Parasites: what you can't see can hurt you

Stefan Gorling

Antisocial renegades are skirting legal frontiers to exploit your private information. They use software parasites to display advertising and spam relays or to collect confidential information about you, which they sell. These are not teenage pranksters. They are professionals competing to exploit security flaws first. And they exploit social behaviour to engineer sophisticated, targeted attacks. But, being aware of the risks, we can work to reduce the threat.

You have patched all your computers, installed the latest anti-virus software. Perhaps you have even tuned your firewall rules, added some intrusion detection and honed the efficiency of the spam filter. Is it time to lie back and enjoy summer?

Do so at your peril. Patches, anti-virus software, intrusion detection etc. are all good stuff to keep malicious code at bay. But it provides little protection against leaks of sensitive data if your users err.

It is not really about having dumb users anymore. These days it is no longer uncommon to hear security specialists admit that they too have fallen into the traps. Consider an email message from PayPal to warn you that your account is about to expire. It advises you to follow the www.paypal.com link and login to keep it active. It is hard to explain to a user that, in this case, the hotlink is an executable system file rather than a link to a website.

Having read this, no doubt you are leaning back in your chair, happy in the knowledge that your spam filter would have caught the executable. But what about parasites?

Parasites

Organizations and individuals are starting to suffer more and more from software that I call software parasites. I use the term deliberately to avoid a sterile discussion about naming and categorising various strains of malicious software. It is more worthwhile to focus on how they act.

I will concentrate on parasites that are not always detected by anti-virus software. These are often called spyware, adware or malware. There are other parasites such as trojans, worms etc. but as they are often caught by anti-virus software, I shall not discuss them here.

A parasite takes without giving, weakens without killing. It infects a host and lives by stealing from it.[1] Its purpose is to infect, to hide and to propagate. Electronic parasites are usually sent out by a master who tells them what to do, and to whom they report.

Such programs differ from computer viruses in that they are often embedded in other programs, or the user (who may be unwitting) installs them when he or she agrees to the terms in the end user licence agreement (EULA) for another program.

The security threat posed by spyware and other parasites is very grave. The software resides in the computer and is hard to find. From there it might track the user's online activity, capture keystrokes from the keyboard to steal passwords, credit-card numbers, etc., copy files from the network or simply open up a back door so that the master can control the machine remotely while the user is away.

Infestation

There are many parasites in the wild. Research shows that most computers connected to a network have some parasites. Some studies estimate that the average PC has 28 pieces of spyware running on it[2]. Even if this is an exaggeration, we may be sure that parasite infestation is not a theoretical problem. If you have no strategy to avoid them, you are probably infected.

Parasites include:

- Explorer toolbar software, which installs a third-party toolbar with features to "help" you visit the "right" pages.
- Spyware, which sends back private from your URL visits, keyloggers, files, etc. to a central server.
- Adware, which trigger advertisement displays when you enter specific URLs.

Dialers, which make your computer dial a premium rate number

Take for example a product from Ssppyy.com[3]. The company sells "The Most Powerful Remote Install Spy Software". For $59.95 you can buy a program to monitor all activity on a computer, take screenshots, log what you type at your keyboard and forward the emails you send. All information is compressed at regular intervals and mailed to an anonymous email address of your choice. If you pay the extra $40 for the professional version you receive a file browser that allows you to access all folders on the target host and network.

Big Brother is watching

Their selling point is that it could be used for monitoring your employees, your children or your spouse. And of course your competitors could use it to monitor you.

Symantec's database of "Expanded Threats"[4] describes the transmission as follows:

"Spyware.Ssppyy may arrive as an email greeting card. When you receive the email, Spyware.Ssppyy will silently install itself on your computer."

Symantec is one anti-virus companies that lists spyware in its database; not all do. Searching the virus databases at other major vendors for "ssppyy" yields varying results, so check with your anti-virus vendor. But remember, this is not a virus; it is a shareware program. And you can double-check because the Ssppyy homepage lists a number of major security products that it claims can't detect the program.

Greetings, sucker

So the question is, how many of your users open electronic greeting cards? If just one clicks on a fake card, your whole system could be compromised without anyone noticing. When these parasites infect your corporate network it is not only the workers' personal privacy that is at risk, the privacy of the whole organisation is at stake.

It is not all about viruses anymore. To simply rely on your anti-virus software to guard against parasites is to underestimate the problem. Even anti-virus software is pushed to keep pace with the rate at which current viruses disperse. A study has shown that the Blaster worm infected 90% of all vulnerable computers in its first 10 minutes of activity[5]. This leaves very little time for an anti-virus company to receive a sample, find a pattern to block it, publish it, and for network administrators to put in the fix.

Therefore anti-virus software is not a silver bullet for your organization. It is a painkiller. It makes your head hurt a little less, but it cannot cure the disease. When even system administrators can admit that they have been fooled, we cannot assume that our users can avoid the pitfalls.

User choice

Parasites such as spyware and adware present two new problems compared to purely malicious code. First of all, the users often choose to install the software, especially if it is embedded in a program that the user has downloaded on purpose. Or the user could agree to install the software in order to visit a certain homepage.

The other problem is to decide what is good and bad behaviour. Anti-virus software vendors differ on how to treat the parasites.

If you download the KaZaa peer-to-peer file sharing software, you also get a software module from Claria Corporation (previously known as Gator). This tracks every Web page address you visit and reports it back to their servers. This helps to drive context-specific pop-up ads. Without this piece of software, KaZaa will not work properly. I believe this bit of adware straddles the line between legitimate software and malicious code. My advice is to find a less intrusive alternative.

A connected computer is never totally secure. Therefore we are not in the business of securing computers. The aim is to ease the pain induced by security problems but still give users a working environment. There are a number of measures that can lower the risk of sensitive data leaking from the organization.

Most small and medium enterprises (SMEs) let their users add software to their machines. They tacitly accept that their users use peer-to-peer (p2p) software such as KaZaa or Gnutella to download music to their local hard drives. Naturally they do not condone it as it breaks copyright law. Nevertheless, many network administrators know or suspect that it is happening, but pressure of other work and the difficulty of detection makes it hard to police.

Lock-out

We always have the option to lock down the users computers completely, to remove all privileges from their accounts, to enforce the use of an approved set of applications, and to disallow anything that is not in the official policy. Even though this is desirable from a security standpoint, it is often not practical, at least, not in SMEs. Enforcing such strict rules is often seen as fascism as users cannot or will not understand the security risk they induce by installing unapproved software.

Moreover, there are genuinely useful products out there that do not always come to the attention of the policy makers, but which do make the users' lives easier. One might argue that there are indeed legal uses of p2p software, but the security implications are huge. Usability studies shows that most people are not aware of what data they actually share[6]. They might be sharing all your corporate documents, to the rest of the world, including your competitors.

Second, these forms of software are popular infection vectors for parasites and viruses. Shared files on p2p networks are often infected with viruses or trojans. Even though they share no data, some malicious code may change your network settings.

Instant messaging

Some analysts expect Instant Messaging to be the next security problem, given its growing popularity in corporate environments. Here information is spread unencrypted in a network where people identify themselves by cryptic aliases or numbers. The environment makes it easy for someone to spoof a known identity to send you a malicious file.

When locking down the desktop is not feasible, we need strict rules on what the computer is to be used for, and what is banned. Appropriateness determines what software a user may install and what he/she may not. For rules to be effective, they should be understandable, and the users trained. Therefore we cannot simply ban the use of software, but must explain why. Further, to be effective, the rules must be enforced. There is no point having a policy against p2p software if you never take an inventory of your users' applications and remove all inappropriate software.

Some vendors have produced software that detects and removes parasitic programs. One popular vendor is Ad-Aware[7], but there are many others. Such software may complement your current anti-virus solution.

Wrong looks

Firewalls are great tools that, configured correctly, do much to secure your

network. However, most configurations look outward to prevent incoming attacks but allow anything to pass to the outside. A wise security policy will consider limiting outgoing traffic so that parasites are less likely to succeed in pushing data back to their masters.

One example is outgoing access to the SMTP port (25). Today parasites send up to 80% of all spam[8]. Spyware and other parasites often have their own mail server. This lets them send mail without going through the corporate mail server. Blocking outgoing traffic on this port for all your (non-mail server) computers stops many of these parasites from working properly. This cuts the risk of data leaking as well as the risk of winding up on a spam blacklist.

NB notebooks

Another serious latent security risk is notebook or laptop computers. Many companies provide them to make staff more efficient. Some staff regard it as a fringe benefit in the same way that some firms pay their staff's mobile phone bills even for weekend and personal calls. If a portable computer is truly a fringe benefit, the user has to be able to install software on it, to play games during the weekend or to chat on-line. This exposes the machine to all that lurks in the wild. When it returns to the office, it might contain viruses detectable by your antivirus software, but also spyware that is not.

The following story may illustrate a few points. One morning when people returned to work in a SME a virus was detected indirectly due to an error condition it caused in Microsoft Windows. The virus was new, so the resident antivirus software did not detect it. The network was shut down and the virus was cleared out manually from each machine. Microsoft released a fix, but the machines had to be connected to the Internet to patch them.

Just when all machines were certified clean and were downloading the patch, an employee from another office arrived, sat down in a conference room to work on his laptop and logged onto the local area network. In a few minutes the rest of the machines on the LAN were hit again and the cleaning process had to start over.

While such denials of service are irritating, they are seldom catastrophic. This is not the case when the machine is stolen from the financial or sales director's car, or left in a bar. Some of the damage is reduced if the notebook has an encrypted hard drive. But if it's not, the data is available to whoever buys the unit on eBay.

Disposal policy

This makes a proper policy for disposing of computers and storage media essential. A reformatted hard drive often still holds all the data for anyone who can unformat the disk. Every so often there is a story about bank or medical records turning up where they should not[9,10] , so be sure to overwrite the whole disk with random data before disposing of it. There are free tools out there to help, and it is really simple to do.

Another thing to consider is how data enters and leaves the office network. If people take their notebooks home, and send and receive work-related data via a public network, how does that affect your security model?

Even if companies do not provide notebooks, they still face problems. Will staff copy or e-mail files to their home computers to work on them during the weekend? That machine may be the same one where the kids have shared their whole drive with a file-sharing network to get faster transfers.

Conclusions

Data protection does not end with virus protection and setting up a firewall to block sensitive ports. Data protection is an issue for all aspects of a corporation. It is not only a technical, but even primarily a social and behavioural problem. Your computer security solution must be balance how, when and where your users use their computers to work with their data, and even what they do in their spare time.

The data you set out to protect faces threats not only from the viruses in the file-server, but also from notebooks thieves, users' children and spouses, and even electronic-greeting cards. Network security in a networked society requires eternal vigilance, even in a summer breeze.

References

[1] Serres, Michel (1982). The Parasite, The Johns Hopkins University Press Earthlink (2004-04-15).

[2] EARTHLINK AND WEBROOT TRACK THE GROWTH OF [2]SPYWARE, Available: http://www.earthlink.net/about/press/pr_spyAudit/

[3] SSPPYY.com (2004-06-13). SSPPYY - #1 Selling Spy Software, Available: http://www.ssppyy.com

[4] Symantec (2004-06-14). Symantec Security Response - Spyware.Ssppyy, Available: http://securityresponse.symantec.com/avcenter/venc/data/spyware.ssppyy.html

[5] More, Paxon, Savage, Shannon, Staniford & Weaver (2003). The Spread of the Sapphire/Slammer Worm. Available: http://www.caida.org/outreach/papers/2003/sapphire/

[6] Good, Nathaniel S. & Krekelberg Aaron (2003). Kazaa Usability Study, Available: http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf

[7] Lavasoft (2004-06-14). Homepage, Available: http://www.lavasoftusa.com

[8] Sandvine Inc (2004-06-02). Spam Trojans a growing problem for ISPs, Available: http://www.sandvine.com/news/pr_detail.asp?ID=50

[9] Garfinkel, S. & Shelat, A. (2003), Rememberance of Data Passed: A Study of Disk Sanitization Practices, IEEE Security and Privacy, January/Feburary issue 2003

[10] Hamilton, Tyler (2003-09-15). 'Error' sends bank files to eBay, Available: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Typ e1&c=Article&cid=1063577414565&call_pageid=968332188492&col=968793972154