Preventive Measures For Malware In P2P Networks.

Prof.P.Pradeep Kumar,Naini Shekar Reddy,R.Sai Krishna,Ch.Kishor Kumar,M.Ramesh

Abstract

Peer-to-peer (P2P) networks continue to be popular means of trading content. However, very little protection is in place to make sure that the files exchanged in these networks are not malicious, making them an ideal medium for spreading malware.

The recent surge of peer-to-peer (P2P) networks consisting of thousands of hosts makes them a breeding ground for malware proliferation. Although some existing studies have shown that malware proliferation can pose significant threats to P2P networks, defending against such an attack is largely an open problem.

Malware is highly pervasive in P2P file-sharing systems and is difficult to detect automatically before actually downloading a file due to the insufficient and biased description of a file returned to a client as a query result. To alleviate this problem, we provide preventive measures for malware. And also we provide two basic approaches for preventing malware.

Keywords: P2P network, Malware, Reactive and Proactive Approach

1 Introduction

A P2P computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers."[2] Although this statement is mostly correct there are a few different types of P2P architectures which should be outlined:

1.1 Centralized Architecture - Requires a centralized server which hosts connect with in order to access a list of shared items. Each host provides a list of items they are willing to share. The server maintains this list of shareable items from all hosts. The actual download itself is performed between the hosts when an item is requested, not by the server.

1.2 Decentralized Architecture - This model does not require a centralized server. All hosts which connect to a decentralized P2P network send a request to all hosts which are currently logged on. The requesting host then receives a response from one or more hosts currently connected the network. Different sections of a file can be downloaded from multiple hosts.

1.3 Hybrid Architecture - This architecture offers a combination of the centralized and decentralized architecture.

Exactly **why are P2P networks a problem** when at the surface it seems like an easy way for users to transfer files? Well, besides the legal liabilities which organizations face due to their users downloading intellectual property such as music, software, literature, etc, for free, there is a ton of malicious code which traverses these networks. What better way for an attacker to launch the next big worm? Malicious code such as trojans and spyware can be wrapped in legitimate looking packages using all sorts of programs and downloaded via a P2P network. Unsuspecting users will launch these programs believing that they are legitimate, but not realizing that a trojan was installed. An attacker may now have remote access to an organization's internal network or potentially gathering confidential user information via a spyware program. In addition, the more modern P2P clients can consume an incredible amount of your network bandwidth. As an example, shareaza, can simultaneously connect to four P2P networks: Guntella, Guntella2, eDonkey and BitTorrent.

Most organizations are under the impression that P2P networks can simply be stopped by blocking the default port that is required for these networks to communicate. Think again. Most P2P networks can be configured to listen on TCP port 80 (HTTP). Almost every organization in the world permits the use of HTTP through their firewall. Doesn't it seem like we are fighting a losing battle? How can an organization effectively block this traffic?

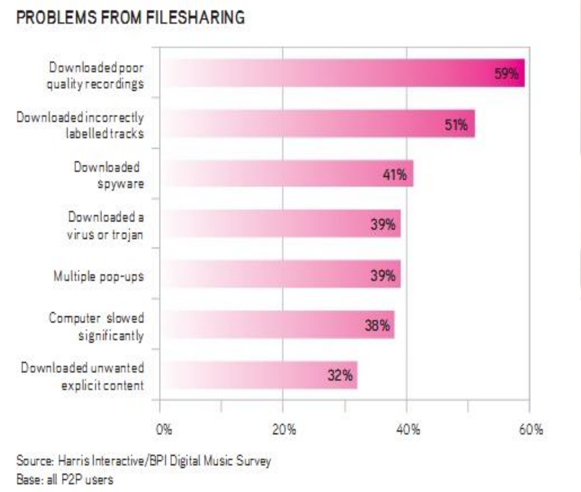
2 P2P Networks

2.1 Peer-to-peer file sharing

Peer-to-peer file sharing is a form of file sharing using peer-to-peer networking. P2P allows users to download files such as music, movies, and games using a file sharing software client that searches for other connected computers (called ‘peers’). Similarly, other computers on the network are able to search for files on your computer. This differs from traditional file downloading that searchers servers for the requested file.

The widespread adoption and facilitation of peer-to-peer file sharing was helped by several factors. These include increasing Internet bandwidth, the widespread digitization of physical media files, and the capabilities of home PC's increasing to better handle playing and storing digitized audio and video files. Users were able to transfer either one or more files from one computer to another across the Internet through various file transfers and file-sharing networks.

2.2 Problems From Filesharing



Source: Harris Interactive/BPI Digital Music Survey
Base: all P2P users

Fig. 1 Problems From Filesharing

3 Malware

Along with viruses, one of the biggest threats to computer users on the Internet today is malware. It can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally screw things up. Malware programs are usually poorly-programmed and can cause your computer to become unbearably slow and unstable in addition to all the other havoc they wreak. Many of them will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean. This guide will detail the different varieties of malware along with basic preventive measures. In a follow-up article, we will examine the removal process and review a set of spyware removers. Although also considered to be malware, programs such as viruses, worms, trojans, and everything else generally detected by anti-virus software will not be discussed here, and the use of the word malware will only explicitly refer to software that fits in the categories listed below. You can get infected by malware in several ways. Malware often comes bundled with other programs (Kazaa, iMesh, and other file sharing programs seem to be the biggest bundlers).

3.1 Types of malware

Adware

Adware is the class of programs that place advertisements on your screen. These may be in the form of pop-ups, pop-unders, advertisements embedded in programs, advertisements placed on top of ads in web sites, or any other way the authors can think of showing you an ad. The pop-ups generally will not be stopped by pop-up stoppers, and often are not dependent on your having Internet Explorer open. They may show up when you are playing a game, writing a document, listening to music, or anything else. Should you be surfing, the advertisements will often be related to the web page you are viewing.

Spyware

Programs classified as spyware send information about you and your computer to somebody else. Some spyware simply relays the addresses of sites you visit or terms you search for to a server somewhere. Others may send back information you type into forms in Internet Explorer or the names of files you download. Still others search your hard drive and report back what programs you have installed, contents of your e-mail client's address book (usually to be sold to spammers), or any other information about or on your computer – things such as your name, browser history, login names and passwords, credit card numbers, and your phone number and address. Spyware often works in conjunction with toolbars. It may also use a program that is always running in the background to collect data, or it may integrate itself into Internet Explorer, allowing it to run undetected whenever Internet Explorer is open.

Hijackers

Hijackers take control of various parts of your web browser, including your home page, search pages, and search bar. They may also redirect you to certain sites should you mistype an address or prevent you from going to a website they would rather you not, such as sites that combat malware. Some will even redirect you to their own search engine when you attempt a search. NB: hijackers almost exclusively target Internet Explorer.

Toolbars

Toolbars plug into Internet Explorer and provide additional functionality such as search forms or pop-up blockers. The Google and Yahoo! toolbars are probably the most common legitimate examples, and malware toolbars often attempt to emulate their functionality and look. Malware toolbars almost always include characteristics of the other malware categories, which is usually what gets it classified as malware. Any toolbar that is installed through underhanded means falls into the category of malware.

Dialers

Dialers are programs that set up your modem connection to connect to a 1-900 number. This provides the number's owner with revenue while leaving you with a large phone bill. There are some legitimate uses for dialers, such as for people who do not have access to credit cards. Most dialers, however, are installed quietly and attempt to do their dirty work without being detected.

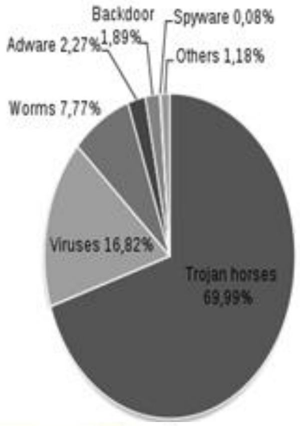
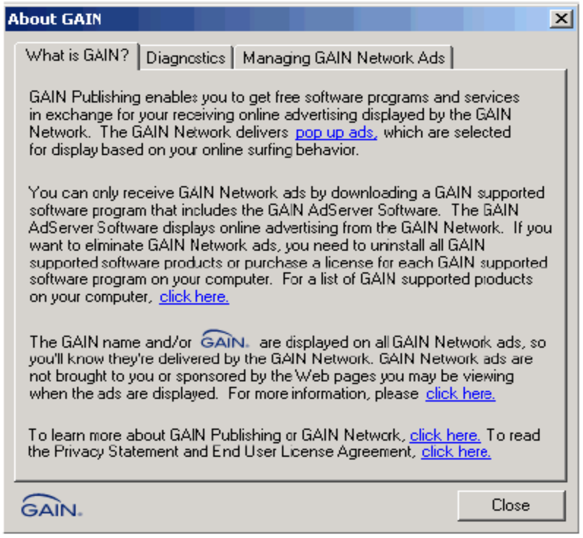


Fig. 2 Malware By Categories

Gain

One of the oldest and best known examples of malware is from the company Claria, which changed its name from Gator in 2003. Unlike most malware creators, Claria is a legitimate corporation with several big name advertisers and offices in both the United States and Europe. Claria is the maker of Gator Advertising and Information Network Publishing (or just GAIN), which actually consists of two programs that run in the background and work together. One program pops up ads while the other collects personal information. GAIN is typically bundled with other programs, including several published by Claria.

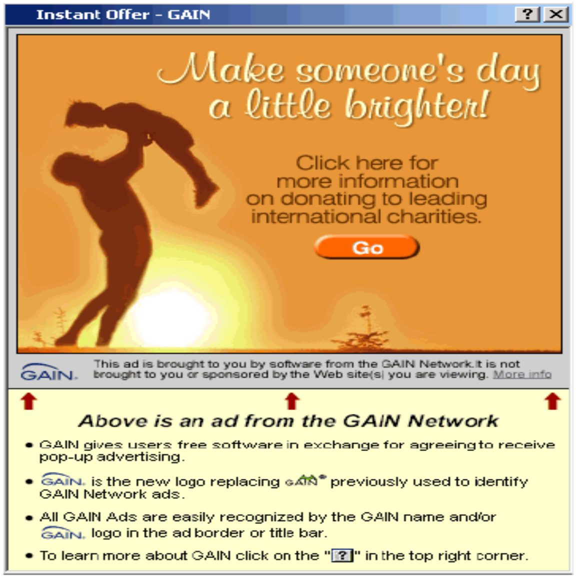


GAIN Publishing enables you to get free software programs and services in exchange for your receiving online advertising displayed by the GAIN Network. The GAIN Network delivers pop up ads, which are selected for display based on your online surfing behavior.

You can only receive GAIN Network ads by downloading a GAIN supported software program that includes the GAIN AdServer Software. The GAIN AdServer Software displays online advertising from the GAIN Network. If you want to eliminate GAIN Network ads, you need to uninstall all GAIN supported software products or purchase a license for each GAIN supported software program on your computer. For a list of GAIN supported products on your computer, click here.

The GAIN name and/or GAIN. are displayed on all GAIN Network ads, so you'll know they're delivered by the GAIN Network. GAIN Network ads are not brought to you or sponsored by the Web pages you may be viewing when the ads are displayed. For more information, please click here.

To learn more about GAIN Publishing or GAIN Network, click here. To read the Privacy Statement and End User License Agreement, click here.

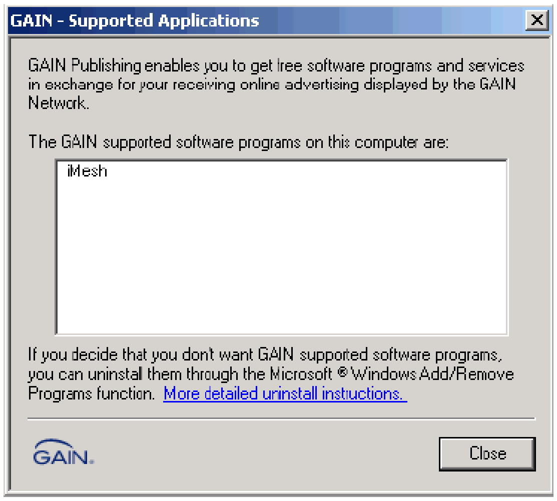


This ad is brought to you by software from the GAIN Network.It is not brought to you or sponsored by the Web site(s) you are viewing. More info

Above is an ad from the GAIN Network

- GAIN gives users free software in exchange for agreeing to receive pop-up advertising.
- GAIN. is the new logo replacing GAIN* previously used to identify GAIN Network ads.
- All GAIN Ads are easily recognized by the GAIN name and/or GAIN. logo in the ad border or title bar.
- To learn more about GAIN click on the "?" in the top right corner.

As far as malware is concerned, GAIN at first glance looks to be a well-behaved program. As can be in the above examples, all GAIN ads are usually clearly marked as such. Also included with GAIN is a utility that will display which program or programs it was bundled with, and thus require its presence, as shown below.



GAIN Publishing enables you to get free software programs and services in exchange for your receiving online advertising displayed by the GAIN Network.

The GAIN supported software programs on this computer are:

iMesh

If you decide that you dont want GAIN supported software programs, you can uninstall them through the Microsoft ® Windows Add/Remove Programs function. More detailed uninstall instructions.

Unfortunately, GAIN does not come with an uninstaller of its own. One must use the uninstaller used by the program GAIN came bundled with and hope it does a thorough job. A closer look at GAIN reveals more troubling features of the program. The first trouble signs come from the GAIN Privacy Statement (the privacy statement from the latest GAIN version, 6.0, is used here). From the privacy policy, we learn GAIN is doing a bit more than simply serving ads. These other functions cause GAIN to cross categories and also fall into the realm of spyware.

From the statement, we learn that Claria likely is not only getting money from advertisements, but they are also gathering information that they can then sell to other entities. Claria also anonymously collects information it finds on the user's computer, including their zip code, first name, software that is installed, even what password they use for eWallet, a program Claria distributes. They do not stop there, however.

We also associate the anonymous information we collect with a particular computer through a randomly generated anonymous ID number.

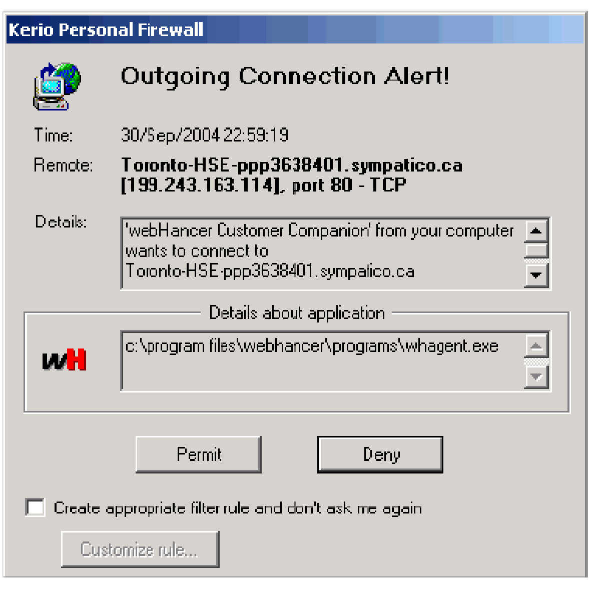
In short, Claria maintains a database with profiles of each machine on which GAIN has been installed. Each profile has all the information mentioned before, along with anything they can infer from that data. Claria doesn't simply store this information away, but also shares some of it with third parties:

We share certain anonymous information we collect in aggregated form with some of our partners and prospective partners... Our partners may use this anonymous aggregated information to improve their services, and may, in some cases, share this anonymous aggregated information with third parties such as their customers. Keep in mind that, as intrusive as Claria's data collection policies may sound, Claria is still a corporation with a public image to worry about. It is an easy target for lawsuits should Claria attempt something that goes against their user agreements (whether such agreements are legally binding is largely untested). The larger problem comes from the vast majority of spyware programs are created by groups or individuals who will have no problem stealing whatever data they can from you, and they will not keep it anonymous or private. Most spyware creators do not have a valid website, much less any sort of user agreement or privacy statement they are obliged to keep.

WebHancer

webHancer is a spyware application that is commonly bundled with other programs. Upon installation, it starts a program that runs in the background.

This program, according to webHancer's Privacy Policy, collects details of your surfring, such as the URL, page size, page load time, page completion state, and network delay time of the sites you visit. Looking at their products page, it is obvious they are going to sell the information gathered to other entities, as they attempt to answer questions like "What other sites are my customers visiting? Before? After? Where are they buying?" webHancer claims to have their program installed on millions of desktops, and it's likely that most of those running the program have no idea what it's doing.


Kerio Personal Firewall

Outgoing Connection Alert!

Time: 30/Sep/2004 22:59:19

Remote: Toronto-HSE-ppp3638401.sympatico.ca [199.243.163.114], port 80 - TCP

Details: 'webHancer Customer Companion' from your computer wants to connect to Toronto-HSE-ppp3638401.sympatico.ca

Details about application

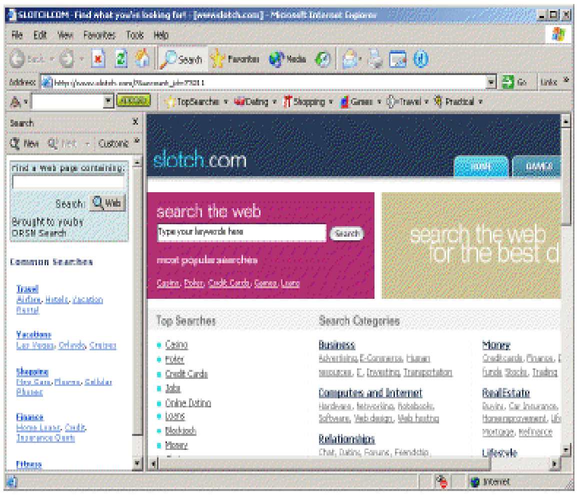
c:\program files\webhancer\programs\whagent.exe

□ Create appropriate filter rule and don't ask me again

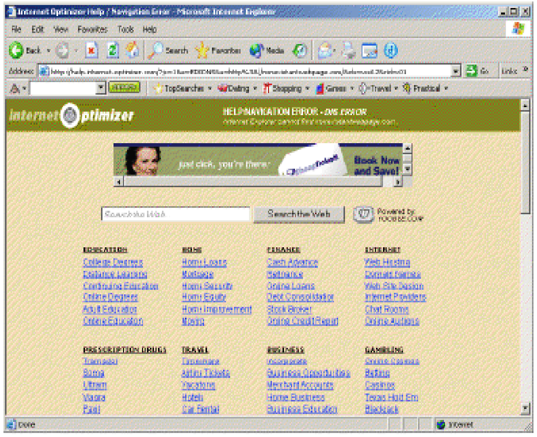
While browsing the Internet for several minutes with Kerio Personal Firewall installed (we'll discuss firewalls later), I was constantly being alerted that webHancer was attempting to access the Internet, always while a page was loading or immediately after it was finished loading. This didn't happen on every page, and there did not seem to be any real relationship between what web site I was viewing and when webHancer would attempt to connect (it went crazy while I was loading Slashdot, for example, but was quiet when I went to Ars). Because of its deep hooks into Windows, webHancer has been known to leave the computer without working networking after being uninstalled (to fix this, the company suggests installing and uninstalling webHancer again) and may cause errors in other programs.

ISTBar

ISTBar is a combination toolbar and hijacker. It installs a toolbar with search functions provided by slotch.com, a web portal. The toolbar also has links to various web sites and a list of "TopSearches," which include such classic keywords as "Britney Spears," "Blackjack," and "Loans." ISTBar also sets your home page to www.slotch.com (which is infested with pop-up ads) and adds its own search sidebar to replace the default one.



ISTBar includes the ability to download and install other software. Among the processes started by ISTBar is a hijacker that redirects you to internet-optimizer.com when you enter a bad URL This sends the link you attempted to retrieve to internet-optimizer.com in the process.

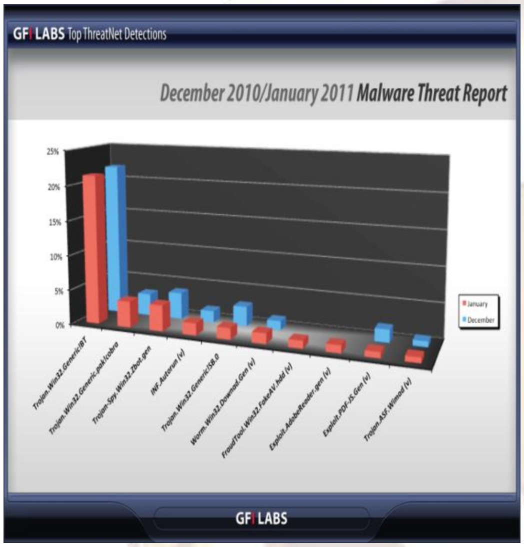

Internet Optimizer Help / Navigation Error - Microsoft Internet Explorer
File Edit View Favorites Tools Help
internet optimizer
HELP/NAVIGATION ERROR - DNS ERROR
Book Now and Save!
Search the Web
EDUCATION
HOME
FINANCE
INTERNET
PRESCRIPTION DRUGS
TRAVEL
BUSINESS
GAMBLING
Done
Internet

3.3 GFI's Top 10 Malware List

Top 10 detections for December

Detection	Type	Percent
Trojan.Win32.Generic!BT	Trojan	21.38
Trojan.Win32.Generic.pak!cobra	Trojan	3.71
Trojan-Spy.Win32.Zbot.gen	Trojan	3.69
INF.Autorun (v)	Trojan	1.68
Trojan.Win32.Generic!SB.0	Trojan	1.59
Worm.Win32.Downad.Gen (v)	Worm.W32	1.47
FraudTool.Win32.FakeAV.hdd (v)	Trojan	1.06
Exploit.AbobeReader.Gen (v)	PDF Exploit	1.06
Exploit.PDF-JS.Gen (v)	PDF Exploit	0.80
Trojan.ASF.Wimad	Trojan	0.73

Table.1 Top 10 Malware List



Malware Evolution

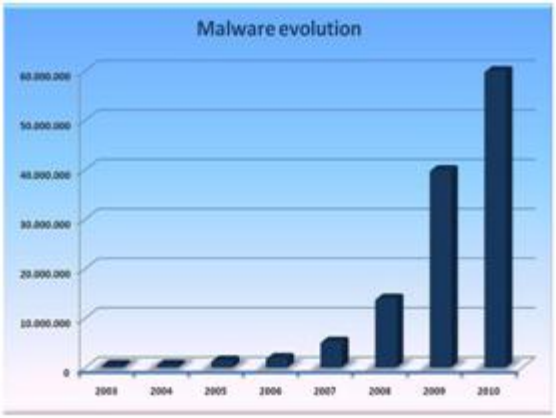


Fig 3 Malware Evolution

Sites infected due to malware

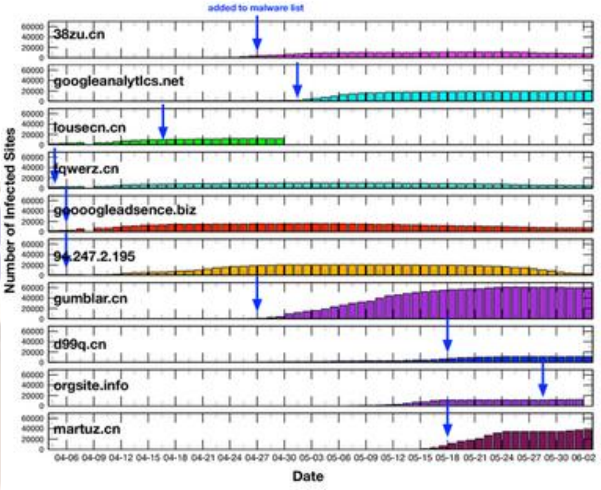


Fig. 4 Sites infected due to malware

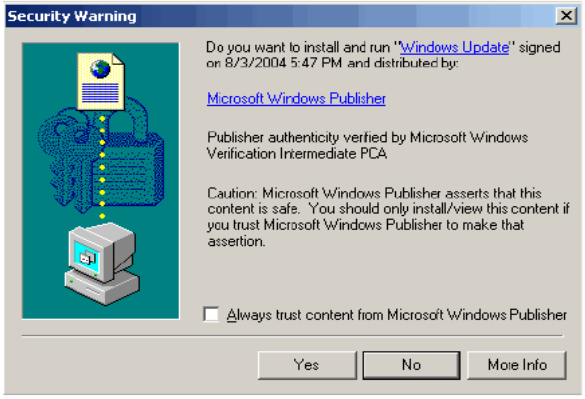
4 Malware prevention

The easiest way to deal with malware is to not get it in the first place. A little bit of common sense helps, but experience goes a lot farther. Experienced computer users, like it or not, hopefully possess the common sense that will let them avert potential disasters.

This edge can be acquired. The distinction is largely one of attitude, one which for lack of a better term I'll call "skeptical computing." We can examine this attitude and see how it reacts to common sources of trouble. Skeptical computing breaks down into two parts. The first is having a minimum level of expectations for the working state of their computers. Operating systems for personal computers are extremely stable and reliable. Computers are no longer the cantankerous contraptions they were with Windows 9x or earlier versions of Mac OS. It's not acceptable to have a computer that runs at a snail's pace with advertisements flying up left and right. If things aren't working as they should, you can find a fix, whether through Google, anonymous forums, or your friendly neighborhood guru.

4.1 Drive-by-Downloads

Internet Explorer can prompt users to download software that gets automatically installed on computers. The intention is that programs, such as Flash, that certain web pages depend on for viewing, can be seamlessly loaded so the user's browsing experience isn't interrupted. However, many malware developers take advantage of this process to foist their wares on unsuspecting users. Let's look at two examples, one legitimate and one malicious:



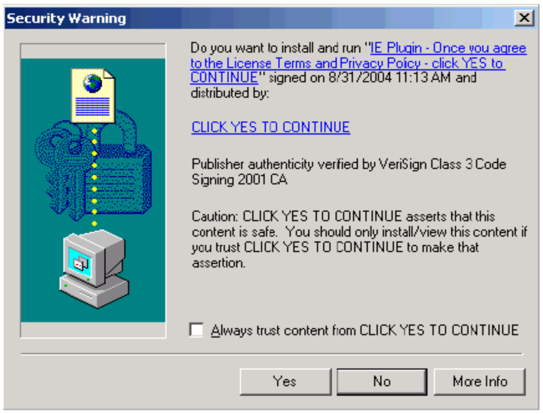
Do you want to install and run "Windows Update" signed on 8/3/2004 5:47 PM and distributed by:

Microsoft Windows Publisher

Publisher authenticity verfied by Microsoft Windows Verification Intermediate PCA

Caution: Microsoft Windows Publisher asserts that this content is safe. You should only install/view this content if you trust Microsoft Windows Publisher to make that assertion.

□ Always trust content from Microsoft Windows Publisher



Do you want to install and run "IE Plugin - Once you agree to the License Terms and Privacy Policy - click YES to CONTINUE" signed on 8/31/2004 11:13 AM and distributed by:

CLICK YES TO CONTINUE

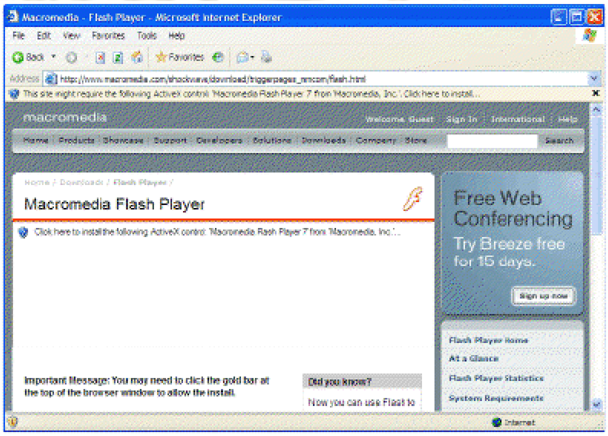
Publisher authenticity verfied by VeriSign Class 3 Code Signing 2001 CA

Caution: CLICK YES TO CONTINUE asserts that this content is safe. You should only install/view this content if you trust CLICK YES TO CONTINUE to make that assertion.

□ Always trust content from CLICK YES TO CONTINUE

It's important to separate the generic form filler from the content provided by the program in each case. The item on the left identifies itself as "Windows Update," the other "IE Plugin - Once you agree to the License Terms and Privacy Policy- click YES to CONTINUE." The program on the right is imploring you to click yes, not Internet Explorer. It also doesn't really tell you what the program is. Disregarding the second half of its name, it just identifies itself as "IE Plugin." It's not clear where it came from or what it would do if you installed it. This is one major tip-off. Both products identify their supposed (remember, be skeptical) publisher. The one on the left is from "Microsoft Windows Publisher," the right from "CLICK YES TO CONTINUE." What would a program gain from obscuring its origin, especially by inserting a message in its place that suggests that clicking yes is your only option?

The last unique piece of information is the group that verified the publisher's identity. This bit doesn't tell you very much in either case. Both sound legitimate. However, weighing what else we know, it's safe to say that the program on the right is bad news. The program on the left looks trustworthy. While our deductions were accurate in both cases, you should also consider what you were doing when you received the prompt. The left prompt appeared while browsing Windows Update, the right prompt showed up on a warez site. It's quite reasonable to expect that OS updates would require something to be installed. When you're looking at something seamy or of questionable legality, you should be on the lookout for possible malware. It should be noted that drive-by download prompts have changed in Windows XP SP2. The new design stops controls when new dialogs pop up and forces you to think more about what you're about to download. Let's look at what happens when Flash wants to install itself.



http://www.macromedia.com/shockwave/download/triggerpages_mmcom/flash.html

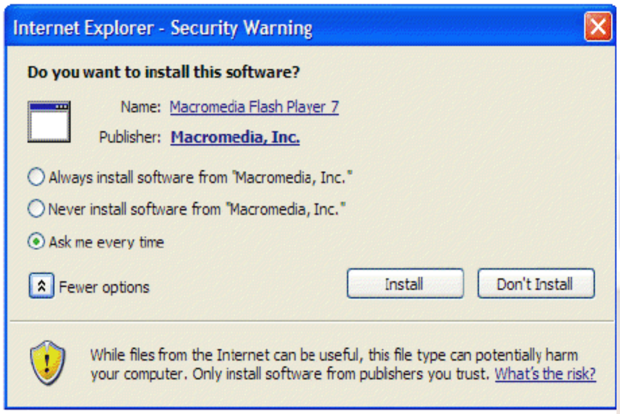
This site might require the following ActiveX control: 'Macromedia Flash Player 7' from 'Macromedia, Inc.'. Click here to install...

Click here to install the following ActiveX control: 'Macromedia Flash Player 7' from 'Macromedia, Inc.'...

Important Message: You may need to click the gold bar at the top of the browser window to allow the install.

Unlike in prior versions of Windows, a dialog box is not the first thing to appear. Instead, a brief message appears in the toolbar, similar to IE's built-in pop-up blocker. It informs you that the page wants to install an ActiveX Control. The information, program name, and publisher are exactly the same.

When you click on the message, you can either allow the installation, or seek further help ("What's the Risk?"). The help is a generic section of IE's help page informing you of the risks associated with installing ActiveX controls. If you choose to install, you then see a dialog similar to the one we looked at before: can tell it to always deny the installation of controls from any given publisher. Definitely useful for users who frequently get asked to install particular pieces of malware, or just those who have a vendetta against Flash.



Internet Explorer - Security Warning

Do you want to install this software?

Name: Macromedia Flash Player 7

Publisher: Macromedia, Inc.

○ Always install software from "Macromedia, Inc."

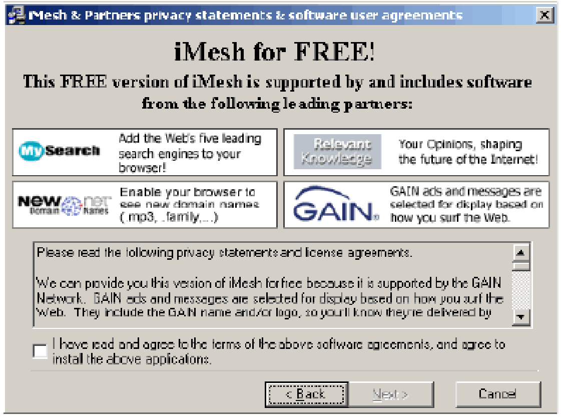
○ Never install software from "Macromedia, Inc."

● Ask me every time

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

4.2 Bundlers

Much malware, especially adware, comes bundled with other programs. P2P software is a common source of bundled adware. The following message comes up while installing iMesh:



iMesh & Partners privacy statements & software user agreements

iMesh for FREE!

This FREE version of iMesh is supported by and includes software from the following leading partners:

MySearch — Add the Web's five leading search engines to your browser!

Relevant Knowledge — Your Opinions, shaping the future of the Internet!

New.net Domain Names — Enable your browser to see new domain names (.mp3, .family,...)

GAIN — GAIN ads and messages are selected for display based on how you surf the Web.

Please read the following privacy statements and license agreements.

We can provide you this version of iMesh for free because it is supported by the GAIN Network. GAIN ads and messages are selected for display based on how you surf the Web. They include the GAIN name and/or logo, so you'll know they're delivered by

□ I have read and agree to the terms of the above software agreements, and agree to install the above applications.

You can't say the program isn't honest. It lets you know it's ad-supported, which pieces of adware get installed, and what you agree to in the process. Messages about required programs for displaying ads should set off warning sirens in your head. That information alone should be enough to make you stop installation.

4.3 Basic protection approches to malware

Organization/users can formulate their anti malware stategy depending upon the type and complexity of malware attackas that they are exposed to,and the level of risk associated with such attacks.different organizations use different tools and approches to counter malware attacks.selection of such tools and approches is often based on their funtionality suitability and cost.the basic –malware approches that are traditionaly used on their nature of their action .

They are

1. Reactive approach

2. Proactive approach

Reactive approach :

Reactive approch is an incident response process.inthis method once a problem is encountered ,the investigation of the problem, anlysis and finding remedy,and documenting the resolutions for future remedial are done,mostly in the sameorder.

The existing anti-malware tools available ,idetify the malware by scanning the computer executable files and check if any known malware have sneaked into the system.this is done by detecting programs that are making changes to operating system registry.here the anti-malware tools and products chase the malware by identifyi ng them after they have entered the system and the system shows some symtoms of being some infected ,depending on their behavior and instances. When dealing with reactive appraoch of your system ,which is being infected corporates have three alternmatives for dealing with malware.they are:

1. Running malware removal tool to detect and repair malware.

2. If anti –malware tools fails,malware can be removed manually by the administration or by formatting the ssystem.3.use anti-malware tool to present them from entering the system

As presentive measures companies include disaster recovery plans ,reinstalling Operating system ,system formating and moving to alternative as their reactive approaches.all these methods neeed to be in place ,so that can function as and when they are needed.as with any reactive approches these techniques are time-consuming , error prone and costly.

What to do if system is infected with malware using reactive approach?

1. Make sure the firewall in place iis working .get positive control over inbound outbound traffic on the systems and on the network.
2. Address the most likely suspects first ,clean the most comman malwaretheats and then check for unknown theats.
3. Isolate the infected system .get is off the network and the internet.stop the infection from spreading to other outbreak system on the network during the cleaning process.
4. Research outbrech control and cleanup techniques.
5. Download the latest virus definiations from anti-virus software vendors.
6. Ensure that anti-virus systems are configured to scan all filles.
7. Run a full system scan.
8. Restore missing or corrept data.
9. Remove or clean infected files.
10. Confirm that the computer systems are free of malware.
11. Reconnect the cleaned computer systems to the network.

Proactive approach:

Expreances state that proactive approach has its own advantage over reactive approach. As new technologies emerge,malware writers are adoptong high –level programing lagvages ,new technologies and methods of attacks with varied features and payloads.in reactive appraoch a malware can be identifying only if they are in existence ,i.e at least executed once.wheres in a proactive approchs a malware can be identified as new ,as they are and they can be quarantied or deleted even they get executed.

Proactive approches include various techniques that can enable the user to indetify the malware when they attempt to invade tha system. Unfortunately getting infected with malware is useually much easier than getting rid of it, and once you get malware on your computer it tends to multiply.

What to do if system is infected with malware using proactive approach:

1. Apply the latest firm ware to hardware systems and routers as recommended by venders.
2. Apply the latest security patches to server applications and other applications.
3. Subscribe to security –related email lists from venders and patechs when recommended
4. Ensure that all microsoft computer system are running anti-virus software.
5. Ensure that automated processes are running to regularity update the virus difunitions.
6. Maintain a database that keeps tracks of what patchs have been applied.
7. Review security logs.
8. Enable perimeter or host based firewalls.
9. Use avulnerbility scanners such as the microsoft baseline security anlysis that helps to detect common security misconfiguration and missing security updates on your compter systems.
10. Use least privileged user accounts (lua).if flow priviliged processes are compresed ,they will do less damage than high –priviliged process.

Conclusion

Peer-to-peer (P2P) networks continue to be popular means of trading content. However, very little protection is in place to make sure that the files exchanged in these networks are not malicious, making them an ideal medium for spreading malware.
Malware is highly pervasive in P2P file-sharing systems and is difficult to detect automatically before actually downloading a file due to the insufficient and biased description of a file return to a client as a query result.To alleviate this problem we provide preventive measures for malware. And also we provide two basic approaches reactive and proactive for prevention of malware.

REFERENCES

[1] Clip2, "The Gnutella Protocol Specification v0.4," http://www.clip2.com/ GnutellaProtocol04.pdf, Mar. 2001.

[2] E. Damiani, D. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, "A Reputation-Based Approach for Choosing Reliable Resources in Peer-to- Peer Networks," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 207-216, Nov. 2002.

[3] X. Yang and G. de Veciana, "Service Capacity in Peer-to-Peer Networks," Proc. IEEE INFOCOM '04, pp. 1-11, Mar. 2004.

[4] D. Qiu and R. Srikant, "Modeling and Performance Analysis of BitTorrent- Like Peer-to-Peer Networks," Proc. ACM SIGCOMM, Aug. 2004.

[5] J. Mundinger, R. Weber, and G.Weiss, "Optimal Scheduling of Peer-to-Peer File Dissemination," J. Scheduling, vol. 11, pp. 105-120, 2007.

[6] A. Bose and K. Shin, "On Capturing Malware Dynamics in Mobile Power- Law Networks," Proc. ACM Int'l Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 1-10, Sept. 2008.

[7] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa, and S. Chien, "A First Look at Peer-to-Peer Worms: Threats and Defenses," Int'l Workshop Peer-To-Peer Systems, Feb. 2005.

[8] F. Wang, Y. Dong, J. Song, and J. Gu, "On the Performance of Passive Worms over Unstructured P2P Networks," Proc. Int'l Conf. Intelligent Networks and Intelligent Systems (ICINIS), pp. 164-167, Nov. 2009.

[9] R. Thommes and M. Coates, "Epidemiological Models of Peer-to-Peer Viruses and Pollution," Proc. IEEE INFOCOM '06, Apr. 2006.

[10] J. Schafer and K. Malinka, "Security in Peer-to-Peer Networks: Empiric Model of File Diffusion in BitTorrent," Proc. IEEE Int'l Conf. Internet Monitoring and Protection (ICIMP '09), pp. 39-44, May 2009.

[11] J. Luo, B. Xiao, G. Liu, Q. Xiao, and S. Zhou, "Modeling and Analysis of Self-Stopping BT Worms Using Dynamic Hit List in P2P Networks," Proc. IEEE Int'l Symp. Parallel and Distributed Processing (IPDPS '09), May 2009.

[12] W. Yu, S. Chellappan, X. Wang, and D. Xuan, "Peer-to-Peer System-Based Active Worm Attacks: Modeling, Analysis and Defense," Computer Comm., vol. 31, no. 17, pp. 4005-4017, Nov. 2008.

[13] A. Ganesh, L. Massoulie, and D. Towsley, "The Effect of Network Topology on the Spread of Epidemics," Proc. IEEE INFOCOM, 2005.

[14] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos, "Epidemic Spreading in Real Networks: An Eigenvalue Viewpoint," Proc. IEEE Int'l Symp. Reliable Distributed Systems (SRDS), 2003.

[15] M. Newman, S. Strogatz, and D. Watts, "Random Graphs with Arbitrary Degree Distribution and Their Applications," Physical Rev. E, vol. 64, no. 2, pp. 026118(1-17), July 2001.

[16] D. Stutzbach and R. Rejaie, "Characterizing the Two-Tier Gnutella Topology," Proc. ACM Int'l Conf. Measurement and Modeling of Computer Systems (SIGMETRICS), pp. 402-403, June 2005.

[17] R. Pastor-Satorras and A. Vespignani, "Epidemic Dynamics in Scale-Free Networks," Physical Rev. E, vol. 65, no. 3, p. 035108(1-4), Mar. 2002.

[18] O. Diekmann and J. Heesterbeek, Mathematical Epidemiology of Infectious Diseases: Model Building, Analysis and Interpretation. Wiley, 1999.

[19] P. van den Driessche and J. Watmough, "Reproduction Numbers and Sub- Threshold Endemic Equilibria for Compartmental Models of Disease Transmission," Math. Biosciences, vol. 180, pp. 29-48, 2002