

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.

Attachment
Table 1 – Malicious Software, Tools, Hash(s) Value, and Registry Key
January 29, 2009

Filename	Purpose	MD5/SHA-1 Hash(s) or Registry Key
appsqlio.exe	Reverse shell tool	387cda6eb91f0b3a054de20c02320338
obsqlio.exe	SQL output redirector	f640e53718bc83cb8bb10b1eafb50edf
blobsqlio.exe	Packed version of gsecdump	959523fc10584da9bfb31a524ff472aa
sn.exe	Packet sniffer	e07b83abda5b566b3e9a30515a59ecc3
msdtsc.exe	Packet sniffer	4724103b13e6ce832fbb2c08a419eac6
svclhost.exe	Network communication tool	da4ab50185c7b246d1d2c8fa7bd7a5ed
rexesvr.exe	Command line execution	003f6cda98a40529cc87fd1387714fd7
svcl.exe	Renamed version of sn.exe	e07b83abda5b566b3e9a30515a59ecc3
eqslquery.exe	Script that automates the installation of rexesvr.exe	bc354dcf5221aea9fae8a3283c09504d
rarx.exe	Compression tool	fd729427144044730c572fd5b9be7dd9
Soft.exe	Backdoor	ea75939da539a3879e5b442b11b51f24
Isasstd.exe	Backdoor	07536e77ece9e70f5bf3d6f357c77b04
Isasstm.exe	Backdoor	e2736b8e0628a07fc3a6dcccad99245e
smn.exe	Backdoor	b0ff54c190455feda3f67b53c4a4453d
mstsk.exe	Utility to inject code on running processes	ddfd9073a5f222e223f5f2156c71629d

**Attachment
Table 2 – Bad IPs
January 29, 2009**

Signature	Type	Raw Details
Malicious IP Address	IP Address	90.15.59.86
Malicious IP Address	IP Address	85.221.196.131
Malicious IP Address	IP Address	85.221.138.252
Malicious IP Address	IP Address	64.247.58.239
Malicious IP Address	IP Address	89.37.241.180
Malicious IP Address	IP Address	83.4.164.214
Malicious IP Address	IP Address	72.36.215.253
Malicious IP Address	IP Address	202.71.103.77
Malicious IP Address	IP Address	194.146.248.7
Malicious IP Address	IP Address	85.17.105.34
Malicious IP Address	IP Address	91.193.63.15
Malicious IP Address	IP Address	89.37.240.118
Malicious IP Address	IP Address	91.145.136.65
Malicious IP Address	IP Address	82.232.177.64
Malicious IP Address	IP Address	89.76.218.105
Malicious IP Address	IP Address	89.37.241.241
Malicious IP Address	IP Address	89.76.220.36
Malicious IP Address	IP Address	83.55.141.204
Malicious IP Address	IP Address	216.55.169.234
Malicious IP Address	IP Address	89.43.45.232
Malicious IP Address	IP Address	62.21.81.104
Malicious IP Address	IP Address	89.37.242.28
Malicious IP Address	IP Address	89.43.45.159
Malicious IP Address	IP Address	77.253.108.16
Malicious IP Address	IP Address	91.189.139.168
Malicious IP Address	IP Address	85.221.136.196
Malicious IP Address	IP Address	77.253.115.137
Malicious IP Address	IP Address	213.84.163.246
Malicious IP Address	IP Address	83.110.17.228
Malicious IP Address	IP Address	12.210.14.103
Malicious IP Address	IP Address	74.138.172.183
Malicious IP Address	IP Address	85.17.239.11
Malicious IP Address	IP Address	69.244.206.15
Malicious IP Address	IP Address	69.141.149.138
Malicious IP Address	IP Address	88.156.44.152
Malicious IP Address	IP Address	216.80.124.225
Malicious IP Address	IP Address	76.100.75.1
Malicious IP Address	IP Address	216.196.173.93
Malicious IP Address	IP Address	75.64.114.45
Malicious IP Address	IP Address	89.32.130.86
Malicious IP Address	IP Address	58.65.239.58
Malicious IP Address	IP Address	66.36.229.201
Malicious IP Address	IP Address	74.54.131.130
Malicious IP Address	IP Address	74.53.114.16

**Attachment
Table 2 – Bad IPs
January 29, 2009**

Signature	Type	Raw Details
Malicious IP Address	IP Address	203.190.175.39
Malicious IP Address	IP Address	203.190.172.18
Malicious IP Address	IP Address	69.70.122.98
Malicious IP Address	IP Address	65.111.171.20
Malicious IP Address	IP Address	65.111.171.21
Malicious IP Address	IP Address	174.36.196.207
Malicious IP Address	IP Address	208.43.74.19
Malicious IP Address	IP Address	216.55.162.167
Malicious IP Address	IP Address	216.55.164.44
Malicious IP Address	IP Address	200.115.173.25
Malicious IP Address	IP Address	85.17.239.11
Malicious IP Address	IP Address	82.13.14.61
Malicious IP Address	IP Address	193.11.110.32
Malicious IP Address	IP Address	207.255.204.160
Malicious IP Address	IP Address	216.244.34.155
Malicious IP Address	IP Address	24.159.22.70
Malicious IP Address	IP Address	67.182.137.29
Malicious IP Address	IP Address	67.85.92.181
Malicious IP Address	IP Address	68.50.185.130
Malicious IP Address	IP Address	68.94.212.161
Malicious IP Address	IP Address	69.110.26.21
Malicious IP Address	IP Address	69.14.110.49
Malicious IP Address	IP Address	69.212.211.243
Malicious IP Address	IP Address	70.162.2.249
Malicious IP Address	IP Address	71.238.147.129
Malicious IP Address	IP Address	71.239.155.202
Malicious IP Address	IP Address	72.242.241.189
Malicious IP Address	IP Address	74.62.212.143
Malicious IP Address	IP Address	75.118.180.255
Malicious IP Address	IP Address	76.204.117.205
Malicious IP Address	IP Address	76.22.3.137
Malicious IP Address	IP Address	76.239.29.46
Malicious IP Address	IP Address	76.242.106.40
Malicious IP Address	IP Address	79.118.160.231
Malicious IP Address	IP Address	79.139.245.79
Malicious IP Address	IP Address	82.13.14.61
Malicious IP Address	IP Address	83.99.227.209
Malicious IP Address	IP Address	89.114.215.182
Malicious IP Address	IP Address	91.177.6.209
Malicious IP Address	IP Address	216.55.126.167
Malicious IP Address	IP Address	216.55.185.9
Malicious IP Address	IP Address	212.126.1.244
Malicious IP Address	IP Address	212.126.9.154
Malicious IP Address	IP Address	212.126.11.27
Malicious IP Address	IP Address	212.126.12.89

**Attachment
Table 2 – Bad IPs
January 29, 2009**

Signature	Type	Raw Details
Malicious IP Address	IP Address	212.126.14.197
Malicious IP Address	IP Address	212.126.18.171
Malicious IP Address	IP Address	212.126.20.83
Malicious IP Address	IP Address	212.126.22.64
Malicious IP Address	IP Address	212.126.25.247
Malicious IP Address	IP Address	212.126.31.182
Malicious IP Address	IP Address	212.126.32.67
Malicious IP Address	IP Address	212.126.46.199
Malicious IP Address	IP Address	212.126.47.93
Malicious IP Address	IP Address	212.126.53.23
Malicious IP Address	IP Address	212.126.55.166
Malicious IP Address	IP Address	212.126.57.215
Malicious IP Address	IP Address	212.126.72.14
Malicious IP Address	IP Address	212.126.73.220
Malicious IP Address	IP Address	212.126.78.153
Malicious IP Address	IP Address	212.126.83.57
Malicious IP Address	IP Address	212.126.84.117
Malicious IP Address	IP Address	212.126.92.167
Malicious IP Address	IP Address	212.126.94.174
Malicious IP Address	IP Address	79.9.108.226
Malicious IP Address	IP Address	88.214.208.44