



828 West Taft Avenue
 Orange, CA 92865
 714-282-6111
 714-282-6117 Fax
www.8e6.com

An Inside Job: Extending Enterprise Protection to Remote Laptops

By The Forsite Group

Introduction

Most of the malware that contaminates corporate laptops is virtually invisible to standard security gear.

The most serious threats to enterprise security aren't those that exploit unknown vulnerabilities or unguarded back doors. These days, IT managers face a far greater threat from telecommuters and business travelers—virtually any employee who takes a laptop home at night or on the road.

To be clear, it's not the employees themselves who are the problem. What's happening is that teleworkers are unintentionally and unknowingly infecting their laptops with spyware, trojans, worms, and other malicious code. Then they turn around and plug those laptops into the enterprise when they're back in the office.

Worse, even if telecommuters realized what was happening, there's little they could do to rectify the situation. The malware they're encountering is designed to masquerade as "real" links and Web advertising. It lurks on blogs. It may go undetected on legitimate sites. Something as simple as moving from one wireless network to another can cause an infection.

Here's where the bad news gets particularly grim: Most of the malware that contaminates corporate laptops is virtually invisible to standard security gear, such as firewalls, intrusion detection/protection systems (IDS/IPS), and security information managers (SIMs). Hackers know this, and they put that knowledge to "good" use. Most don't have the skills needed to break into a well-defended enterprise. But spyware, which is readily available online and relatively simple to assemble using menu-driven tools, will do the job for them.

The Coming Plague?

Where Americans work when not in the office (in millions):

- Home- 45*
- Client/Customer site- 24*
- Car- 21*
- Plane/Train- 8*

ITAC

Equally troubling, these types of attacks could rapidly become a plague, as laptops continue to replace desktops on enterprise networks and telecommuting and wireless become business as usual.

Both trends are accelerating rapidly. A 2005 survey of 134.5 million American workers, conducted by ITAC (International Telework Associations & Council) asked respondents where they worked during the past month. Answers included home (45 million), client/customer site (24 million), car (21 million), and train or plane (8 million). How many of those millions knew if they were using a safe wireless net or if their airlink was downloading dirty code onto their laptops?

That's a particularly pressing question, given the enterprise shift from desktop to laptops. According to an IDC study quoted in *ComputerWorld*, an average of one in three business PC users worked on a laptop in 2005, up from one in five

in 1999. IDC expects that average to reach one in two within the next few years.

BusinessWeek reports that approximately 15 percent of the U.S. workforce is currently “distributed” (maintains no permanent office at their companies), according to Work Design Collaborative, with 40 percent distribution expected by 2012. Some companies are well ahead of the curve: At IBM, 40 percent of the employees already qualify as distributed.

Contamination and Cleanup

An average of 1 in 3 business PC users worked on a laptop in 2005.

IDC

With so many “no-collar” workers on staff, it’s not surprising that IBM has firsthand experience with some of the more troubling aspects of teleworking. An example of this occurred a few years ago when one of the subrings at its East Fishkill (NY) facility was infected with a particularly nasty virus after telecommuters plugged their contaminated laptops into the LAN.

The IT department detected the virus and traced it back to a particular LAN port, which it shut down. Unfortunately, the department didn’t tell anyone in the affected workgroups what it was doing; when the port went out of service, employees plugged into another one, infecting another subring. Ultimately, IBM brought down both portions of the LAN, manually ran a patch on every attached laptop and desktop, and then brought the LAN up again port-by-port. This cautious approach paid off, since IT discovered several machines that were still infected and could patch them before the entire LAN was contaminated. All told, it took more than a day to completely eliminate the virus. (IBM declined to comment on the incident.)

Fighting the Good Fight: Again

IT systems were hit with 50% more viruses in 2004 than the year before.

Recovery costs averaged \$130,000.

Information Week

What can enterprise IT managers do to protect their companies? They need to understand the severity of the situation, what’s driving it, and why it’s only going to get worse. Then they need to familiarize themselves with tools that can help get things under control. These include laptop-based firewalls and antivirus/antispyware software, as well as a filtering technology that uses intelligent agents to extend centralized Web-monitoring and filtering to teleworkers.

Some IT professionals seem to be reluctant to acknowledge this latest threat. If that’s so, the reason may simply be battle fatigue. *InformationWeek* reports that IT systems were hit with 50 percent more viruses in 2004 than the year before, with recovery costs averaging \$130,000, according to a survey of 300 companies and government agencies.

Some of IT’s hesitation to confront these new problems may be due to corporate culture. End-users tend to consider laptops a perk of their jobs. They’re business tools when employees are working and personal platforms when they’re not. Limiting freedoms that end-users have come to expect is not going to be easy—or pleasant.

New Threats For a New Century

The threat of spyware, worms and viruses transmitted via IM and P2P has risen 3,295% in the 3rd quarter of 2005, compared with the same period of last year.

CNET

One thing is clear: IT managers are facing security threats unlike any they've dealt with before. Spyware, worms and viruses transmitted via Instant Messenger and peer-to-peer networks (such as those used to share bootlegged movies and music) are a perfect case in point. Conventional security products were not designed to detect these attacks. That's a dangerous oversight, since CNET notes that these threats rose an astonishing 3,295 percent in the third quarter of 2005, compared with the same period last year.

It's not just the way malicious code is delivered that's changed. The primary purpose of many viruses and worms, like Melissa and SoBig, is to hijack e-mail packages and generate enough messages to clog Internet connections and force companies to shut down corporate mail servers—a denial of service (DoS) attack on a global scale. The Love Bug virus added an ugly wrinkle: the ability to destroy data.

Spyware, in contrast, wants to keep its hosts up and running so it can secretly scan systems, monitor activity, and relay information to confederates somewhere in cyberspace. Spyware ransacks its host and attached systems, searching for corporate and personal data, including account numbers, log-in sequences, and passwords; credit card numbers; and browsing and buying patterns—all of which can be sold (often several times over) to the highest bidders.

Some spyware isn't content just to raid corporate data; it also corrupts it. What's more, malware can significantly degrade laptop and network performance, reduce employee productivity, and rack up sizable administrative expenses.

Compounding spyware's inherent threat is the fact that it's been able to infiltrate end-user computers so extensively in such a relatively short time. In 2004, *Network Magazine* estimated that some 90 percent of all Internet-connected systems were already hosting as many as 30 spyware programs. Global ISP Earthlink corroborated those findings: It ran approximately 4.6 million scans using its Spy Audit program, discovering 116.5 million instances of potential spyware (25 programs per PC). (To learn more about spyware, download 8e6 Technologies' white paper, "Neutralizing the Spyware Threat." Source URL: http://www.8e6.com/spyware_wtp_form.htm)

Spyware's near-perfect penetration helps explain an equally disturbing statistic. Between February 2005 and January 2006, according to the Privacy Rights Clearinghouse, more than 52 million Americans had "secure" personal data compromised—data that includes names, addresses, and social security and driver's license numbers. Of that total, only 7.4 million breaches are due to loss or theft of laptops and tape and disk media. The remainder is the result of "hacking." (These numbers are so readily available due to California's Notice of Security Breach law, which requires all data losses, regardless of where they occur, to be reported.)

Spyware? Everywhere

Given the prevalence of spyware on corporate laptops, there's a natural tendency to think that telecommuters must be doing something "wrong," such as visiting adult sites, participating in online gaming, or sharing bootlegged music. This is a variation on the bored-salesperson-in-the-hotel-room syndrome, which suggests that any employee with a laptop and too much time on his or her hands is almost certain to get into some sort of trouble.

Explanations like this are akin to Internet urban legends; they contain some element of truth, no matter how miniscule. But even if every bored business traveler in the United States were to live up to this stereotype, it still wouldn't account for spyware being present on 90 percent of business laptops.

Some employees catch a bad case of spyware by doing something innocuous, like clicking on a link in an IM message that appears to have been sent by a friend. Others do nothing more devious than visit what they think are legitimate sites. Internetnews.com reveals that Weightwatchers.com was hit with adware that delivered banners for rival DietWatch.com—and loaded laptops with a variety of spyware. Weight Watchers successfully sued the malware manufacturer, but corporate IT was left to clean up the company's laptops. Blogs, which are often run by individuals who are short on time, technology expertise, and funding, tend to be loaded with malware.

As mentioned, communicating via wireless networks can qualify as at-risk behavior. Not all wireless nets are equally well policed by security experts, which makes it far easier for hackers to hide malicious code on network servers. Hackers also have been known to deploy dummy wireless infrastructure for the express purpose of downloading malware onto unsuspecting users' laptops.

The Day the Music Died

And sometimes teleworkers wind up with compromised machines because they've been tricked into doing what appears to be the right thing. The Sony BMG spyware scandal, which is discussed in detail on Law.com, is a casebook example of this type of activity.

Sony BMG is the world's second largest music company, accounting for approximately 25 percent of all U.S. album sales. In 2005 it added copy-protection software to some of its CDs; this program had to be installed before customers could play or duplicate Sony BMG music on Windows computers.

Late in 2005 several security experts revealed that the third-party copy protection technology Sony BMG was using automatically installed a "rootkit" on customer computers—a piece of code that's typically used to hide viruses and spyware from the machine's operating system, as well as from antivirus and antispyware programs. There was a good reason for resorting to a rootkit. The copy-protection scheme *is* spyware. It collects and transmits information about customer listening habits over the Internet to Sony BMG servers, despite assurances from the company that "no information is ever collected about you or your computer without your consent."

Once word got out, hackers lost no time exploiting the rootkit's ability to render code invisible, developing and releasing viruses that could exploit it. At that point leading makers of antispyware and antivirus tools, including Microsoft, Symantec, and Computer Associates, labeled the Sony BMG copy protection software a security threat, a sentiment echoed by the U.S. Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security.

Sony BMG released a patch that removed its software, rootkit and all. That didn't prevent it being named as defendant in more than 10 class action lawsuits in state and federal courts. Other states are still deciding whether or not to take legal action.

Hackers Hitch A Ride

Network firewalls, antivirus software, and IDSs expect threats to come from the outside. Why should employee laptops present a problem?

Many of today's cybercriminals are professionals, which is why they target laptops. As noted, it's infinitely more difficult to crack the security defenses at a major corporation than it is to dump malware onto an end-users' laptop. In the new world of cybercrime, where information has become a very valuable commodity, why would hackers waste time trying to get around sophisticated security systems that have been set up to keep intruders out when they can sail right past those defenses tucked into corporate laptop?

That scenario begins to explain why conventional security products offer little or no defense against spyware and similar code. Simply put, they were never intended to. Network firewalls, antivirus software, and IDSs expect threats to come from the outside; they protect the enterprise from hazards associated with incoming traffic. Employee laptops are already inside the perimeter, so they shouldn't present a problem. Spyware, in fact, is useless if it can't stream information back out through corporate defenses.

This doesn't mean that IT managers have no way of protecting their companies from spyware and similar threats. To do so, however, they must start concentrating on the real danger: laptops themselves.

Some organizations configure corporate laptops so the only way they can reach the Internet is via a VPN (virtual private network) routed through the enterprise. Essentially, the browser itself is configured so that all URL requests are tunneled back to the enterprise and handed off to switches and routers, which pass the requests onto the Net—as long as they comply with acceptable-use policies. Responses must pass through firewalls and other security mechanisms that screen and monitor incoming packets.

The two main advantages to this approach are that it institutes ironclad control of how teleworkers use their laptops, while taking advantage of existing network security. The chief disadvantage is that it's very bandwidth and resource intensive. Every Internet connection established from anywhere outside the company must be tunneled twice: once for the request and once for the reply. In addition, implementing this sort of scheme can quickly become a full-time job for the IT department.

Living La Vida Laptop

Antivirus software typically offers no protection against zero-day exploits, and it only takes one infected laptop to contaminate the entire enterprise.

There are other, less restrictive, ways to reduce the risk of contamination using products specifically developed for laptops and desktops.

One such device is a packet-filtering firewall. Telecommuters connecting to the Internet via broadband connections from home, hotel rooms, or airport wireless hotspots are continually being pinged and scanned by human hackers and automated scripts, looking to find an unprotected port. A packet-filtering firewall knows both what constitutes legal traffic and which ports it can use. It identifies illegal traffic, just as an enterprise firewall would, and dumps it.

If a laptop has been contaminated, firewalls with outbound traffic controls can help prevent them from being transformed into launching pads for DoS attacks. If the firewall detects unusually heavy outbound traffic on one or more com ports, it shuts those ports down and issues an alert to the user.

Antispyware packages are important to overall network security, but do not provide complete laptop protection.

Antivirus software is a must. The key here is making sure antivirus signatures are absolutely current. Given the speed at which new viruses are developed, simply keeping every laptop up to date can quickly turn into an administrative nightmare. Further, antivirus packages typically offer no protection against zero-day exploits, and it only takes one infected laptop to contaminate the entire enterprise.

A number of vendors now offer antispyware packages, which also should be standard issue on telecommuters' laptops. Typically, these programs regularly scan a system, searching for spyware, adware, and the like. If any is found, the software alerts the user, attempts to remove the malicious code, and indicates if it's been successful or not. Some products can be configured to alert IT personnel as well, so infected laptops can be intercepted before they can be plugged into the corporate network.

Antispyware packages suffer from several shortcomings. For one thing, they are still fairly rudimentary, so they may give users and IT personnel a false sense of security. For another, new spyware, like its viral counterpart, is being churned out daily. So antispyware software must be updated constantly. Usually, the program can be configured to do this automatically.

The complex nature of spyware is another limitation. It typically alters dozens of files and laptop settings, so detecting and removing it is just the beginning. Corporate IT still has to reconfigure the infected machine. Similarly, spyware tends to act more like a cluster bomb than a guided missile: It downloads a bundle of malware apps onto contaminated machines, sometimes 10 or more. Detecting and eliminating all of these may simply be too processor-intensive for a desktop program.

Despite these limitations, antispyware software should still be part of any laptop protection scheme. What's more, as vendors crank out more powerful solutions, many of these issues will be resolved.

Web Filtering and Monitoring for Laptops

A new class of products uses intelligent software agents to extend the performance and capabilities of enterprise-class Web filtering and monitoring appliances to remote laptops.

Whatever their strengths and weaknesses, there are several inherent shortcomings shared by the foregoing products. Since they're all point solutions, they can't be integrated into a seamless, integrated security shield. As noted, they're also processor-bound: At some point a laptop may be forced to compromise on both performance and protection, the worst of both worlds.

The most serious drawback, however, is that many of these solutions are reactive rather than proactive. They may be very effective at repairing damage once it's been done, but they can't prevent that damage from occurring in the first place.

That's exactly the purpose of a new class of products that uses intelligent software agents to extend the performance and capabilities of enterprise-class Web filtering and monitoring appliances to remote laptops.

These agents perform several complex tasks in real time to ensure that enterprise protection is seamless. To begin with, they monitor all Internet activity on the laptop, informing the central appliance if they spot a packet headed for a known spyware source. The appliance sends a block page to the laptop, which prevents it from trying to access the site. It also transmits a TCP reset to the site, canceling the session. Since all this happens in milliseconds, there's no chance that sensitive data can be shipped to the spyware site or that malware can be downloaded to the laptop. This approach also guarantees that every laptop is automatically safeguarded as soon as a new source of malicious code is identified, without administrative intervention or overhead.

The same process ensures that every laptop conforms to a company's acceptable-use policies, which prevents teleworkers from visiting potentially problematic sites while protecting the company itself against potential liabilities and lawsuits. Here again, the intelligent agents automatically implement any changes to a company's policies, so laptops are in sync with all other devices on the enterprise.

The best Web-filtering and monitoring appliances also address the risks inherent in IM and P2P communications, identifying IM packets transmitted to unknown servers, private servers, and proxy servers. This screens out IM-borne malware and prevents laptops from performing an end-run around blocking. In much the same way, these appliances—and by extension, their agents—identify P2P traffic to prevent log-ins and file transfers to an array of services such as KaZaA and Gnutella.

The reporting capabilities of Web filtering and monitoring appliances also are critical. If companies can compile detailed records of URLs visited, user names, and IP blocks, it's armed with the information it needs to reduce risky behavior among teleworkers and the risk of infection overall.

It's important to understand that the Web-filtering and monitoring appliance does the brunt of the work here. The intelligent agents simply keep it informed as to laptop activity, so protection doesn't exact a performance penalty. Equally important, this solution is completely proactive. It prevents laptops from getting into trouble rather than trying to address problems after they've occurred.

Putting Ideas Into Action

The 8e6 Remote Client ensures the same world-class filtering that safeguards users inside the corporate firewall protects telecommuters.

One example of this emerging class of products is the new Remote Client for 8e6's R3000 Internet Appliance. The client ensures that the same world-class filtering that safeguards users inside the corporate firewall protects telecommuters. This includes filtering and blocking based on URLs, IP addresses, HTTP (hypertext transfer protocol), FTP (file transfer protocol), newsgroups, search engines, and anonymous remailers—as well as IM and P2P protocols.

The 8e6 Remote Client is centrally managed from the R3000, a dedicated, standalone appliance that readily scales to accommodate enterprise growth. The client continually logs URLs that remote employees visit. It's completely transparent to end-users and can only be configured by authorized personnel.

In addition, the Remote Client can be linked to 8e6's dedicated reporting appliance, the Enterprise Reporter 3.0. This scalable, standalone device preprocesses, indexes, and presents information gathered by the Remote Client in a virtually limitless variety of custom, cross-referenced formats. These include by time (daily, weekly, monthly, and yearly), by user, by category, and by individual URLs and IP addresses. Drill-down menus make it easy for IT managers to mine valuable data, while the Enterprise Reporter's intuitive, point-and-click GUI takes the effort out of configuration and report generation.

The Remote Client automatically detects if it's plugged into the enterprise or operating remotely. This capability ensures a seamless transition from local to remote mode, without requiring IT administrators to spend time reconfiguring end-user laptops.

Summary

Wireless networks, laptops, and telecommuting are transforming the enterprise, and raising new security issues in the process. Hackers, as usual, are ahead of the curve, writing malicious code designed to exploit security soft spots and target laptops and wireless communications. Despite some high-profile hacks and attacks, cybercriminals' advantages should be short lived—if IT managers recognize the new rules of enterprise networking and take advantage of emerging products specifically developed to protect laptops—such as 8e6's Remote Client. Part of this process also involves educating telecommuters about work habits that could conceivably jeopardize the entire enterprise. Until this is done, and effective security mechanisms are put in place, teleworkers truly represent a serious—though unintentional—threat to enterprise stability and safety.



For more information on 8e6 Technologies and 8e6 appliance-based solutions for Internet Filtering, Web-use Reporting, and Spam Control, visit www.8e6.com.