Bet you didn't know your PC could be a Zombie.

By Andrew Ockrim

WASHINGTON, D.C., Oct. 27, 2005 – Like medical researchers studying a highly contagious virus, Microsoft Internet Safety Enforcement investigators carefully experimented with a tiny piece of malicious code, used by computer criminals to hijack personal computers without their owners' knowledge. Placing a single copy of the code onto a healthy computer and then connecting the computer to the Internet, almost immediately, the researchers noticed the first signs of life. The infected computer sent an alert with its Internet location and hijack status to a distant server. Then, connection requests from hundreds of remote computers poured into the PC, commanding the infected computer to distribute millions of illegal spam e-mails. These requests meant one thing: the investigators had successfully created a "zombie" computer.

Turning your computer into a Zombie

While the zombies of Hollywood B-movies are easily identifiable by their gruesome appearance and hunger for flesh, zombie computers are silent stalkers. People who use the Internet but don't properly protect their PCs from computer criminals may never know that their machines have been compromised – even after their infected machines begin causing problems for other people and potentially, themselves.

Computer criminals have turned their attention to creating zombies. They do so by tricking people into loading malicious code by hiding it in e-mail attachments or in music, video or other files that people download online, or even within data transferred when clicking on an infected Web site or embedded image.

Illegal spam sent by zombie computers has increased dramatically in recent months and, as of this summer, accounts for more than half of all spam, according to studies conducted by industry groups. In addition, computer criminals can use zombie computers to launch phishing attacks that try to steal personal information, such as credit card and banking details and use it for identity theft.

As more people sign up for high-speed Internet connections at home, computer criminals have set their sights on a growing population of potential zombies that never sleep. "High-speed connections are an extremely convenient and powerful way to access the Internet, but people need to realize that their connections don't turn off when they walk away from their computers."[1] In less than three weeks, the Microsoft lab's zombie computer received more than 5 million requests to send 18 million spam e-mails. However, spam messages are only the tip of the iceberg for zombies (also known as bots *<robots>,* bot-nets *<robot networks>* and a multitude of different names.

The *infection* stage involves using various techniques to spread the bots, both direct and indirect. Direct techniques include exploiting vulnerabilities of the operating system or services. Indirect attacks employ other software for the dirty work – they include using malicious HTML code on web pages, exploiting Internet Explorer vulnerabilities or using other malware distributed through peer–to–peer (file sharing) networks or through DCC (*Direct Client–to–Client*) file exchange on Internet Chat applications.

Direct attacks are usually automated with the use of worms. All worms have to do is search the Internet for vulnerable systems and inject the bot code. Each infected system then continues the infection process, allowing the attacker to save precious resources and providing plenty of time to look for other victims. All of this is done without the PC owner's knowledge or input.

The mechanisms used to distribute bots are one of the main reasons for so–called Internet *background noise*. Windows in particular seems to be the attackers' favourite target because it is easy to find unpatched Windows computers or ones without firewalls or anti-spyware applications correctly installed and updated. It is often the case (and much easier) to target home PC users and small businesses, which overlook security issues and increasingly have always-on broadband Internet connections. However, MAC attacks are increasing and some experts predict it will even itself out in the not too distant future as there has been a lag in security development for the Mac operating systems.

The first thing the bot/zombie does after it is successfully installed is connect to an IRC server and join the control channel with the use of a password. The bot (your PC) is then

---

[1] Aaron Kornblum, cited in "Stopping Zombies Before They Attack," *Microsoft*. http://www.microsoft.com/presspass/features/2005/oct05/10-27Zombie.mspx 15/09/2006.

ready to accept commands from the master application. This all happens in seconds in the background whilst the user is completely oblivious.
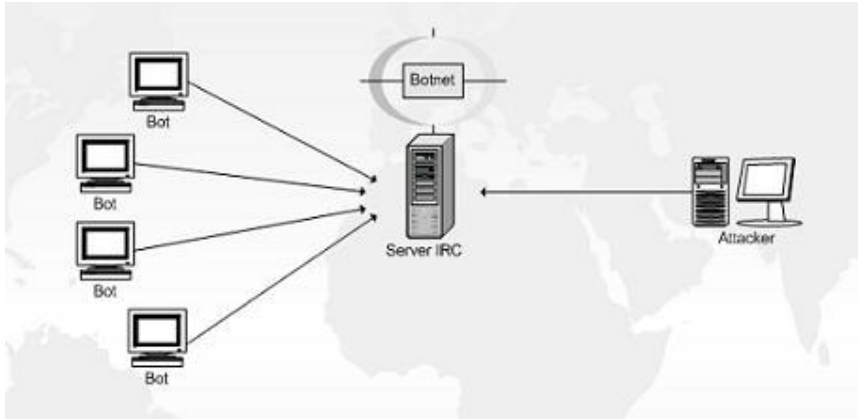

Fig 1. A simple graphic of a basic bot-net.

How zombie networks fuel cybercrime

The botnet controllers are cashing in, potentially using your PC for free. Eavesdropped chat-room exchanges reveal that a Zombie and botnet attacks appear to cost between $500 and $1500, with smaller botnet attacks priced between $1 and $40 per zombie harnessed. It's such a reliable way to make money that crackers don't need day jobs.

To detect zombies active in their networks, corporate systems administrators check for telltale network traffic indicators. But crackers are now covering their tracks by making the bots corrupt their own program code when extracted. This makes it very hard for home users and small businesses without the skills, to find them.

Similar to cockroaches, you spray in the kitchen behind the cupboards but they find other ways to survive. You only get rid of some. The trick is not to attract them in the first place and to be vigilant about prevention.

Why worry about security and all this??

Simple, because you don't want your PC to be used to attack your friends or livelihood, or do you? The other trailing issues are that once compromised, your PC is literally in the hands of the cracker. They potentially will be able to see everything you do online and offline by installing applications like key-loggers in order to steal your passwords and track your every move online. This is besides it being used to send millions of illegal spam messages that you may held legally accountable for.

In the wrong hands, minimal amounts of personal information can be used to set up false identities in your name and you may be left with massive bills and legal expenses.

Don't think for a second "it won't happen to me". It will and you will be very surprised at how fast it all happens.

Your stolen bank details will have your accounts cleaned out within 3 mins. Your stolen personal information such as birth date, address and such will be used to create false credit cards produced and on the streets within 4 - 48 hours, ringing up a nice debt in your name.

You will be inundated with spam and your details are very likely to be sold to telemarketing companies or mass mailing companies.

And this is only the tip of the iceberg… It can get a lot worse than that. There are numerous accounts of innocent people being arrested and jailed in their own countries (and overseas) on warrants issued in relation to stolen identities and computer crimes that they didn't commit. It can take years and thousands of dollars to clear your name.

So is it worth the effort and learning curve to purchase genuine software and maintain it to combat these threats? Well if it costs $200-300 for the software – surely it's cheaper than 2-3 years worth of lawyer's fees or worse…

Signs your computer may be infected

- Computers that are running way too slowly may have a bot on them. (Of course this is a purely subjective criteria and is not always a reliable sign. Too many people think that their computer is infected with something just because it behaves a little flaky. Other causes of slowness could be spyware, too many applications set to start up automatically or in the quick start bar, sluggish cumbersome apps, filesharing or a very fragmented hard drive. Regardless, if the computer is running very slowly for no obvious reason, then you may have something worth investigation.)
- Sudden slow computer performance on the internet
- Frequent network activity without you impetus
- Unexplained spikes in your internet bandwidth usage
- Continual high use rates even when you are not downloading or using heavily

So what do you do?

The scope of this article isn't intended to include comprehensive education on the kind of behaviour that can lead to becoming a zombie. Here are a few tips though:

1. Consider using Firefox or Opera internet browsers instead of Internet Explorer. They are generally more secure and infinitely more configurable to help prevent malicious web scripts and code. They also enable you to quickly disable ActiveX and Java.

2. Think long and hard before downloading software from sources you don't personally trust. This goes for both (pirated) file sharing services and apparently legitimate shareware download sites. (You may want to Google the software / vendor prior to downloading it – make sure it's the same thing and genuine).

3. Never download software from a pop-up/pop-under screen when browsing an internet site (especially the ones that tell you your PC is at risk). You have a more than 99% chance it will be packed with malicious software. Just because it's online doesn't guarantee integrity or authenticity. Do you take up every junk mail offer you receive? It's basically the same thing.

4. If you get an attachment in an email that you weren't expecting, don't open it. This even applies if you know the sender (if they are zombies they wont even know it was being sent to you). Running spam blocking software can help prevent messages with questionable attachments from getting into your inbox in the first place.

5. Use a commercial firewall to protect computers from cracking attacks while connected to the Internet. An effective firewall application can help to both prevent infections and notify you when something on your computer or the net is attempting to establish a questionable network connection.

6. Get computer security updates or use the automatic updating features to shield computers from viruses, worms and other threats. (Operating system and applications)

7. Purchase an anti-virus package from a major provider. Ensure that it is kept up-to-date daily to help protect against the latest threats. (use automatic updates)

8. Purchase anti-spyware software and beware of tricks designed to get people to download and install unwanted and sometimes destructive software. This software is sometimes distributed in non-commercial music downloads, file-sharing programs and free games.

9. It's also wise to deactivate support for scripting languages such as ActiveX and JavaScript (or at least control their use).

10. Do not use wireless networking unless you know exactly what you are doing. Wireless networks, especially for home/small biz use, are amongst the hardest to secure and should only be configured by an experienced security specialist. It is absolutely worth every cent, to pay a professional to do this (not a friend's son or your local computer retailer). The vast majority of wireless networks are about as secure as a "wet cardboard box." Think very carefully before you launch into this technology. Wired networks are still far more secure and reliable.

11. Don't use Outlook Express. It's convenient, ready to go and familiar. Outlook is the default email client for every windows version since 1998. Most spam and email virii are written to take advantage of that. Switch to Eudora, Thunderbird, Opera, Pegasus or Incredimail – all have superior features and offer much better protection. After a week you won't understand why you stuck it out for so long.

What is a firewall?

A firewall is a barrier between the Internet and your computer. It gets its name from physical firewalls in buildings/cars that prevent fires from spreading. A firewall is similar to a lock on a door - it prevents those without keys from entering a home or a room. Firewalls enforce security policies. These policies or rules are in the form of built-in filters that permit access only to authorised users. These filters also deny access to unauthorised users or to dangerous materials that can harm your computer.

Resources for more information

Because the potential threat is so great, the anti-zombie campaign stresses prevention as the best defence against spam and zombie attacks.

Common Software Vendors **(no particular order or preference)**
Antivirus (and also make firewall software):

AVP   http://www.avp.com
E-trust   http://www.etrust.com
F-secure: http://www.f-secure.com
Grisoft   http://www.grisoft.com
Sophos: http://www.sophos.com
Trend Micro: http://www.trendmicro.com
Symantec: http://www.symantec.com
Panda: http://www.pandasoftware.com
McAfee: http://www.mcafee.com
Network Associates   http://www.networkassociates.com
Computer Assoc: http://www.cai.com
Central Command: http://www.centralcommand.com
Kaspersky Lab: http://www.kaspersky.com

Firewall
Tiny Software: http://www.tinysoftware.com
Zone Labs: http://www.zonelabs.com
Black Ice: http://www.blackice.com
Agnitum   http://www.agnitum.com
Grisoft   http://www.grisoft.com
Sunbelt Software   http://www.sunbelt-software.com
Norman   http://www.norman.com

Spyware Removers:
Spyware Eliminator: http://www.aluriasoftware.com
Spy Sweeper: http://www.webroot.com
AntiSpy: http://www.omniquad.com
SpySubtract: http://www.intermute.com
SpyRemover: http://www.itcompany.com
SpyHunter: http://www.enigmasoftware.com
Ad-aware Pro: http://www.lavasoft.com
Spyware Doctor   http://www.pctools.com/spyware-doctor
Spybot Search-Destroy   http://www.safer-networking.org/en/index.html
Sunbelt Software   http://www.sunbelt-software.com

Other Resources

PCStats.com offers a Beginners Guide: Firewalls and Internet Security for those wanting to learn about firewalls. The URL is http://www.pcstats.com/articleview.cfm?articleID=1450

A tutorial on setting up ZoneAlarm Pro:
http://www.solutionsreview.com/ZoneAlarm_Pro_Setup.htm

ZDNet offers guides for securing a wireless network:
http://reviews-zdnet.com.com/4520-7297_16-5540710.html

You can test your system's security at any of these sites:
Shields Up   https://www.grc.com/x/ne.dll?bh0bkyd2
PC Flank   http://www.pcflank.com/about.htm
Audit My PC   http://www.auditmypc.com
Security Spacehttp://www.securityspace.com. (A basic audit or a single test is free)
HackerWhacker   http://hackerwhacker.com. (The first test is free)

Conclusion.

This article was written to inform less experienced computer users about some of the threats they face when being online. This represents my experience and that of some of my clients. Many of the tools and applications in resource lists are simply those that spring to mind and are not intended to be exhaustive or even comprehensive. I offer no preferences outside of supporting the commercial products, due to the increased support options available for paid products. If your local guru is out of town on holiday you have the fallback of calling the companies' support line for help.

There is no substitute for research and education and I encourage all readers to take a personal interest and keep up to date with your knowledge and your software. After all you take precautions to lock your doors and windows when you want to secure your living space, why would you not take a similar approach to your online space.