

Site Data Reflections

The top five Web intrusions

Volume Number 2



MasterCard Worldwide has taken a leadership position in helping secure the payments industry by requiring acquirers to both comply with the MasterCard Site Data Protection (SDP) Program and ensure that their merchants and service providers who store account data adhere to the Payment Card Industry (PCI) Data Security Standard.

Recognizing that timely information is critical in defending against account compromise, MasterCard has authored a series of articles, collectively called *Site Data Reflections*, which incorporate insights from industry security leaders. These articles draw upon our common experience in data security and forensics investigations, address current and emerging threats, and explore topics we believe are important to the overall security of your network. This article focuses on the top five unauthorized Web intrusions.

The Top Five Causes of Web Site Intrusions

For online merchants, a Web site intrusion can have potentially devastating consequences, including service disruption, vandalism, extortion, and the loss of consumer confidence. For cardholders and their issuers, the results can be equally direct: compromised card account numbers mean existing cards must be canceled, new cards issued, and any fraudulent charges absorbed on the issuer's bottom line.

While intruder motivations vary, these attacks can and do inflict significant damage to networks and compromise confidential customer data, too often with catastrophic consequences for e-commerce enterprises and consumers alike.

The good news is that by taking a few simple, inexpensive, common-sense precautions, many Web site intrusions can be avoided. The key to defending against these attacks is information. In conjunction with Cybertrust, we developed this list of the top five causes of Web site intrusions.

#1 Ineffective Patch Management

Almost every major Web site intrusion MasterCard has investigated could have been prevented with effective patch management. MasterCard conducts in-depth forensics investigations on impacted merchant Web sites, and in almost every instance we have found that account data compromise could have been prevented by simply updating Web sites with the latest software patches. It is imperative that IT Security teams deploy a patch-management program and keep it current. The investment in such a program provides excellent returns, as in most cases a simple download of a publicly available patch can often correct the vulnerability and deter a potential intruder. Yet this basic step often is not taken, leaving systems flawed and invitingly vulnerable to hacker attacks.

The National Infrastructure Protection Agency has stated that, "Network administrators must remain educated, and defenses must evolve along with the threats and offensive capabilities." You can build the most sophisticated and secure infrastructure, but if you don't manage patches and updates effectively, you may be leaving the front door wide open.

#2 No Security Scanning

Potential intruders are looking to exploit easily detected vulnerabilities in your network. To identify vulnerabilities, they often use scanning tools to find the path of least resistance into a network. For security professionals, scanning is an effective and inexpensive way to monitor your network for known vulnerabilities that may be exploited by hackers. However, while security scans are widely available tools, they are unfortunately grossly underused. For example, in our investigative forensics experience, we have seen that many hackers rely on the use of backdoor vulnerabilities, which provide easy and undetectable entry. Hackers use these tools to case a Web site before launching an attack. As many as 95% of these backdoor vulnerabilities would have easily been detected by basic scanning. The bottom line—scan your Web site!

#3 Weak Network Level Security

A key factor in effective network security management is the segmentation of production resources from resources that are visible from the Internet. All too often, companies lack proper network segmentation, allowing intruders to enter from the Internet and then roam throughout their entire corporate network. To correct this, companies should employ proper physical segmentation of their network, creating secure access control. See the "MasterCard Electronic Commerce Architecture and Best Practices" document on www.mastercard.com/sdp for more information on effective network segmentation.

Almost every major Web site intrusion MasterCard has investigated could have been prevented with effective patch management.

As many as 95% of these backdoor vulnerabilities would have easily been detected by basic scanning. The bottom line—scan your Web site!

#4 SQL Injection

A new vaccine for the flu? Most definitely not. But, like the flu, SQL injection can get inside its host and systematically break down its defenses. Although it has been around for years, SQL injection remains a favorite tool of the hacker. Based on our forensic investigative experience, the vast majority of compromises are accomplished through SQL injection. SQL is a standard computer language IT professionals employ to access and manipulate databases. In the electronic world, these databases may store critical cardholder account data information. Therefore, the SQL queries that are used to access these databases are a prime target for hackers. Simply put, they attack the SQL query and inject characters into it. The injected characters cause the SQL query to perform an unexpected, usually malicious, action. This unexpected action can allow the intruder to access sensitive information or, in an extreme scenario, the intruder can bypass network authentication and gain control of your network. Thankfully, there are simple solutions and commercially available tools that can protect your network against this long-time favorite hacker tool.

#5 Lack of Real-Time Security Monitoring

Everyone looks forward to the weekend, especially Web site intruders. Forensic analysis has shown that many sites are compromised between the time IT security professionals leave work on Friday and return on Monday. With no real-time monitoring during weekends, intruders can attack without concern of detection. In the fast-paced world of the Internet, the ability to rapidly recognize and react to network threats—even on weekends—is something no business can survive without. Widely available tools, such as firewalls, application logs, and critical server CPU utilization can provide an organization with a real-time pulse on the health of their network.

Prudent network protection need not be a complex, costly endeavor. A majority of Web site intrusions can be prevented by taking basic, cost-effective steps. Ensuring that network patches are current, employing standard security scanning, and providing real-time network monitoring are simple steps easily taken that deter casual hackers and enhance any network's security. The tools and information are readily available.

In the world of electronic commerce, information is not only power, it is protection.

For more information on MasterCard security leadership, please visit www.mastercard.com/sdp or www.mastercardsecurity.com

MasterCard provides a suite of security solutions to prevent, detect, and report fraud.