

Visa Inc. Data Security Alert

Malicious Software and Internet Protocol (IP) Addresses

January 29, 2009

This document provides information security officers, managers, technical analysts and incident response teams with information regarding recent data security computer attacks. This information is being provided to better equip Visa clients, merchants and agents in mitigating the threat of a network intrusion and data compromise.

This alert includes specific information on malicious software (see *Table 1* attachment) and bad IP addresses (see *Table 2* attachment) identified during Visa's computer forensic investigation. This information was recently used by several entities to discover security breaches that would otherwise have been undetected.

Visa highly recommends that clients, merchants and agents review the information contained in this alert and perform a scan to determine if their networks and hosts have been exposed to these malicious tools.

Malicious Software

- Malicious software or "malware" is designed to damage or infiltrate computer systems. An example of a malware is a packet sniffer. A packet sniffer, also known as a network analyzer, captures and interprets a stream or block of data (referred to as "packets") as it travels on the network. Packet sniffers can have legitimate or illegitimate uses on a network. Intruders can "sniff" packets being sent between network users and can collect sensitive information such as usernames, passwords, payment card data, or Social Security Numbers. Visa highly recommends that Visa clients, merchants, and agents review the list of malicious software and work with their internal information security team to determine if malware exists within their network. A comprehensive list of malware and MD5 hash values can be found in the *Table 1* attachment.

Note: Visa also provided this information to security product vendors to ensure that they develop signature files that can detect these types of malware.

Malicious IP Addresses

Every computer operating on the internet is assigned a unique number comprised of four "octets" called an Internet Protocol (IP) Address. Based on Visa's forensic investigation, we have identified IP addresses being used by intruders to gain unauthorized access to an entity's network. Visa highly recommends that Visa clients, merchants, and agents review the list of malicious IPs to monitor and block these IPs from their firewall rule sets.

A comprehensive list of malicious IPs can be found in the *Table 2* attachment.

The protection of account information is a responsibility shared by all participants in the Visa payment system. Visa is committed to providing educational information to its key stakeholders about potential vulnerabilities and urges financial institution clients to share this information with their vendors, processors, and other agents.

Mitigation Strategies

To guard your network against these malware and IP addresses, Visa clients, merchants and agents should review the network vulnerabilities identified below and implement mitigation controls where appropriate.

1. Configure firewalls to scan for – and block -- the attached IPs

Firewalls are typically used to prevent unauthorized Internet users from accessing networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

2. Utilize a Network-based Intrusion Detection System

Network-based intrusion detection systems (NIDS) are designed to monitor network traffic in order to distinguish between "normal" network activity and "abnormal" or "suspicious" activity that may identify an attack.

3. Utilize a Host-based Intrusion Detection System

Host-based intrusion detection systems (HIDS) are designed to monitor the behavior of host/computer systems to distinguish between "normal" activity and "abnormal" or "suspicious" activities. A key function of HIDS is to detect unknown activities caused by malware, packet sniffers or rootkits by monitoring incoming and outgoing communications traffic. HIDS will then check the integrity of critical system files and directories and watch for suspicious processes and executables.

HIDS can also monitor the usage of system accounts with elevated or administrative privilege. Unexpected use of accounts with administrative privilege is often a sign of a larger compromise.

4. Properly Segment Network

Payment card account information can be compromised at Visa clients, merchants, and agents that lack proper

For information on securing cardholder data, please visit www.visa.com/cisp.

network segmentation.

5. SQL injection

A review of recent data security breaches suggests Structured Query Language (SQL) injection attacks on e-commerce Websites and Web-based applications that manage card accounts (e.g., PIN updates, monetary additions, account holder updates) have become more prevalent.

SQL injection attacks are caused primarily by applications that lack input validation checks, un-patched Web servers and poorly configured Web and database servers. These attacks pose serious additional risks to cardholder data stored or transmitted within systems and networks connected to the affected environment. For more information on SQL injection, please refer to the Visa Data Security Alert, "SQL Injection Attacks," also attached to this alert e-mail.

Visa's "What to Do If Compromised" Procedures

In the event of a security incident, Visa clients and their agents must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings. The following steps, used in conjunction with the instructions delineated in Visa's *What to Do If Compromised* document, should be adhered to in the event of a security incident. These steps include:

- Immediately contain and limit the exposure
- Isolate compromised systems (do not log on to or access systems)
- Work with your internal information security and incident response team
- Keep a log of all actions taken and follow the chain of custody control
- Be on high alert and monitor traffic on all systems with cardholder data
- Notify your merchant bank
- If you are a financial institution, notify Visa Fraud Control and Investigations at (650) 432-2978 and notify your banking regulator
- Notify local law enforcement
- Consult with your legal department regarding state and federal notification laws

For More Information:

Please refer to the *What to Do If Compromised* document available on www.visa.com/cisp.

Additional information on these topics and many others is available at www.visa.com/cisp (see "Alerts and Bulletins"), as well as through the *Visa Business Review* publication available through Visa Online (VOL).

You may also contact Visa Fraud Control and Investigations at (650) 432-2978 or send an e-mail to usfraudcontrol@visa.com.

For information on securing cardholder data, please visit www.visa.com/cisp.