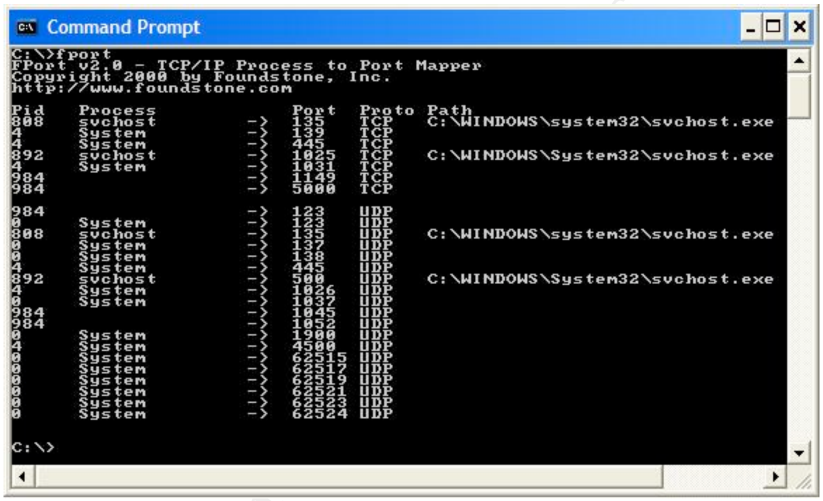
Figure #2: The new process cmd.exe was started

© SANS Institute 2005 Author retains full rights.

If you find a program or service that you are unable to identify visually, you can begin by clicking on it and review the originating company or the *.DLLs that are associated with it and may help to determine its operating function. If you are still unable, search the web for the item. Remember, the "web knows all". If you learn the process is malware related, follow the corrective actions for its eradication from your system from a reliable source.

2. Port Monitors:
   - Tools: FPort[12], nmap[13], TCPMon[14]

Port monitors are tools that can indicate which TCP and UDP ports are actively listening "i.e. open" for communications and also associate each port with the application that is actively listening on that port.

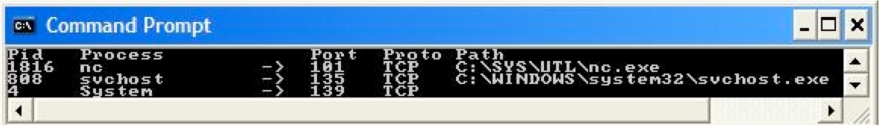


```
C:\>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto Path
808   svchost      ->  135   TCP   C:\WINDOWS\system32\svchost.exe
4     System       ->  139   TCP
4     System       ->  445   TCP
892   svchost      ->  1025  TCP   C:\WINDOWS\System32\svchost.exe
4     System       ->  1031  TCP
984                ->  1149  TCP
984                ->  5000  TCP

984                ->  123   UDP
0     System       ->  123   UDP
808   svchost      ->  135   UDP   C:\WINDOWS\system32\svchost.exe
0     System       ->  137   UDP
0     System       ->  138   UDP
4     System       ->  445   UDP
892   svchost      ->  500   UDP   C:\WINDOWS\System32\svchost.exe
4     System       ->  1026  UDP
0     System       ->  1037  UDP
984                ->  1045  UDP
984                ->  1052  UDP
0     System       ->  1900  UDP
4     System       ->  4500  UDP
0     System       ->  62515 UDP
0     System       ->  62517 UDP
0     System       ->  62519 UDP
0     System       ->  62521 UDP
0     System       ->  62523 UDP
0     System       ->  62524 UDP

C:\>
```

Figure #3: Fport displaying open TCP & UDP ports and the application utilizing each port.

To illustrate the introduction of a new port, I used the application netcat[15] to open up a listener on TCP port 101. To do so, I executed the command, "nc –l –p 101 –t –e cmd.exe". {Please be aware, this command is dangerous!!}

In Figure #4, I then confirmed that a new TCP port 101 was actively listening.



```
Pid   Process          Port  Proto Path
1816  nc           ->  101   TCP   C:\SYS\UTL\nc.exe
808   svchost      ->  135   TCP   C:\WINDOWS\system32\svchost.exe
4     System       ->  139   TCP
```

Figure #4 NC application was listening on TCP port 101.

While fport and nmap are superb at providing information about open ports at a point in time, TCPMon provides continuous open port information using a GUI front end. If you identify an open TCP or UDP port on your computer, try to identify the application associate with it. Compare your findings to the SANS' list of well known ports[16] or ONCTec LLC's list of ports[17] to see if it could be

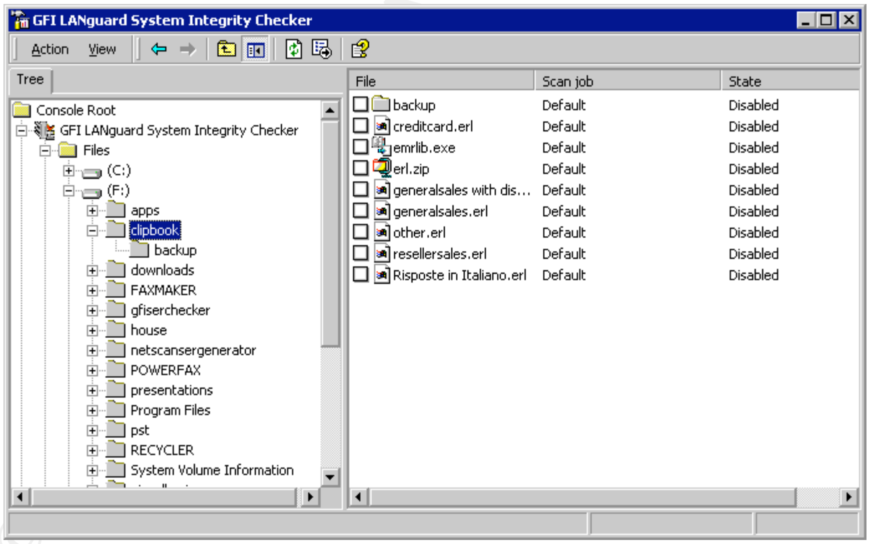
© SANS Institute 2005 Author retains full rights.

used by malware. If you believe that it is, attempt to identify the specimen and seek information on it's eradication. If you are unable to determine the application and cannot verify if it is truly for malware, attempt to block the port by updating your personal firewall policy to block its access. If you find out you were wrong, you can go back and readjust the policy.

3. File (Integrity) Monitors:
   - Tools: GFI LANguard System Integrity Monitor[18]

   File integrity checkers inherently work as detailed above. Upon installation these applications calculate (usually MD5) hash values on all files and/or folders identified to be monitored by the integrity checker. Upon subsequent integrity checks, if a file has been altered or deleted, an alert is generated which can be reviewed by the person performing the monitoring. In this version, an email notification is sent to the individual specified during installation.

   It is important to identify critical file and folder that will be monitored by the integrity checker. Detecting changes in operating system, applications and/or key end user data files and folders can be valuable information when searching for malware. Malware files lurk in very common and sometimes even unsuspecting locations. As an example, one would want to pay special attention to files that may have been placed in the hidden *C:\RECYCLER* folder.



File	Scan job	State
□ backup	Default	Disabled
□ creditcard.erl	Default	Disabled
□ emrlib.exe	Default	Disabled
□ erl.zip	Default	Disabled
□ generalsales with dis…	Default	Disabled
□ generalsales.erl	Default	Disabled
□ other.erl	Default	Disabled
□ resellersales.erl	Default	Disabled
□ Risposte in Italiano.erl	Default	Disabled

Figure #4: Identifying files to be monitored by the integrity checker

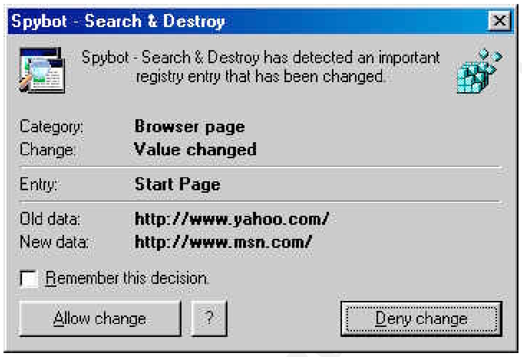
In the event that you find your data has been compromised, you may be able to remove the malware without damage to the file(s). However, if it cannot be removed, you will have to restore the file(s) from your backup. If there is an application file that has been compromised, it may require that the application be reinstalled. If you are unable to eradicate the known or unknown malware specimen, then you may have to result to reinstalling your entire system. Complete system restoration efforts really support the benefit for taking a

© SANS Institute 2005 Author retains full rights.

proactive approach with backups, and prevention with anti-virus and personal firewall applications.

4. Registry Monitor:
   - Tools: TeaTimer (Spybotd)[19], Regmon[20]

These tools monitor any changes that are made to the registry. Since the registry maintains a large variety of system configurations, nearly all changes are updated within the registry. Malware specimens regularly attempt to add their components into the Windows run section in an effort to be executed upon every system start. Tools like these will be able to notify the user upon any such change. Web browsers, along with many other programs, update the registry as they are used. For example, when I manually changed my default home page in my web browser, the following warning (see Figure #5) was generated by TeaTimer.



Spybot - Search & Destroy has detected an important registry entry that has been changed.

Category: **Browser page**
Change: **Value changed**

Entry: **Start Page**

Old data: **http://www.yahoo.com/**
New data: **http://www.msn.com/**

□ Remember this decision.

Figure 5: Intercepted request for a registry change for the web browser

Take special note of what actions you are performing when you work on your computer. If such a warning appears, determine if it related to what you are doing at that time. One would expect that if you are installing an application, then registry changes may be associated with the installation and therefore not a surprise. However, unexpected changes occurring when opening emails or document that you have opened before might be causes for curiosity and possibly concern.

It is important to note that novices should be very careful when performing any manipulation within the Windows registry. A simple modification may generate errors during the computer's boot cycle or possibly worse events. For those who would like to learn more about the Windows registry and how to manipulate it, review Microsoft knowledgebase article 256986[21], or select one of many books available on the subject from your local book retailer.

© SANS Institute 2005 Author retains full rights.

5. Memory Monitor:
   - Tool: Windows Task manager

   Though the Windows task manager is capable of providing information on active processes and programs executing on the system, it is also capable of providing the memory usage associated with each active process. This capability can aid in identifying malware (also called memory hogs) that attempt to incapacitate systems by monopolizing and/or depleting all available system memory. On the performance tab inside of the task monitor, a near real-time graphical scrolling banner provides details for both page faults and CPU usage for a short duration. For those who require it,

   On a side note, these monitors are also valuable in identifying when available system memory is reaching it peak. They can be very useful for individuals who must manipulate large amounts of data as well as programmers who must ensure that the applications they are developing make efficient use of available system memory.

6. Hard Disk Activity Monitor:
   - Tool: Hard Disk Indicator [22]

   Similar to how one would monitor for unexpected changes to the registry and other system files, unexpected and frequent hard disk accesses could be another indicator of malware activity. Small utility tools like the hard disk activity monitor provide a convenient visual appearance of a "LED" which lights up during hard disk activity.

   Be careful not to allow paranoia to get the better of you every time your hard drive is accessed. As malware can be stealthy, there are many other processes that execute in the background of an operating system. Some such background tasks may include scheduled anti-virus scans, automated updates or even backups.

   If you find that there is infrequent or possibly even regular hard drive activity and you are unsure why, try opening up the task manager to the processes tab and see if you can identify the process that is presently utilizing the CPU and or memory. If it appears to be an application that you are presently running or a system file that you are familiar with, then it is probably a false alarm. However, if it is something that you are not familiar with, search the web to see if you can learn the proper function for that process.

© SANS Institute 2005 Author retains full rights.

7. Network (Protocol) Monitor:
    - Tool: Ethereal[23]

    By far one of the most popular and readily used network protocol analyzers is ethereal. This multi-platform tool is used by novices and experts alike to capture network data and is capable of performing deep packet inspection and analysis on the information captured.

    For the detection of malware, ethereal can be utilized to capture all data being received and sent out of a network interface for real-time analysis or post analysis by reading the information from a captured trace. Using ethereal to determine if malware is lurking in the background of computer system may take some time depending on the amount of traffic that is presently traversing across the network interface. When performing analysis of network traffic, it is a best practice is to capture all data rather than filtering the data that you are looking to analyze. This will allow the analyst the ability to review all of the expected and unexpected (possibly malware) data. Once the entire capture has been saved, analysis can begin and the appropriate filters can be applied to focus on the specific traffic that was intended to be analyzed.

    With it's abundance of capabilities, the ethereal website provides and extensive and well published user guide to help new users master this tool. By learning to apply filters, one can filter out all known traffic and begin to analyze the remainder to determine what information is being sent or received. Deep packet inspection of such data should yield definitive results on what exactly is traversing the network.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Conclusion:

As these malware threats are sure to continue to become more numerous, complex and even dangerous with each passing day, management, system administrators and even individuals of home computers must never underestimate the threats today or in the foreseeable future. Established corporate security policies should extend to the employees' home computers if they are allowed to use them to connect back to their corporate networks using VPN services.

As people use their computers more for financial and other personal needs, it is imperative that users of home personal computers must be more aware and cautious to safeguard themselves as best they can from malware. The possibility that at sometime one of these entities in the wild may make their way into a corporate and home networking environment is almost a certainty.

In order to prevent a hacker from "owning your computer" and turning it into one of many "zombies", my recommendation is to use the tools discussed above to actively monitor for signs of malware. This is in addition to the use of antivirus, personal firewall and spyware applications and maintaining regular updates for all applications will allow you to proactively fight in the war against malware and should reduce the overall risk of infection.

As indicated in Andrew Lee's article, "The biggest worms in the world"[24], the prediction for the future security practices, policy and defense in depth strategies for computing will continue to include an active antivirus scanner relying on signature based updates, but will also require, "require more robust detection and only products offering strong heuristic detection – to catch new variants without the need for updates…"

> Predicting the future
> One thing that has been made obvious by the proliferation of these and other worms, and the speed with which they spread and infect machines, is that the traditional anti-virus scanner, based only on signature updates, will eventually become extinct. The future requires more robust detection and only products offering strong heuristic detection - to catch new variants without the need for updates - in combination with signature based scanning will be truly effective.

Unfortunately, the thirst of human curiosity and the lax safe computing habits are contributors to why malware is so successful in propagating. History continues to show us that humans will click on anything!!!

Since much information contained on home computers is vital and confidential, it is imperative that a well constructed data backup plan be regularly maintained. Backups play a key role in disaster recovery plans because no one ever knows where or when a malware attack might strike next. As an example, read the February 2005 article

© SANS Institute 2005 Author retains full rights.

"Spywary"[25] where the publisher of Information Security Magazine, Andrew Briney, wrote about his recent eye-opening experience with spyware.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

REFERENCES

[1] SANS Institute. Track 1 – SANS Security Essentials, Volume 1.4, Version 2.2. SANS Press. Jan. 2004.

[2] Skoudis, Ed, and Lenny Zeltzer. Malware: Fighting Malicious Code. Upper Saddle River: Prentice Hall Professional Technical Reference. Nov. 2003.

[3] Webroot Software Inc. Feb. 2004. http://www.webroot.com/spywareinformation/spywaredefined/

[4] Richardson, Robert. "CSI/FBI 2004 Computer Crime and Security Survey". Ninth Edition, Computer Security Institute, Page 10.

[5] Klein, Paula. "Losses From Viruses Reach 5-Year High Swell". Information Week. 25 Oct. 2004. http://informationweek.com/story/showArticle.jhtml?articleID=51000347

[6] United States Department of Health and Human Services, The Health Insurance Portability and Accountability Act of 1996 (HIPPA). 21 Aug. 1996. http://aspe.hhs.gov/admnsimp/pl104191.htm

[7] Gram-Leach-Bliley Act (GLB) a.k.a Financial Modernization Act of 1999. 12 Nov. 1999. http://www.privacylaw.net/GLB.htm

[8] Richtel, Matt. The New York Times. 8 Feb 2000. http://www.nytimes.com/library/tech/00/02/biztech/articles/08yahoo.html

[9] Jupiter Research. 21 Oct. 1996. http://www.jup.com/jupiter/release/oct96/oct21.shtml

[10] Windows Task Manager. Microsoft Corporation. http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prmb_tol_gwii.asp

[11] Russinovich, Mark. Process Explorer Version 8.6.1. Sysinternals Inc. 2004. http://www.sysinternals.com/ntw2k/freeware/procexp.shtml

[12] Pond, Weld. Fport Version 1.1nt. 2 Feb. 1998. http://www.foundstone.com/resources/proddesc/fport.htm

[13] Fyodor. http://www.insecure.org/nmap/nmap_download.html

[14] Russinovich, Mark. TCPView . Sysinternals Inc. 9 Aug. 2004. http://www.sysinternals.com/ntw2k/source/tcpview.shtml

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

[15] Pond, Weld. Netcat Version 1.1nt. 2 Feb. 1998.
http://netcat.sourceforge.net

[16] von Braun, Joakim. SANS™ Institute. 9 Feb. 2001.
http://www.sans.org/resources/idfaq/oddports.php

[17] ONCTec LLC. http://www.onctek.com/library/trojans.html

[18] GFI LANguard System Integrity Monitor version 3.0. GFI Software Ltd. 18 Jul. 2003. http://www.gfi.com/lansim/lansimfeatures.htm

[19] Kolla, Patrick, M. Spybotd - Search & Destroy version 1.3. http://www.safer-networking.org/en/download/index.html

[20] Russinovich, Mark. Registry Monitor Version 6.12. Winternals Software. 14 Aug. 2004. http://www.sysinternals.com/ntw2k/source/regmon.shtml

[21] " Description of the Microsoft Windows registry". Microsoft Corporation. 1 Feb. 2005. http://support.microsoft.com/kb/256986

[22] Dalakostas, Dimitris "Lonewolf". Hard Disk Indicator v 1.3. 21 Nov. 2002. http://www.lonewolf.gr/software/default.asp.

[23] Comb, Gerald. Ethereal version 0.10.9. http://www.ethereal.com/download.html

[24] Lee, Andrew, SC Magazine, "The biggest worms in the world" URL: <http://www.scmagazine.com/features/index.cfm?fuseaction=featureDetails&newsUID=0d8aa45d-91d5-47c9-b276-f3467480c342>

[25] Briney, Andrew. "Spywary." Information Security Magazine. Feb. 2005: Page 72.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005

Author retains full rights.