



## **Aurora Enterprises: Solutions for Malware Attacks**

This paper discusses the new and dangerous threat to computers posed by today's sophisticated malware, and how the Aurora portfolio of security solutions can help prevent malware attacks.

### **Executive Summary**

Malware, or "malicious software," has been an ongoing concern in the IT community. The most common types of malware are:

- Viruses
- Worms
- Trojan Horses
- Spyware

As computer usage increased since the 1980s, and the Internet has become more interactive, the variety and gravity of malware attacks have also escalated to the point that countermeasures are essential to maintain a safe online experience. Companies can no longer approach security as an afterthought. Given the extent of the existing threats, the security of technology and communication must be a primary design consideration.

The best defense against malware is a combination of common sense safety measures, preventative maintenance, taking time to stay current with new anti-virus technology, and security solutions from Aurora Enterprises. Aurora's experience guarantees the most efficient and effective methods to protect IT systems.

### **Overview**

Though the term "malware" had yet to be invented, the usage of malicious software dates back to the 1970s. But it was in the 1980s, when personal computers began their progression into becoming essential tools in the home and office, that the industry first realized the extent of the threat.

As computers became more sophisticated, so did the viruses unleashed to harm them. Many of the first malware attacks were created simply to damage or destroy, but now virus writers, motivated by personal gain, are attempting to steal bank account details and passwords.

Security concerns are eroding public confidence in IT systems. All private and public companies, as well as federal, state and local government entities are vulnerable to a variety of malware issues. As the fallout from an attack can be catastrophic, companies must address these concerns and put safeguards in place to protect their clients.

The evolution of Web 2.0 adoption has created new security concerns that cannot be addressed by 1.0 solutions. Reputation and intent-based techniques have emerged as the most effective, reliable and affordable solutions available.

Aurora Enterprises is a leading California-based IT Solution Provider specializing in data security solutions. The company's expertise in messaging security and encryption has earned Aurora an excellent reputation amongst security vendors and corporate clients. Aurora can work with your staff to create a security implementation program that covers every aspect of your IT operation.

### **What is Malware?**

The term "malware" takes its origin from the phrase "malicious software," and can be used to describe a variety of software parasites, including viruses, worms and Trojans, that can interfere with computer usage, violate online privacy and steal confidential data.

As computer usage and online communication has grown over the past two decades, to the point now where it's difficult to find a home or business without email or an Internet connection, malware attacks have dramatically increased as well. Thousands of computer users are at risk every day.

Technology is now in the midst of an escalating arms race of ever-more sophisticated attacks, countered by evolving state-of-the-art protection. Both sides have claimed their share of victories over the years – firewalls are created only to be breached, malware databases are designed, then rendered obsolete by polymorphic parasites that cannot be easily defined and classified.

Sadly, whether it's a threat targeted toward a specific company or an email virus created merely to cause mischief by someone with too much time on their hands, malicious software has become a big business. An understanding of existing threats, and the methods available for securing online data and communication, is vital for safe computing. Through foresight, vigilance and preventative maintenance, it is possible to safeguard an IT network. The best and most economical time to do so is before a problem occurs.

### **Know Your Enemy**

Malware: Short for malicious software, this is a blanket term for any type of software created specifically to cause damage to a computer, a server or an IT network. The most common types of malware are viruses, worms, Trojans and spyware.

Virus: Just like a cold virus can be passed from person to person, extending the breadth of its damage, a computer virus is a program or script that spreads from one file to another without the knowledge of the computer user. Most viruses are spread through email attachments.

Worm: A worm is a specific type of virus that propagates itself across many computers, usually by creating copies of itself in each computer's memory.

Trojan Horse: While a Trojan Horse is really just another virus, it deserves separate classification because of the way it presents itself. The Trojan Horse (of history or legend, depending on one's source) was a statue delivered to the city of Troy as a gift. The Trojans accepted the gift and wheeled the horse into their city, but it was filled with Greek infiltrators who slipped out at night and destroyed the city. Similarly, Trojan Horse malware presents itself in one form – an email from a friend, or a software update from a trusted manufacturer – while concealing its true malicious nature. Trojans can be designed for any malware application, from stealing information to erasing a hard drive.

Cookies: A cookie is a small bit of text in a file on your computer that identifies you to a particular website, and records information about you during your visit. Cookies were designed to create a custom experience for site users and to make their visit more efficient. No other entity outside of the original site should have access to the stored information. Unfortunately, however, some sites use cookies to track a user's Web surfing habits, which can be considered an invasion of privacy.

Spyware: Like cookies, a spyware program tracks a computer user's online habits. It is sometimes packaged in a free program download. Once installed, spyware can download targeted advertisements and overlay them on the websites you visit, or transmit this information to the author of the spyware program. In addition to the obvious privacy invasion, spyware can also debilitate your online experience by slowing down your computer's ability to read email or browse websites. Poorly written spyware may cause even greater damage, and in some cases still create problems even after it has been removed.

### **Web 2.0 = Malware 2.0**

As the Web has evolved over the past decade, what was once a basic information and communication source has been transformed into a colorful, interactive world of sights, sounds and moving images. But the arrival of "Web 2.0" also means the threat of malware 2.0, as all of the new capabilities in Web page design and content have created even more opportunities for those determined to corrupt them.

Security must keep pace with hackers, and solutions are available. However, companies and consumers have been so eager to embrace the benefits of Web 2.0 that they often overlook the importance of updating their online protection. What worked against yesterday's viruses is no match for the current variety of targeted attacks using socially engineered email messages, phishing scams and assaults on Internet applications.

In fact, some malware attacks now utilize the very technology that was created to provide enhanced security. For example, the use of HTTPS over HTTP can no longer be relied upon to ensure a secure financial transaction. And since many security solutions do not apply to encrypted traffic, this new and virtually undetectable malware can achieve its

objective despite URL filtering, signature scanning and other HTTPS barriers that most companies assume are still impenetrable.

### **Alarming statistics**

A study commissioned by Secure Computing found that 73% of companies surveyed experienced a virus attack, 57% discovered spyware in their IT system, and more than 45% had to deal with Trojans and key loggers. And because the attacks are more sophisticated, it often takes longer to expose them – sometimes as long as 300 days or more. That means a hacker might be able to exploit a system vulnerability for almost one year before defensive measures are taken. And these are only the attacks that are publicized – IBM estimates that nearly 140,000 more vulnerabilities are discovered annually, and not reported to the public.

### **Changing Strategies, New Targets**

The email inbox used to be front line of a malware attack. Today, the threat is more likely to be application-based. According to Gartner, “The Internet, and Internet applications, will be the primary source of malware infections in enterprise in 2008 and beyond. Malware filtering in the Web gateway will increase from 10-15% penetration in 2006 to 70% by 2011.”

Many applications do not inspect data returned from a visit to an Internet Web site, a vulnerability that hackers have exploited by appending malicious code to Web pages. In 2006, malware writers used a Wikipedia article to lead users into a linked booby-trapped page that planted viruses on the computers of unsuspecting users. In 2008, a loophole in Google's website sent users to malicious websites and executables. Spammers used HTML-formatted email with a link that apparently points to a Google page, but instead directs users to a site that tries to install malware.

### **Stormy Weather**

Perhaps that most severe example of a Web-borne malware attack was the Storm worm, introduced in January of 2007, which generated more than 9 million emails, each attempting to direct recipients to Web sites with malicious code. It is the first worm to fully exploit the convergence of Web and messaging communication spectrums in the malware space.

Its name is a reference to the subject line of the first carrier emails, “230 dead as storm batters Europe.” But what made Storm unique is its ability to morph into other messages based on other topical references that made the messages seem authentic. After a brief hiatus, attacks resumed in September of 2007, beginning with Labor Day greeting messages, followed by fake YouTube warnings, holiday ecards, and attacks on the Google blogging community.

A systemic, self-mutating infection that can clone itself anytime, anywhere, without requiring a central server, Storm took global malware propagation to the next level.

## **Malware Protection: The Basics**

Common sense can solve many problems, including those caused by malware, before they can cause any damage.

1. Evaluate your security settings. Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk.
2. Check routers and firewalls. The best line of defense against viruses and other potential disasters that arrive through email are routers that offer additional security functions, and firewalls configured with an appropriate rule set to stop attacks from reaching your company's web server. If you are running Windows XP you can use the built-in software firewall under Control Panel, and there are free versions of firewalls that work on all versions of Windows.
3. Stay current with new technology. A virus scanner recognizes and protects your computer against most known viruses and Trojan Horses, and evaluates programs to determine if it contains any virus-related characteristics. However, attackers are continually writing new viruses, so it is important to keep your anti-virus software up to date. Keep your computer's software patched and current.
4. If a computer program is attached to your e-mail and you are unsure of the source, delete it immediately. Do not download applications or executable files from unknown sources, and use caution when trading files with other users. Since many viruses are sent in the guise of a reputable source, confirm the identity of the recipient before taking action.
5. Use caution before installing a new program. Is this something you really need, or are there any risks that may outweigh the benefits? Examine any fine print that may reveal the presence of spyware. Anti-spyware programs can prevent some spyware from being installed, but once again the best strategy is to discriminate in what you choose to download and/or install.

## **Advanced Malware Solutions**

The first step to creating a strategy to combat the malware threats to Web 2.0 is to improve user awareness and training on these threats. This should be followed by a re-examination of the company's current security policies and protection capabilities. If there are vulnerabilities, they can be addressed with next-generation proactive protection that provides enterprise-level performance, scalability and manageability support.

New technology investment may be required, but it is vital to invest in solutions that will actually achieve the desired result. The following guidelines offer recommendations on products that achieve best-practice results.

1. Use real-time reputation-based URL and message filtering for all domains. Reputation-based defenses complement traditional URL filtering and can substantially improve risk-mitigation by blocking user access to servers with a questionable reputation. It is not uncommon for 10,000 malicious Web sites to be identified every day. Choose a system that provides both Web and messaging reputation, to catch any potential email-borne threats

2. Deploy anti-malware protection using real-time, local “Internet-based” analysis of code to protect against unknown threats, as well as signature-based, anti-malware protection for known threats. The best protection systems not only detect and neutralize attacks, but also automatically notify a global reputation system when malware is discovered, so other companies will also be protected.

3. Implement bi-directional filtering and application control at the gateway for all Web traffic. Both encrypted and unencrypted protocols must be controlled in both directions, to watch for malware entering the system or data leaking out. With HTTPS no longer a guarantee of safety, filtering at the gateway can provide additional security while respecting the privacy of the transaction.

4. Provide data leakage protection on all key Web and messaging protocols. As with the previous step, both encrypted and unencrypted protocols must be controlled as HTTPS no longer guarantees security.

5. Ensure that all caches and proxies are secure. All cached objects should be filtered each time prior to delivery, to prevent the risk of delivering malicious code to the user.

6. Design a security infrastructure for layering of defenses with a minimal number of security devices. The goal is to manage both inbound and outbound risk, and to increase security by making certain that the devices implemented are working in conjunction with each other to improve results. A single solution approach not only improves performance and efficiency, it can reduce costs as well.

7. Use comprehensive access, management and reporting tools. Choose solutions that employ real-time, “at-a-glance” reporting on email and Web gateways.

### **Security Solutions from Aurora Enterprises**

Aurora Enterprises helps companies establish comprehensive Web 2.0 security for desktops and servers, and 24/7 protection against malware. Aurora provides secure file transfer solutions that deliver enterprise-grade security, reliability and performance.

Aurora’s experience with security solutions guarantees the most efficient and effective methods to protect IT systems. We start with the basics – keeping unwanted spam out of email, and protecting the system against viruses, while making certain that hackers will be denied access to confidential information.

Aurora provides state-of-the-art integrated gateway appliances for both Web and messaging gateway security that protect against malware, data leakage and Internet misuse. Our award-winning anti-malware and outbound compliance engines set the industry standard for comprehensive protection.

When the Storm worm struck, TrustedSource™ technology, available through Aurora, began to track its progress before many companies were aware of its potential for havoc. By designing a simulator program to mirror its behavior from a network perspective, it was possible to create a profile of its progress. Today, this global reputation service accumulates data from thousands of sensors in 72 countries, reviews more than 110 billion messages every month, and can block up to 80% of suspicious connections based on reputation data.

Where is an attempted security breach in your IT system most likely to occur? Different companies have different vulnerabilities. Aurora provides clients with the means to determine the scope and magnitude of the malware threats that confront their IT network, and concentrates our security solutions against these potential violations with particular vigilance. We protect against external attacks and insider vulnerabilities.

### **Conclusion**

Despite the growing threat posted by malware attacks, many businesses still do not consider the active protection of computer systems a necessary ongoing investment. Since prevention is always better – and less expensive – than a cure for a compromised IT system, the time to take action is now.