Removing Pests from Windows (Part 1)

Date Launched: Sep 22, 2004
Last Updated: Sep 22, 2004
Section: Articles :: Misc Network Security
Author: Ricky M. Magalhaes

In this two part article I will discuss pests and potential issues associated with pests that may be encountered within windows. IT security professionals are faced with these resource and information divulging threats daily and because at his point there is not mature technology to deal with the problem officially it is challenging to remove these pests form the computer or server manually. These pests are like parasites of the digital world. These parasites feed off the electronic resources of the host machine, eventually draining the machine to standstill point.

Caution: If you are going to try some of the changes suggested in the article it is recommended you make backups of your system and the registry before attempting the changes. The backups need to be tested for integrity to ensure that you can restore the data without any problems. Please note that the changes suggested work for some systems and need to be tested on your unique configuration.

Start with Policy

It is essential that policy add a number of layers to be employed in order to ensure an organization's security is adequate. These layers, based on the defense by monitoring concept, ensure that if any of the layers are compromised, the additional layers of security employed are sufficient to stop Malware/Spyware stealing resources and information. It is paramount that the top-down security model is followed to ensure that key computers are identified and assessed so on merit. This also helps the IT professional to identify computers and users that may present organizational risk. The importance of securing those assets and resources becomes important because it increases efficiency. If the connection trust model is used this methodology adds numerous layers of defense.

Protect the entry points, prevention is better that cure.

- Do not use servers for browsing or downloading. IT professionals should not allow Internet Browsing or downloading form any server computer.
- Ensure that disc drives (Floppy discs, flash discs, USB drive Etc.) are not promiscuous and do not travel and connect to other computers that could transfer infections to the drives.
- Pirate software (Warez Etc.) Pirate software can be infected as it is not obtained from a trusted source. It may also contain Trojans and other software

like agents that could potentially turn the computer into an infected zombie machine.

- Peer to peer (P2P) connections. (File sharing applications and file sharing networks) This software empowers the user to download software and other files from unknown sources. There is nothing stopping a malicious user from taking a popular piece of software and editing it so that it scripts and installs an agent onto the computer that downloads a keystroke log up to a server on the internet.
- Messaging software (the new unnoticed threat, messaging software can transfer files) some software that is used for instant messaging can also transfer files, these files can be uploaded and because the messenger users are trusted the file transfer is often accepted. The downloaded files need to be scanned for viruses and Trojans.
- Networks (need I say more?) Networks are a bunch of computers that have been connected together by some sort of fabric. It is over this media that some viruses and pests travel over.
- Email attachments (One double click away from the next worm) Email attachments if left un-scanned can pose a threat.
- Internet browser (Click or don't click and it downloads) Internet browsers display files that are thousands of kilometers across the world, browsers have the ability of downloading the files and executing them. Millions of files are downloaded daily some of these are malicious.
- Ensure that you have a popup blocker installed or your internet explorer security levels at an adequate enough level that will block any code form being installed on your computer that could potentially be malicious.
- Ensure you have a personal firewall or that you are behind a corporate firewall at very minimum. Firewalls not only protect you from external threats but also help in mitigating the risk of your documents being sent outbound using non conventional software types.
- Personal firewalls also stop users that are on the LAN that may potentially cause data loss or that may threaten availability.

Viruses or Malware

Funding for development can sometimes be obtained from large advertising organizations if the advertising banners or other spying software code is incorporated into the application and bundled and distributed on the advertising organizations behalf. Incidentally in the license agreement (that many people do not read) it states that some information will be sent to and from the computer. Some people agree to spying in some cases when they click 'I agree'.

Viruses are applications that are designed to replicate from one machine to another. Some of them are written to irritate computer users and others are written with malicious intent. We have been fortunate in this day and age that the worms that have been released have caused little loss of data compared to what could potentially happen. As the world economies become interconnected organizations become dependant on the internet. The internet is the medium that viruses are using to spread however; more viruses are becoming independent of the media and fabric that they use to spread. Wireless and cellular networks are now being targeted as more and more devices become interconnected in this way. As technology develops so do the applications and malware. Malware are applications that sacrifice the performance of a system for their own use and the application uses the resources on the infected computer and this can potentially be to the detriment of the user's

the infected computer and this can potentially be to the detriment of the user's system causing problems with installed applications.

These applications are generally resident (continuously run in memory loaded and utilize processing power and other resources like bandwidth and RAM) these resources cost money and in effect these applications are expensive. Each application that loads up on the computer uses up some of the processor, if the applications have not been written correctly this may result in the computer hanging even causing processor or memory leaks. This type of behavior can cause the computer and some of the applications installed on the computer to slow down considerably. A good example of this is when Internet explorer takes long to load. This may be caused by spyware or applications that hook into internet explorer. I have yet to come across a productive commercial product that is used for productivity that has this effect on internet explorer. The more of these applications that load the slower the computer becomes as most of the applications are written so that they leverage off other applications and behaviors that occur on the computer. If the computer is not restarted often, after a while you may notice that the computer slows down and this may be caused by the software escalating the computer's status to super node. A super node distributes and has listings of software. There have even been cases where some viruses infect other viruses cause excessive amounts of disc I/O as the replication goes into a loop.

Browser power

IT professionals often miss this entry point as it seems least likely. However this area is reason to fret. With the use of ActiveX and Java there are few commands that can not be run on the computer by the browser. When these applications load they can potentially initiate commands that edit startup files so that drives are formatted or master boot records erased. Imagine the damage that can be caused just by visiting a URL, this old yet unpredictable method will give the antivirus companies a new-found threat that may prove challenging to control. The browser application can be written so that it is not downloaded to the computer but rather executes and exists in the virtual realm and is only executed when the browser is hijacked or redirected.

Like most pests the parasitic approach is more beneficial and it is not in the author's best interest to erase or destroy the machine as the spying organization can benefit more from the information gathered. The whole effort is made by the organization for one reason they want to capture your information or your habits. Some parasites in the animal world kill or impede the host. These parasites in the computer world are equivalent to Malware or Trojans. At first they seem to be beneficial but once they are entrenched cause destruction and threaten the performance of the machine.

For many years now, problems experienced within Windows have been blamed on the operating system or on the web browser. Even if a good antivirus package is installed it may still not block the threat of malware or spyware as the software is not intended for that use. In July 2004 over 900 viruses and malware applications were released. Point and click programming technology makes the coding of a virus or malware program simple and some websites even have sample code that a malicious user can download, modify, and adapt for their specific use.

Some applications have parts of code that spy on the user and even report mouse co-ordinates so that when an advert is presented through a pop-up it will display in the area that the mouse most frequents. Advancements in technology have enabled the "spy" companies to market goods from their selected suppliers after a search is performed on a preferred search engine. Some spies even mimic the coloration of the

search engine to make the display page presented by the spies appear similar to the search engine. These browser hijackers not only consume bandwidth but also consume system resources and in some ways frustrate users that are not aware of such threats.

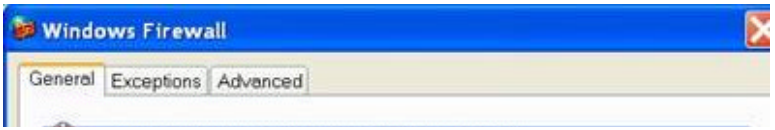
If the system works properly after it has been installed and then slows down after a while the offending module will be one that has been installed after the machine was properly installed and running effectively. Something has been added to the machine that is slowing the computer down and that something is most probably a badly written application that consumes bandwidth and resources.

Possible changes to a computer after installation

IT professionals can use Automated tools to ensure that the below tasks are performed on hundreds of machines.

- SUS/WUS to ensure that patches for applications and operating systems are current.
- Windows update to ensure driver updates and reinstallation.
- SUS/WUS to ensure that service packs are installed, these are clustered hot fixes and patches that get bundled into one large fix.
- Group policies to disable IE cookies, these files store user data and website configurations and preferences.
- Group policies to prevent applications that are installed as some can cause the machine to slowdown if they are poorly coded. Only standard approved software should be installed.
- Group policies to tie down activeX controls these controls can load up and start process on the computer without user intervention.

Above is an example of a popup blocker that is installed when service pack 2 for windows XP is installed. This popup blocker stops most malicious code from executing a secondary window that can trigger other malicious activities or annoying popups. IT professionals can educate their users to make use of this feature to reduce risk, explaining that popups could potentially launch an attack.



Above is an example of personal firewall software that can be installed. This particular piece of software is installed with Service Pack 2 for Windows XP and particularly useful in stopping non-standard applications from communicating with the Internet or other computers. One will have to add the application to the exception list in order to bypass the security. As you can see you are able to specify 'do not allow exceptions' and this in turn adds an extra layer of security. By using group policies that force personal firewalls to be turned on will increase security not only on the LAN but for each connected interface. If users are educated by IT professionals it may prove useful as the this technology helps both the user and the IT professional to manage intrusion risk.

Setting group policies so that the user can not write to the registry will mitigate the risk of having a user or malware/spyware from writing to the registry. Registry entries can be used to start up applications that may be malicious can be found either in the runonce or in the run key. To find other keys click edit and search for Run or Runonce.

In the second article of this series I will cover other places that intruders hide application startup links.

Summary

In this article I have covered some methods that intruders may use to gain access to your systems or that intruders may use to leverage your systems resources. IT professionals need to remain vigilant of these unseen threats. At the end of the day it's all about who controls the resources and the intruder will target your machine or machines because either you have information or physical hardware and bandwidth as a resource. All intruders have a motive and this motive is somewhat clouded by the methods used and overlooked as just a pest. By not acknowledging the threat the matter is often underrated and the appropriate amount of attention is not paid. In the next article Removing Pests from Windows (Part 2) I will cover some more techniques used by intruder and some other places that intruders use to hide their payloads.

About Ricky M. Magalhaes

Ricky M. Magalhaes is a security specialist that has worked as a consultant and IT technical specialist for the past 8 years. He has been primarily responsible for implementation and design of Security, network architecture, communications, network infrastructure and Security R&D for many South African organizations that he works with. He is a windows 9x product specialist and has been working with the windows product since version win 3.11. He has also written articles on security for www.windowsecurity.com ; www.ISAserver.org ; www.governmentsecurity.com and many other well known security and technology websites.