

Data Security Alert-Malicious Software & Internet Protocol Addresses



Visa reminds all that 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. This information is being provided to better equip clients, merchants and agents in mitigating the threat of a network intrusion and data compromise.

This alert includes updated information on malicious software (see Table 1 attachment) and Internet Protocol (IP) addresses (see Table 2 attachment) identified during Visa's computer forensic investigations.

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 a block of data (referred to as a "packet") as it travels on the network. Packet sniffers can have legitimate or illegitimate use 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.

It is recommended that clients, merchants, and agents to work with internal information security team to determine if malware exists within their network. An updated list of malware and hash values can also be found in the Table 1 attachment.

Malicious IP Addresses

Every computer operating on the Internet is assigned a unique number comprised of four “octets” called an IP address. Based on Visa’s forensic investigations, IP addresses have been identified as being used by intruders to gain unauthorized access to an entity’s network. It is recommended that clients, merchants, and agents work with internal information security teams to review, monitor and block malicious IPs from their firewall rule sets. Prior to blocking IPs, it is recommended that entities perform due diligence and ensure that blocking will not cause connectivity issues on legitimate access. An updated list of malicious IPs can be found in the Table 2 attachment.

Mitigation Strategies

To guard your network against malware and malicious IP addresses, clients, merchants, and agents should review the network vulnerabilities identified below and implement mitigating controls where appropriate. While these essential security practices do mitigate critical vulnerabilities, there are many factors that may affect an actual implementation. These measures alone may not be appropriate or sufficient depending on the implementation of an entity’s IT infrastructure and its business needs. Visa provides this information solely to build awareness of data security and industry best practices. Visa also disclaims any opinion of effectiveness or responsibility for any data compromise or other consequences as a result of these measures. Payment system participants should ensure that they are aware of these vulnerabilities and should take steps, where appropriate, to mitigate risk. It is important that all payment system participants continue to be diligent and maintain Payment Card Industry Data Security Standard (PCI DSS) compliance at all times.

Configure firewalls to scan for the attached IPs and determine whether or not to block IPs

Prior to blocking IPs, Visa recommends that entities perform due diligence and ensure that blocking will not cause connectivity issues on legitimate access. 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.

Utilize a Network-based Intrusion Detection System

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

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 root kits 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.

Properly Segment Network

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

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, and account holder updates) have become more prevalent.

SQL injection attacks are caused primarily by applications that lack input validation checks, unpatched 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.

▪