

Hospitality Industry

Targeted by Data Thieves

Protect Your System to Avoid the Malware Nightmare

While your guests are sleeping peacefully or enjoying a meal, vulnerabilities in your network may be exposing their payment card data to criminals. In fact, half of all known data compromises in 2008 involved restaurants and hotels based on Visa's findings. Recent data security breaches reported to Visa confirm criminals continue to target hotels and restaurants.

Criminals attack systems that process sensitive payment card data such as security codes, PINs and full track data because of their potential use in committing payment card fraud. While many restaurants and hotels have reduced their risk by eliminating the storage of sensitive card data and using payment software that is compliant with the Payment Application Data Security Standard (PA-DSS), criminals are redoubling efforts to steal card data through the use of memory-parsing malicious software, known as malware.

New Trend Among Data Thieves

With less data being stored, hackers have been forced to adjust their attacks.

Criminals are well aware that merchant payment networks serve as the main vehicle for transmission of cardholder data between systems. The hospitality industry has increasingly embraced the network model in which point-of-sale (POS) systems connect to a central backend server or host. However, along with greater speed, functionality and efficiencies, centralized processing environments, such as property management systems, have also been a key target for security breaches.

Criminals are now focusing on attack methods to intercept cardholder data in transit during the transaction authorization process. An intruder can successfully penetrate the outside perimeter of a merchant's insecure network using commonly known vulnerabilities and, through the use of memory-parsing malware, capture cardholder data as it is being processed. Although there may be no stored data to steal, the insertion of malware allows the hacker to snatch the cardholder information at the POS. The malware then begins to automatically upload batches of stolen data to the criminal. Because

of its viral design, malware may be transmitted along with legitimate data and spread between systems. In addition to capturing cardholder data, intruders are using malware to successfully "sniff" or "log" usernames and passwords of privileged accounts that allow them to take control of critical payment processing environments. Identifying and detecting these types of incidents have proven to be difficult, magnifying the impact of malware incidents.

Mitigating the Threat

As restaurants and hotels remain choice targets for criminals, it is important to take steps to prevent network intrusions that lead to malware nightmares.

The Payment Card Industry Data Security Standard (PCI DSS) prescribes network security guidelines that can help avoid vulnerabilities such as poor firewall rules configuration, lack of network segmentation and management of network devices – all of which can expose sensitive data to non-trusted networks and expose the network and any connected systems to malware, spyware and viruses.

Any networked restaurant or

Recent data security breaches reported to Visa confirm criminals continue to target hotels and restaurants.

Any networked restaurant or hotel should consider implementing the following security practices:

Install and properly maintain a firewall at all times.

Enable firewall logging and maintain firewall logs for one year.

Monitor firewalls and logs for suspicious traffic and activities, particularly outbound traffic to unknown Internet addresses.

Implement strong access controls.

Routinely examine and secure all systems and networks for unknown and unauthorized software and newly added hardware devices.

Ensure that anti-virus, anti-malware and anti-spyware software programs are up to date.

Use outside resources to help identify new security vulnerabilities.

hotel should consider implementing the following security practices:

- Install and properly maintain a firewall at all times. Disabling a firewall can put a business at heightened risk of Internet attacks and potential system compromise.
- Enable firewall logging and maintain firewall logs for one year. These audit trails assist with reconstructing system events, help identify suspicious network activity, and are instrumental in facilitating forensic investigations.
- Monitor firewalls and logs for suspicious traffic and activities, particularly outbound traffic to unknown Internet addresses. A 2008 Verizon Business study of forensic investigations found that of 82 percent of data breaches, evidence, such as audit logs, were available to the organization prior to actual compromise.
- Implement strong access controls. Access controls will help restrict inbound and outbound network access to only traffic necessary for the cardholder data environment.
- Routinely examine and secure all systems and networks for unknown and unauthorized software and newly added hardware devices.
- Ensure that anti-virus, anti-malware and anti-spyware software programs are up to date. Investigations confirm that outdated security software is often found at compromised entities. This fact underscores how critical it is to install security software and new updates immediately.
- Use outside resources to help identify new secu-

rity vulnerabilities. Visa provides a frequently updated data security alert listing malware and IP addresses identified in forensic investigations, publicly available at www.visa.com/cisp.

As criminals continue to target the hospitality industry, efforts to stop them must keep pace. By implementing and maintaining these key security practices, along with all of the PCI DSS requirements, restaurants and hotels

As criminals continue to target the hospitality industry, efforts to stop them must keep pace.

can protect their brands and their customers and reduce the risk of experiencing a security breach and data compromise. Visa conducts periodic webinars to highlight key data security trends in addition to more detailed security training seminars. Businesses should

partner with their merchant-acquiring financial institutions to identify upcoming webinars and training events. Additionally, an array of data security and compliance information, including security alerts and bulletins highlighting compromise trends as well as information about training are available at www.visa.com/cisp.

EDUARDO PEREZ, CFA, has been with Visa Inc., since 2002 and currently leads the Global Data Security Group within the Payment System Risk Department. In this role, he has direct line responsibility for, U.S. Data Security, Global Third Party Agent Risk, Global Authentication Strategy and Emerging Risk, and Global Security Standards.

Be green. Save green.

Provide a superior guest experience while reducing operating costs with Control4® Suite Systems guestroom control solutions.

It's the little things—like having the temperature set just right or the ability to access concierge services from your TV—that create an environment perfectly suited for your guests' stay. Control4® Suite Systems are redefining the guest experience by offering an

automation system designed specifically for hotels that offers control of lighting, temperature, TV, music, draperies, alarm, and guest services for a lot less than you might expect. **Find out more by visiting us at www.control4.com/suitesystems**

