

Global Partner Management Notice

Subject: Visa Data Security Alert—Malicious Software and Internet Protocol Addresses

Dated: April 10, 2009

Announcement:

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 Visa 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.

Visa recommends that Visa clients, merchants, and agents review this list of malicious software and work with their internal information security team to determine if malware exists within their network. An updated list of malware and MD5 and SHA-1 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, we have identified IP addresses being used by intruders to gain unauthorized access to an entity's network. Visa recommends that Visa clients, merchants, and agents review this list of malicious IPs to monitor and block these IPs from their firewall rule sets. **Prior to blocking IPs, Visa recommends 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, Visa 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, and 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.

1. **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.
2. **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.
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 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.
4. **Properly Segment Network** Payment card account information can be compromised at Visa clients, merchants, and agents that lack proper 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, 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.

For more information on SQL injection, please refer to the *Visa Data Security Alert*, “SQL Injection Attacks,” available at www.visa.com/cisp

Summary

Visa recommends that clients, merchants and agents review the information contained in this alert and perform a vulnerability scan to determine if their networks and hosts have been exposed to these malicious software and IP addresses. This information was recently used by several entities to discover security breaches that were otherwise undetected.

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)
- Preserve evidence for forensic investigation
- 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 acquiring bank if you are a merchant
- Notify Visa Fraud Control and Investigations at (650) 432-2978 if you are a financial institution
- Notify your banking regulator if you are a financial institution
- Notify local law enforcement
- Consult with your legal department regarding state and federal notification laws

- Visa may require the compromised entity to engage a Visa-approved Qualified Incident Response Assessor (QIRA). For a list of QIRAs, go to www.visa.com/cisp

See Table 1 and Table 2 on the following pages.

Table 1—Malicious Software, Tools, Hash Values, and Registry Keys

Filename	Purpose	File Size	MD5/SHA-1 Hash Values or Registry Key
Malicious Software (As of February/March 2009)			
wiadebyld.dll	Password collector	23,552	089AC4794A3E257146405EF791AC60F4
Win32.exe	Application that instantiates the wpcap file to sniff network packets, accepts a string argument specifying the pattern to search for packed WinPcap Pro or WinPcap	41,984	MD5: 59F020586B486637A38CFD421B828DF9 SHA1: 651e81997ec837b2df1a1efb472076f0509102f7
Hider.sys	Rootkit used to hide malicious code	Not available	MD5: 2dd6d91c651218b36b30e2e7c5c232d6 SHA1: 704c49121b9b9ff529eb62edc8e86af3ad859b14
Rh.exe	Rootkit Hunter application that is used to look for rootkits on systems and can also perform memory dumps for running processes	5,744	a043df46903c717093972609721c7da5
winsrv32.exe	Application that starts at runtime and runs in the background to "handle" the win32.exe file	254,646	1862f325333ba82651704ad36ff130bd
wpcap.dll	File from WinPcap Pro software	231,952	c5d497b91d5a28b7988101926721b154
packet.dll	File from WinPcap Pro software	479,232	7d34f9aef5c1ddefe948f71b85d8885d
Wns.exe	A reverse shell like smn.exe. Full capabilities are unknown	45,056	738A8C8B86C8099988C84626E274C094
Stamp.exe	Tool to change time stamps of files	45,568	1D16656700DC68584C82B5F84F8BC230
Malicious Software (As of December 2008 /January 2009)			
appsqlio.exe	Reverse shell tool	Not available	387cda6eb91f0b3a054de20c02320338
obsqlio.exe	SQL output redirector	Not available	f640e53718bc83cb8bb10b1eafb50edf
blobsqlio.exe	Packed version of gsecdump	Not available	959523fc10584da9bfb31a524ff472aa
sn.exe	Packet sniffer	Not available	e07b83abda5b566b3e9a30515a59ecc3
msdtsc.exe	Packet sniffer	79,872	4724103b13e6ce832fbb2c08a419eac6
svclhost.exe	Network communication tool	Not available	da4ab50185c7b246d1d2c8fa7bd7a5ed
rexesvr.exe	Command line execution	Not available	003f6cda98a40529cc87fd1387714fd7
svcl.exe	Renamed version of sn.exe	Not available	e07b83abda5b566b3e9a30515a59ecc3
eqsqlquery.exe	Script that automates the installation of rexesvr.exe	Not available	bc354dcf5221aea9fae8a3283c09504d
rarx.exe	Compression tool	Not available	fd729427144044730c572fd5b9be7dd9
Soft.exe	Backdoor	Not available	ea75939da539a3879e5b442b11b51f24
Isasstd.exe	Backdoor	1,536	07536e77ece9e70f5bf3d6f357c77b04

Filename	Purpose	File Size	MD5/SHA-1 Hash Values or Registry Key
Isasstm.exe	Backdoor	23,568	e2736b8e0628a07fc3a6dcccad99245e
smn.exe	Backdoor	1,536	b0ff54c190455feda3f67b53c4a4453d
mstsk.exe	Utility used to inject code on running processes	7,680	ddfd9073a5f222e223f5f2156c71629d

Table 2—Malicious IP Addresses

Signature	Type	Raw Details
Malicious IPs (As of February/March 2009)		
Malicious IP Address	IP Address	64.53.46.223
Malicious IP Address	IP Address	75.144.194.185
Malicious IP Address	IP Address	219.109.215.70
Malicious IP Address	IP Address	66.226.76.19
Malicious IP Address	IP Address	80.56.252.235
Malicious IP Address	IP Address	89.114.16.184
Malicious IP Address	IP Address	82.83.245.127
Malicious IP Address	IP Address	99.238.233.46
Malicious IP Address	IP Address	24.129.42.16
Malicious IP Address	IP Address	24.190.194.17
Malicious IP Address	IP Address	86.104.24.12
Malicious IP Address	IP Address	84.198.76.14
Malicious IP Address	IP Address	79.113.14.198
Malicious IP Address	IP Address	78.42.100.224
Malicious IP Address	IP Address	86.69.42.84
Malicious IP Address	IP Address	193.41.140.250
Malicious IP Address	IP Address	98.163.94.36
Malicious IP Address	IP Address	75.144.194.185
Malicious IP Address	IP Address	219.109.215.70
Malicious IP Address	IP Address	72.9.108.226
Malicious IP Address	IP Address	88.214.208.44
Malicious IP Address	IP Address	85.17.105.37
Malicious IP Address	IP Address	66.179.127.30
Malicious IPs (As of December 2008/January 2009)		
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
Signature	Type	Raw Details
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

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
Signature	Type	Raw Details
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
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

Source: Visa Business News, April 1, 2009

Best Regards,

Global Partner Management Team
First Data Corporation
Email: Gpm@firstdata.com

© 2009 First Data Corporation. All Rights Reserved. All trademarks, service marks and trade names referenced in this material are the property of their respective owners. The information contained herein is provided as a courtesy and is for general informational purposes only. This Alert is not intended to be a complete description of all applicable policies and procedures. The matters referenced are subject to change. Individual circumstances may vary. This Alert may include, among other things, a compilation of documents received from third parties. It should not be used as a substitute for reference to, as applicable, association releases, bulletins, regulations, rules and other official documents. First Data shall not be responsible for any inaccurate or incomplete information. This Alert may not be copied, reproduced or distributed in any manner whatsoever without the express written consent of First Data Corporation.