JK Technologies
Wayne Hedrick
757-291-5545
wayne@jktechnologies.com

Spyware

The Major Computer Problem in 2005

Spyware is a generic term for a collection of evil and misleading programs that get on computers from the Internet. It includes spyware (that tracks your activities with the computer), malware (that causes computers to crash), adware, (that causes pop up ads), browser hijackers (that redirect your Internet searches) and Trojans (software that come in pretending to do some nice thing for you, but it also does hidden tasks such as create Zombie PCs to infect other PCs, use your email system, use your address book, etc…)

Spyware is the major problem with computers in 2005. It is currently a much bigger problem than viruses. Every PC that we've looked at since early 2003 has had at least some of this stuff on it… It causes computers to crash, uses network bandwidth and kills network security. It can email off your credit card information, and any other personal or business information.

It's happened to me…a credit card had fraudulent charges from Spain, apparently via spyware. I've even seen it on the cell phone WAP system. (I browsed for "Reset Jaguar Password" and got results for "PORNO.") CNN reports today Paris Hilton's cell phone had data stolen.

It's also very expensive to repair. We've spent over 30 hours working on one badly infected PC that could not be reformatted. This week, I spent 16 hours on another single business computer with a massive infection. It had to be fixed because the company email was permanently broken, completely due to spyware.

It's also becoming a major problem that JK Technologies is billing for. Most of our time is spent cleaning spyware off of computers. We're not alone. I've attached an article from ZDNET: It's really worth the reading.

JK Technologies Solution
Be Proactive!

I think we can prevent 95% of these problems. And, I think I can save our customers money. Therefore, JK Tech is considering offering a monthly clean up service that will include

1. Spyware/virus cleaning and repair
2. General PC and server maintenance
3. Hard drive and file structure maintenance.
4. Patch installation from Microsoft (these are released weekly to monthly)
5. Operating Service Pack installation from Microsoft
6. After-hours maintenance to prevent loss of productivity.
7. All labor is included for spyware (and related program cleanup.
8. Software licenses are not included however there are many free utilities, or nearly free utilities that are excellent
9. Guaranteed protection. We can't guarantee perfectly clean computers, but I can guarantee that you will receive no additional charges for spyware or viral infections labor with this monthly agreement.
10. Removal of all suspicious programs.

JK Technologies
Wayne Hedrick
757-291-5545
wayne@jktechnologies.com

Such an agreement would not cover:

1. Hardware replacement and upgrades
2. New network additions
3. New hardware or software installations
4. Failed hardware diagnosis and repair
5. Emergency hardware repairs
6. Network hardware maintenance (routers, wires, wireless devices, etc.)
7. Anything other than PC maintenance (hard disk maintenance, file system maintenance, driver maintenance, patch maintenance, and the prevention, removal and repair of spyware, malware, Trojans, viruses, etc.)

As always, we will be fair and logical in our billing practices.

Here are the specifics of the idea. JK Tech would charge a monthly fee based on the number of PCs and servers. The estimated monthly costs are:

Networks with a server:
$99 per server
$19-$49 per PC, depending on the number of computers and the company's history of the spyware problems.

Frequently, peer-to-peer networks have bigger problems because there isn't a server protecting rights to the network.

Peer-to-peer Networks
$39-$69 per PC, depending on the number of computers and the company's history of the spyware problems.

This kind of monthly service should cover the majority of your Technology bills, unless you're upgrading. Your PCs will be up to date and they'll be as protected and maintained as we can make them. Because of the agreement, you will never get an additional bill for spyware or viruses. Your costs will be more predictable in that you won't go for three months without a bill, and then get a huge bill to clean up the PC.

By constantly patching your PCs, and updating antivirus and adapting anti-spyware protection, you should also rarely get the infections. Finally, if your computers become infected, we'll come clean 'em for free. Your technology will be as stable as possible, given the nature of the Internet.

I have to tell you is that Spyware is getting harder and harder to get off of systems. It's taking more time, because the people who write these programs (in Russia, in India, in the Philippines) are getting better at hiding what they're doing…. I spent 16 hours cleaning a business machine on a VPN this weekend…

Such a service would save you money by stopping these serious problems before they grow, and allows the business owner to budget for the necessary network maintenance and protection.

It's simply cheaper to be proactive instead of reactive. It is a major loss in productivity for our clients when the PCs become totally useless.

Unfortunately, there is no simpler solution. Everybody will get spyware this year. The logical question to ask is, "What can I buy to prevent this problem?" There is no single utility that catches everything…. Norton AV 2005 will do a fair job of cleaning viruses before they start an

outbreak, but no single product will provide similar protection against spyware. The worst spyware programs must be backwards engineered and removed manually.

Let me know if you're interested in this type of maintenance and prevention contract. Think of it as the equivalent of oil changes in your car. Technology must be maintained, and in 2005, proactive maintenance is the best approach.

I think this is a logical solution that will give you better technical support and more predictability for your IT support costs.

I'll be glad to come by and talk to you in person.

Wayne
Wayne Hedrick
JK Technologies
291-5545

Important Quotes from the Article:

"It can take anywhere from two hours to all day to fix these. With a limited staff, this can really tie up resources."

At Marist College in Poughkeepsie, NY, the IT department devotes upwards of 90 percent of its resources to combating spyware and issues related to it, according to Analyst Dave Hughes in the school's ResNet department. "ResNet as a whole has spent thousands of hours running spyware scans and other removal tools," he said.

"Spyware on a PC can be just as dangerous as having a virus.

And the kicker: 67 percent of the IT professionals in WatchGuard's survey cited spyware as the greatest security threat to their networks in 2005.

"Much or even most spyware comes from consumers installing 'free' content or software that they shouldn't,"

"Misspell a common domain name and you are likely to land on a domain that will inject spyware into your PC." For users today, he said, "It is difficult to avoid getting spyware if you surf the Internet at all."

JK Technologies
Wayne Hedrick
757-291-5545
wayne@jktechnologies.com

On the Internet at:
http://news.zdnet.com/2100-1009_22-5541802.html?tag=nl.e540-2

By Rick Broida
URL: http://news.zdnet.com/2100-1009_22-5541802.html

What's the biggest threat to business networks in 2005? Front-line IT managers and security firms increasingly peg spyware as public enemy No. 1.

"We now often scan for spyware before we check for viruses"

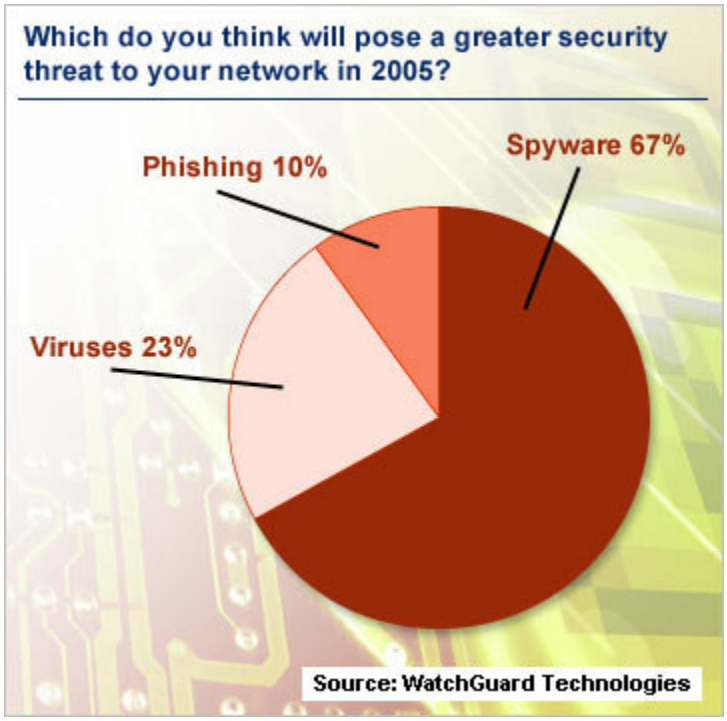
-- Dave Higgins, Saturn Electronics & Engineering

At Saturn Electronics & Engineering, a Detroit-based provider of manufacturing outsourcing services, the problems began last summer. The company's 500 users noticed that Web browsing was sometimes slow. Very slow. IT Manager Dave Higgins suspected virus activity, but manual virus scans turned up nothing. He then scoured the machines with Lavasoft's Ad-Aware and found the culprit: spyware. Once removed, the systems returned to normal operation.

"We now often scan for spyware before we check for viruses," Higgins said. "We are currently seeing Bargain Buddy, GAIN, b3d projector, Gator, n-Case, SaveNow, Search Toolbar, Webhancer, (and) Search Assistant."

Putting spyware first may become standard operating procedure this year. Businesses report spyware incidents rising sharply in recent months, and many IT departments have been on the receiving end of a nasty wake-up call. Typically associated with unprotected home PCs, spyware could soon qualify as the top security headache in the corporate world.

JK Technologies
Wayne Hedrick
757-291-5545
wayne@jktechnologies.com



"An incredible problem"

At Southwire, a producer of building wire and utility cable, at least 70 percent of the company's 2,500 computer users encountered some form of spyware in the last 18 months. That's according to Tim Powers, a senior network administrator at the Carrollton, GA, firm. "Spyware is becoming a larger and larger problem for our desktop support staff," he said.

It's a similar situation at Time Warner Cable in Greensboro, N.C. "We get all kinds of spyware problems," said Sanjeev Shetty, director of information technology services for the 450-user location. "We had one PC that had 1,400 pieces of spyware on it." Shetty estimated that his staff deals with 8-10 spyware-related incidents per week. "It can take anywhere from two hours to all day to fix these. With a limited staff, this can really tie up resources."

Threat

Gridlock looms? ▸
Experts warn that spyware, if left unchecked, will grind business to a halt.

Spyware poses challenges for other kinds of institutions as well. At Marist College in Poughkeepsie, NY, the IT department devotes upwards of 90 percent of its resources to combating spyware and issues related to it, according to Analyst Dave Hughes in the school's ResNet department. "ResNet as a whole has spent thousands of hours running spyware scans and other removal tools," he said.

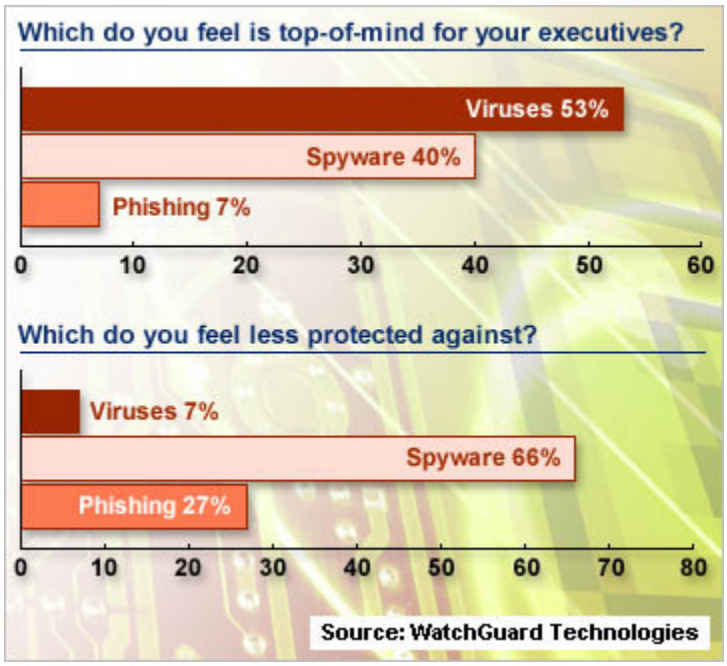
JK Technologies
Wayne Hedrick
757-291-5545
wayne@jktechnologies.com

"It's an incredible problem," added Kathleen LaBarbera, Marist's manager of operations and ResNet. "Spyware on a PC can be just as dangerous as having a virus. Most PC users have heard of spyware, but don't really know what it is or does."

Do you mean adware, malware, Trojans…?

Many analysts and administrators agree that while spyware's impact is rising, its definition remains elusive. The umbrella term most commonly refers to a wide range of unethical software, from difficult-to-uninstall toolbars to home-page hijackers and pop-up window generators. In a new poll of security administrators and IT managers, conducted by security firm WatchGuard Technologies, 50 percent of respondents said the vast majority of users don't know what spyware is.

Two-thirds of respondents said they feel less protected against spyware than against phishing or viruses. And the kicker: 67 percent of the IT professionals in WatchGuard's survey cited spyware as the greatest security threat to their networks in 2005.



The problem has become so serious that Microsoft is working to combat it at the OS level. With 2004's release of Windows XP SP2, the company retrofitted Internet Explorer with a pop-up blocker and gave users a more-robust firewall. In early January, Microsoft unveiled Windows AntiSpyware for Windows 2000, XP, and Server 2003. The software is a rebranded collection of utilities from Giant Software, which Microsoft purchased late last year. The package promises not only spyware detection and removal but also real-time protection. (Many other free utilities must

be run manually.) Currently in beta, Windows AntiSpyware will be free until July, at which time Microsoft is expected to charge for the software and service.

The Firefox solution

What remains to be seen is whether these efforts can keep users from migrating to Mozilla's Firefox. Part of the attraction of the open-source browser is its reputation as being significantly more spyware-proof than Internet Explorer. Corporations have been slower than individuals to change browsers, citing compatibility concerns, but many IT departments are taking a close look at Firefox.

"We have been evaluating Firefox as a more secure browser to help prevent all malware infections," said Higgins of Saturn Electronics. "Currently, it runs about 90 percent of our intranet applications."

"Internet Explorer is an inherently vulnerable browser, partly because it has such a high user base and also due to poor coding by Microsoft," said Hughes. "Here at Marist, we recommend that users use (it) only for Internet Explorer-specific tasks, such as Windows Update, and use Mozilla Firefox for all other browsing."

With spyware attacks now coming from even the most innocuous-seeming software, enterprises may decide to follow suit. Security researchers at Panda Software recently discovered a pair of Trojans -- programs that let outsiders make changes to a user's PC, including loading other spyware -- that leverage DRM (digital rights management) technology built into Windows Media Player. When a user attempts to download a license requested by WMP, the Trojans redirect the browser to a Web site that attacks the user's system with a barrage of spyware.

"Spyware costs money"

Regardless of how a PC gets infected, the results can be serious: compromised company security, overloaded networks, and significant user downtime and inconvenience. Although the symptoms of a system that's overwhelmed with spyware vary, the primary indicators include sluggish performance, broken Internet connections, and possibly even an unusable PC.

"We've seen individual issues ranging from hijacked home pages and pop-ups to aggravatingly slow performance to completely unstable platforms," said Nick Twentyfive, senior network analyst for CTG, an IT and outsourcing solutions company in Buffalo, N.Y. "Back doors installed by spyware can be used by third parties for more serious security breaches. Lost network bandwidth and computer performance reduces productivity. Basically, spyware costs money."

And the problem isn't going away anytime soon. "Spyware's getting harder and harder to remove," he said. "Some of the spyware variants out now have forced anti-spyware companies to make targeted plug-ins to properly deal with them. That's just

JK Technologies
Wayne Hedrick
757-291-5545
wayne@jktechnologies.com

evil."

"Businesses have the talent and budget to create and enforce policies that prevent staffers from installing things themselves."

--Jeff Duntemann, author

Perhaps unsurprisingly, as of mid-January a pair of anti-spyware utilities -- Lavasoft's Ad-Aware SE and PepiMK Software's Spybot Search & Destroy -- ranked as the No. 1 and No. 2 most popular downloads at CNET Download.com. But at least one observer thinks the spyware epidemic is overblown, at least where corporations are concerned.

"Much or even most spyware comes from consumers installing 'free' content or software that they shouldn't," said Jeff Duntemann, author of *Degunking Your Email, Spam, and Viruses*. "At the enterprise level, businesses have the talent and budget to create and enforce policies that prevent staffers from installing things themselves."

Southwire's Tim Powers disagrees: "Misspell a common domain name and you are likely to land on a domain that will inject spyware into your PC." For users today, he said, "It is difficult to avoid getting spyware if you surf the Internet at all."