

Malware Is Banging On Your Network's Door

Malware Threatens Network Security

Malicious software or “malware” is the biggest network security threat facing financial institutions today. Cybercriminals target enterprises that hold a great deal of money or conduct a high volume of transactions on a daily basis. A network intrusion can cost an organization as much as \$5 million. And, the damage to a company's reputation can be irreparable. Statistics show that if a major security breach occurs against a U.S. enterprise, that organization has a 90 percent chance of going out of business within two years. This is particularly alarming considering that malware is currently the fastest-growing trend in the misuse of network resources.

In essence, malware acts like a parasite on a network. It is designed to infiltrate a computer system without permission. Even the most well-intentioned employee may accidentally download malware – such as Zeus (Zbot) – from a Web site or open it via an e-mail attachment. The worm then slips past network security measures and hides against the firewall. Here, it collects data and absorbs private information passing through, such as credit card numbers, account numbers, or social security numbers. The worm then sends that information back to the host, who then sells it to criminals for identity fraud, e-scams, and other personally invasive crimes.

The Threat is Real

This threat of malware is very real. Private information at financial institutions is at risk without the proper network security measures. Unfortunately, a majority of anti-virus programs and network firewalls cannot protect against intrusion risks beyond viruses and Trojan worms. Organizations have to be smarter than the criminals they're up against.

Just as federal regulators have made efforts to protect privacy through statutes such as HIPAA, Gramm-Leach-Bliley, and

PCI DSS, compliance standards in the financial industry are moving toward required advanced network security measures. Massachusetts passed the “Massachusetts Privacy Act” that requires financial firms to have either an Intrusion Detection System (IDS) or Intrusion Prevention Sensors (IPS). With the malware trend growing at an exponential rate, experts anticipate that the remaining 49 states will implement similar legislation within the next two years.

A Firewall is Not Enough

Today's malware is so advanced that a firewall alone will still leave a network vulnerable. A firewall provides a basic line of defense by allowing or blocking connectivity to the network through port connections. Think of a firewall like a house: it allows you to close and lock the doors and windows you don't want outsiders to have access to, while keeping them open for welcome visitors.

The problem with this defense is that the firewall does not investigate the data that

is allowed to enter the doors on the network. If there is danger lurking outside the front door (port connection) and the data finds a way into the home (the network), it will cause an intense amount of damage. And, although it's not practical to check your guests' bags, it is necessary to scan all items entering your network to determine if they are friend or foe because the network's health and safety rely on it.

IDPS is the Answer to Malware

Intrusion Detection and Protection Systems (IDPS) are the newest line of defense in network security and combine two levels of network protection into one: intrusion detection and prevention. These systems identify and prevent malware intrusion by examining information via sensors within the network infrastructure.

An Intrusion Detection System (IDS) monitors activities on the network by searching for malware and producing reports for the system administrator. Intrusion Prevention Sensors (IPS) actively block the malware on the network, dropping the malicious data while still allowing normal data to continue on the network. With IDPS, the solution runs along the MPLS cloud. If the malware is right on the network's doorsteps, the technology is efficient enough to detect and prevent it from entering before the data leaves the cloud.

In a 2009 survey, Forrester Research showed that IDPS is the second most in-demand security solution. Many of the solutions on the market today are either IPS or IDS. PAETEC's IDPS requires no additional equipment purchases, and has the ability to provide powerful and efficient security while also being cost-effective for the customer. PAETEC offers an IDPS solution that outperforms other products in the industry because of its ability to minimize risk and cost for an organization.

IDPS is a substantial part of an enterprise security solution used to protect the network. In order to set up proper network security, layers of products, software, and solutions need to be in place that protect against various threats. Firewalls, anti-virus programs, access controls, and an IDPS solution are all necessary to achieve effective network security.

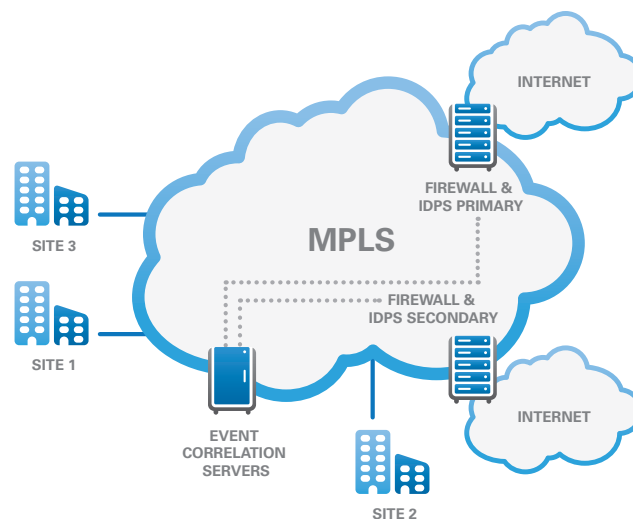
How IDPS Works

An IDPS keeps risks away from important data. It acts like a bouncer standing outside of a bar checking IDs: it detects malware and prevents it from hanging out along the firewall. The IDPS is constantly scanning the network for known threats. These threats are identified in several ways, including through customer-provided data or Web security solutions such as McAfee. It is also continuously searching the network for any possible anomalies.

PAETEC's IDPS sensors provide "zero hour" protection for the customer so an organization is protected as soon as threats are launched. When an anomaly is discovered, both the IDPS customer and

PAETEC's security operations center are alerted. PAETEC engineers contact the customer about the malicious activity, and also help remediate the problem.

Management of an IDPS is just as important as purchasing the solution itself. With current IDS or IPS solutions, IT professionals need to sift through a wall of network data that likely contains a great deal of false positives – information that is classified as malicious, but is, in fact, harmless. PAETEC manages this process for the customer, and has a 99.9999 percent guarantee against false positives, ensuring that the IT professional's time is spent in the most productive way possible.



This diagram shows the network infrastructure and how the IDPS works in conjunction with the firewall, and the MPLS cloud, in order to secure the network.

The ROI of IDPS

The manpower and capital resources required to protect against the threat of malware is significant; however, PAETEC's IDPS provides network protection and a good return on investment for organizations. Since PAETEC's security engineers provide support for the IDPS, the need is eliminated for customers to hire additional IT staff, complete extra levels of certification, or incur capital costs associated with maintaining multiple security devices and information security providers.

In addition, purchasing an IDPS solution is like buying insurance for an organization's reputation. As malware evolves, network security must keep pace. If not, companies will continue to be at risk for damage to their networks and reputations. One network security breach can bring operations to a screeching stop. An IDPS works along with other network security measures in order to prevent this from happening and has proven to be the most effective response in evading malware threats.

Conclusion

The best way to provide adequate security for an organization is to stay informed on threats, analyze vulnerabilities, and work with a partner that can help you build your security solution. IDPS is a crucial layer and PAETEC offers the most advanced solution

to protect your network against data theft. For more information on PAETEC's IDPS solution, or to have PAETEC evaluate the strength of your network firewall, visit www.paetec.com.

Quick Facts:

In the first quarter of 2010, nearly 27 percent of malware attacks occurred in the United States – second only to Brazil. While 98 percent of malware attacks are conducted by nondiscriminating automated systems, 2 percent are sophisticated hackers targeting a specific company network.

Nonetheless, cybercrime acts continue to grow, and remain profitable for the hacker:

- Internet crime in the U.S. increased 23 percent in 2009
- Personal identity sells for \$.40 per person on the black market
- Healthcare data, such as dental records, sells for \$14 per person