

# Visa Inc. Data Security Alert

## Malicious Software

November 4, 2008

This document provides information security officers, managers, technical analysts and incident response teams with information regarding recent computer data security 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 were otherwise 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. The following malware examples were recently identified through computer forensic investigations coordinated by Visa. A comprehensive list of malware and MD5 hash values can be found in the *Table 1* attachment.

- BP0.exe is a remote command shell "backdoor" that allows remote attackers to use the windows command shell to interact with the compromised server and run commands. This malware is hard-coded with a fixed IP address.
- Wiadebyls.dll is a password collector that gathers user credentials as they are used. The malware then transmits those credentials to a hard-coded IP address using the HTTP protocol.
- Wininet.exe is a packet sniffing program configured to capture payment data on the network.
- Wuauclt.exe is a key logger program configured to capture keystrokes and payment data on a point-of-sale (POS) terminal.
- SN.exe is a packet sniffer. Other variants of this malware exist with the ability to filter and log activities.

- Winlogex is a backdoor that was found under the name svchost.exe. This malware executes commands as specified by a remote server. The requesting of commands and the delivery of their output occurs over port 80 and appears as GET and POST requests. This malware also has the ability to install itself as a service, allowing it to persist after a reboot.
- MT.exe, also known as 9.exe, is a malware that provides the ability to list and terminate processes, services and TCP/IP filters, and list current network connections. The mt.exe utility also has the ability to clear system event logs, extract the clear-text password for a logged-in user, and perform secure file and directory deletion.

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

### 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
- Consult with your legal department regarding state and federal notification laws

**For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).**



---

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.

**For More Information:**

Please refer to the *What To Do If Compromised* document available on VOL.

Additional information on these topics and many others is available at [www.visa.com/cisp](http://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](mailto:usfraudcontrol@visa.com)

**For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).**



## Visa Inc. Data Security Alert

### Malicious Software and IP Addresses

November 4, 2008

**Table 1**

File Name	Purpose	File Size	MD5 Hash(s)
bp0.exe	Backdoor	49,152	7997A3B118DFEF1930FD48C0698CD3FA; d1e7183284aa55db71a0e3eb949a5a19
wiadebyls.dll	Password Collector	23,552	089AC4794A3E257146405EF791AC60F4
wiadelal.dll	User Enumeration	57,856	50E5D2D106ADB5D70870E60949E61DEF
sp.exe	Process Injection	69,632	8D049435C6ED6793517801B3F54414E6
service_torun.exe	Malware Installer	16,896	9D479C8BEE257A3B7119CC1B75D49013
Project1.exe	Downloader	398,848	EF78739780A80F100F8495D84DFEBAA6
hider.exe	Process Injection	104,448	5D1623BE9DAA5A70C15ECAD7DE375377
d.bat	Deletes hider.exe and itself.		cc1602121bbb990a785027a0296300
key.exe	Keystroke Logger	40,960	FD5E73A822F4A118FF7C4F1B7F3FC80A
keyloger.exe/ rundll32.exe/ lgr.exe	Keystroke Logger	415,232	46E641182909D3011130A125BDEBCD76
ca_setup.exe	Contains Cain & Abel	6,282,200	3c8c82f3edc758e5385126fab0fc6748
cain.exe	Redirect ARP	not available	931CCB7630C04BFEFA88FF52000BEE07
abel.exe	Redirect ARP	not available	0BE64BB8AE3372E2E77D4ACF652C5679
src.rar	Stealth Malware	not available	46e641182909d3011130a125bdebc76
rar.exe	Packing Utility	not available	541CCA44C5590E34791DCBC48A62DD13
wput.exe	Utility to conduct FTP Puts	not available	B41014C257196234D61CE6F081BE02DA
Netmon.exe	Backdoor	97,280	91fbafd2de6525d8da6e4b9a689f4987; 7a7c4551891dbb7b3666d7bb8c5b82c0
GSJ352JY.TMP	Backdoor	not available	83B3EB73FC86127D5FC455609AEA0343
cmdex.dll	See <i>netmon.exe</i> .	23,040	83b3eb73fc86127d5fc455609aea0343
OrakelSniffert.exe	Sniffing Tool	not available	e98059599b5c58d2becd8824ddba969c
atmdes.exe	ATM Encryption Tool	1,755,487	48546ca4ec1249e880a21048dd88df70
req_all2.sql	SQL statement to modify account balance reset tool.	not available	not available
hsm.exe	HSM Query	732,388	b0cb0cb7497a6147c0033124ef3ee0ad

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).

File Name	Purpose	File Size	MD5 Hash(s)
hsm2.exe	HSM Query	732,222	b81fbbbce48131073fb8f1973bcfea6a
mstsk.exe	Rootkit	not available	94e07fd87cd033a9af4d47301270831c
WUAUCLT.EXE	Keystroke Logger (aka Perfect Key Logger).	438,272	bae0fb25bcf05a5da7fde8dce759ee0d
wuauclthk.dll	Part of Perfect Key Logger.	2,476	58129986fa29f6dadcd99ab45f60bcb3c
WUAUCLTI.DLL	Part of Perfect Key Logger.	215,040	9bd9e593cecf340b3bc9783946860dd9
wuaucltwb.dll	Part of Perfect Key Logger.	40,960	2e6016325548ab79e2d636640c6ec473
1.vbs	Visual Basic script used for downloading files.	not available	3468733cf3399833bcf0a334831333
bc9.exe	Compiled C code utilized to open a backdoor. c:\windows\system32\	not available	431676ccf89ff1eeb1e9fa6f8823de31
svclhost.exe	Executable to stop/start services.	not available	936134fabb98340dea3987fff320392
svclhost.exe	Custom-written malware that is a standard remote command shell backdoor. Allows a remote attacker to use the windows command shell to run commands. This tool is the same as BP6.exe except that it has been repacked and mangled to avoid detection by Symantec antivirus.	not available	1AAF500A990D038A388314087F833B96
soft.exe	Renamed version of svclhost.exe.	not available	d759b06fce53e204c5c5779cb6b3ba9e
stop.exe	A custom written piece of malware that excludes certain drives from Symantec antivirus scanning in an attempt to hide the presence of malware from Symantec antivirus programs.	not available	28579EF7FD9AF26819131FF301AFBE21
Svcnhost.exe	Executable to stop/start services.	not available	4102094fa983e34892746bba93473
msdll.exe	Remote control software.	not available	70942f9838d73325-4987feaa01043

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



File Name	Purpose	File Size	MD5 Hash(s)
svcdhost.exe	Remote control software.	not available	0982caa30984de05930fdf03402395
11.CMD	Hacker script (ipconfig, netstat).	not available	b98d0d59f428324dfa2b748bbac99dd6
11.CMD	Hacker script (cmd.exe).	not available	bf4e35c58a93bfffccaece7d3333cf4
22.CMD	Hacker script (osql).	not available	aa061c3070307da72e8570e1b0776ff9
ktn.exe	Drops widebyld.dll and d.bat	not available	9a94b6148f66ebde50d6503d6827810b
lsasstm.exe	Tunnel to a fixed IP address.	not available	3ec201c28a6a2b2a3415b3ac03429033
lsasstm.exe	Tunnel to a fixed IP address.	1,536	d6aa6f4befcb698c116ebc5a272bb14b
lsasstm.exe	Tunnel to a fixed IP address.	not available	29834345eaf39470db397223ba309
msts.exe	Backdoor Trojan	not available	0edd1f6c91c042bfd8d962302f6fc8c7
svc.exe	Opens connection on DNS port to known hacker proxies on the Internet; drops wget.exe and wzip.exe. Appears to be a key logger with potential to upload data.	not available	5ae3cc4cb605357f1a65cc0b3b597d11
wget.exe	GNU Wget 1.10.2, a non-interactive network retriever.	not available	899bcda15d5d03a968373b7081d9121f
wiadebyld.dll	Command and control interface for bot.	not available	6ada13bb46f50a6f743095cefb391aeb
wzip.exe	Command line compression tool.	not available	f53628ed23119e7398c644680ec8c09f
connectback.exe	Reverse command shell. Provides direct command line access.	4,096	548639ba66fdff6d0595051179330b46
last.exe	Backdoor with rootkit capabilities.	32,768	3ce004dd7951a98edeedf6feb983cc1d
sn.exe (v1)	The sn.exe executable and its variants are network packet capture programs with filtering and logging capabilities.	63,488	12a347b6b40a2cf4031470f42dd57a98
sn.exe (v2)	same	68,608	60e51cb18968b6971ee6fe8f750a2dad
sn.exe (v3)	same	73,216	e07b83abda5b566b3e9a30515a59ecc3

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



File Name	Purpose	File Size	MD5 Hash(s)
sn.exe (v4)	same	45,056	2a0b55aabd9b1c65f132a5cad907ffea
sn.exe (5)	same	not available	27A18A28A5A0CB6486987B140B5A354B
calc.exe	Custom-written malware that is a simple reverse shell backdoor allowing an attacker to enter DOS-style commands.	not available	1A36788209057D1CC3281B979F0C9F23
gur.exe	Custom-written malware that dumps user and group information from a system.	not available	3CD982A1569A1880359C3CDFAA9A9ED0
beyond.exe	A freely available remote access tool.	not available	bc354dcf5221aea9fae8a3283c09504d
fgdump.exe	A freely available tool that implements a rewritten version of pwdump and combines it with a tool called cachedump. Both tools are used to steal credentials.	not available	3e709de2d397a62bd82d301c54a62afb
imokav.exe	A tool required for pwdump to function properly.	not available	d3cb0613e96dba5924de57ba341ad92f
lstarget.dll	A tool required for pwdump to function properly.	not available	0ead8cb834c3c1e9108270efeded5eef
pskill.exe	A freely available tool to stop running processes.	not available	48e3b6c97a2c49c1b00ae6b2287c0244
pslist.exe	A freely available tool to list running processes.	not available	61fd7759f215f9f88ae88525fd30af21
pwdump.exe	A password cracking tool.	not available	4366095f7dbec0f4a693d58d79984d16
rar.exe	A tool that compresses data into RAR format.	not available	fb748921d9a7ccc91380eddf8fcf274d
whosthere.exe	A freely available tool to steal credentials.	not available	e4fe5e8d86afcb20fae83012a7858297
rexesvr.exe	A file executed by beyond.exe.	not available	003f6cda98a40529cc87fd1387714fd7

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).

File Name	Purpose	File Size	MD5 Hash(s)
winlogex aka svchost.exe	<p>The Winlogex backdoor was found under the filename svchost.exe. The purpose of the tool is to execute commands as specified by a remote server. The requesting of commands and delivery of their output occurs over HTTP port 80 and appears as GET and POST requests. This malware has the ability to install itself as a service to allow it to persist after a reboot.</p>	14,848	<p>B4CC4E58F6FA41BD9C99ADA23BBF7052 and d759b06fce53e204c5c5779cb6b3ba9e</p>
MT.exe aka 9.exe	<p>The mt.exe malware provides a diverse array of features related to exploring the configuration and state of host as well as several malicious features. The malware provides the ability to list and terminate processes, services, and TCP/IP filters, and list current network connections. Malicious functionality provided by the mt.exe utility includes the ability to clear system event logs, extract the clear-text password for a logged-in user as well as secure file and directory deletion.</p>	83,968	79E7533E20241D7D5146BE54742E0662

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).

File Name	Purpose	File Size	MD5 Hash(s)
proclDE.sys	The proclDE.sys malware is a primitive Windows rootkit designed to hide a malicious process in a process listing and hide the malware executable file from a directory listing.	4,608	22DA4EE5F9287ACA16A8B6552BEB1631
proclDE.sys	same	2,432	714107D06CBD6BEEFA2BBC5C2A9B2C9F
emp.exe, emporos.exe, mercsoft.exe, elo.exe	Key Logger.	not available	e84109b1a71859856cf101f00f2e3486
B.EXE	Backdoor (reverse shell). Any non-ODBC traffic communicating over TCP port 1433 may indicate the usage of a variant of the B.EXE reverse shell malware.	1,536	13389AF1B033D1D536D1A3C50056BF6C
mgs.exe	Tool for encoding/decoding binary files to and from ASCII hex. Hackers may use this tool when transferring binary data is not allowed. The tool generates an output file called report.txt after successful decryption.	12,288	E0D9A0DDEF26AE56F26B4A46DF69B8D5
uploadtester.asp	This is an Active Server Page backdoor. It allows an attacker to upload files onto the web server that hosts the pages. The malware exists in the web server WEBROOT or in another publicly available directory.	5091 bytes	cf342cf3a89b4eb185ad50365fc5b7e8

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).

File Name	Purpose	File Size	MD5 Hash(s)
freeASPUpload.asp	<p>Both uploadtester and freeASPUpload are open source ASPs that allow a user to upload and download files from the web server.</p> <p>The scripts can be downloaded from <a href="http://www.freeaspupload.net">http://www.freeaspupload.net</a>.</p> <p>The uploadTester.asp is a page that contains a form that can be used to select the file that needs to be uploaded;</p> <p>freeASPUUpload.asp is the page that actually processes the uploaded file and stores the file on the web server.</p>	7997 bytes	a787ff27acc4fb29e539d0bfc7547c01
S1.ASP/S.ASP	<p>ASP backdoor. It allows an attacker to run commands using the xp_cmdshell stored procedure on any system that hosts an IIS server and an MSSQL server.</p>	760 bytes	56687fdb9a6d8560feea27261284635e
	<p>S1.ASP is an ASP-backdoor that, if installed in the webroot of an IIS web server, can be browsed to using a browser.</p> <p>The backdoor allows the attacker to run commands on the webserver using the xp_cmdshell stored procedure. The server has to host a MSSQL database server and has to have stored procedures enabled for a successful query.</p>		

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



File Name	Purpose	File Size	MD5 Hash(s)
INFO.ASPX	ASP backdoor. It allows an attacker to run commands using the cmd.exe executable that is resident on the system. The malware runs in the context of an IIS server.	1194 Bytes	e630e0d634ad56885785ba7ac9fa4b19
csrsvc.exe	Memory Dumper	not available	0590cde18ed26d74d18c545deed312f0
csrsvc.exe	Memory Dumper	75,264	1f9d0d200321ad6577554cc1d0bb6b69
csrsvc.exe	Memory Dumper		ec137291dd52a3a2de246f22d3c3bc7f0
csrsvc.exe	Memory Dumper		8bfa2c3e089c10bc39ae6d0d41e4acf211318db4
MemPDumper.exe	Memory Dumper	75,776	dbaab511f2210228e41c3ffdbe5d3fce
dnsmgr.exe	Track Data Parser	1,162,117	bf27e87187c045e402731cdaa8a62861
dirmon.chm	Output file from track data parser programs.	39,560	ac15d275d4d01c453aab907da7051f81
WinMgmt.exe	Calls csrsvc.exe and dnsmgr.exe and runs an interactive command shell on tcp port 3373. <b>Note:</b> Check for May 2008 timestamp. This is the malware version.	66,048	3e19ef9c9a217d242787a896cc4a5b03
install.bat	Batch file that installs WinMgmt as a windows service.	43	a7c24031cae3f29ec0c30d220c52a087
dump.bat	Batch file installs memory dumper program on a single computer.	267	9393aaf96f3fc25bfcc6649e33edc560
psexec.exe	Sysinternal tool used to run process on remote machines.	135,168	579b43e13294eb85faa7c28b470b19c1
psexec.exe	Sysinternal tool used to run process on remote machines.	not available	78a2c9d79c21ddfc7ced32f5ebec618
play.bat	File that calls install.bat file to install memory dumper on multiple systems.	79	fcb37de3b9b1c831a52a836b7a2f2695

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



File Name	Purpose	File Size	MD5 Hash(s)
Far.exe	DOS-based file manager used by attacker.	620,032	d1d9c26a77beb82b13c82e854042dc92
compenum.exe	Network scanner that outputs a list of accessible systems.	54,272	bcc61bdf1a2f4ce0f17407a72ba65413
shareenum.exe	Network scanner that outputs a list of accessible shares.	53,248	3ca6ec07c6b840e7a256d09839ba0c4f
Trojan-Spy.Win32.PcGhost.412 or pcMSg.dll	pcMsg.dll	ff949f47cba1aa87b334331a5dbb6996	Key Logger.
Trojan-Dropper.Win32.Joiner.dv or SETUP.EXE	SETUP.EXE	fc84b0510aa5d2816e5a57e9d746a1f5	Password-stealing Trojan.
Email-Worm.Win32.VB.bj or FOLDER.HTT	FOLDER.HTT	ba54460b0e409f18db4c13eddd3a78c4	Worm spread through network shares.
Trojan.VBS.Starter.e	IDS.EXE	6f499889dcded807f1e1bd5372977658	Exploits Internet Explorer vulnerabilities.
Net-Worm.Win32.Stap.d	Yahoo Mgr 2.0.exe	7b05bd7cd818838677fbd44401429f16	Worm spread through network shares and e-mail.
Heur.Trojan.Generic	news_doc.exe	1dc757b5d32a9b3444259ff8814dee01	
Email-Worm.Win32.LovGate.c	midsong.exe	9ac3e31f7bde0ee83102e618d1d60c17	Worm spread through e-mail attachments.
Virus.Win32.FunLove.4070	pics.exe	51fdaaf4aefd62266b6e005539a9753b	Virus that can infect local network from a user account.
Virus.Win32.Sality.y	hamster.exe	e137fa94a9e4a514b4d204ce44a772d6	
Virus.VBS.Redlof.k	Folder.000	0f6320a81b05a288a34e731ff1b9d926	Virus that may infect HTML or text files.
Trojan.VBS.Starter.e	folder.010	21010ca7c2924177bb59d4104204279e	Trojan.
Email-Worm.Win32.Mixor.a	rptchk32.exe	96db0759344a6357e5414da2e88dc560	Infected version of Microsoft DirectX 9.0 setup file.
Net-Worm.Win32.Bozori.k	TFTP2256.000	94744e61994ad47b24831bddac63aa11	
Virus.Win32.Small.r	Dc6846.000	093e9b17f5a43ef5b75b2e873e87ddbc	Keystroke Logger.
trojan.win32.agent.ad	autorun.inf.000	6be4b0d0eb557b9a84415fe90204d78b	
Virus.DOS.Esot.509	0000cb8b.msg	a2e9bda55681defee2e534c3db39a611	

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).

**Table 2**

<b>Signature</b>	<b>Type</b>	<b>Raw Details</b>
Malicious IP Address	IP Address	66.235.184.35
Malicious IP Address	IP Address	66.36.229.201
Malicious Host Name	Host Name	spider.keeper.ws
		58.65.239.58
Malicious IP Address	IP Address	209.160.73.236
Malicious IP Address	IP Address	88.255.90.234
Malicious IP Address	IP Address	147.202.44.42
Tool Download Site	IP Address	84.51.21.60
Upload Site	Domain Name	Rapidshare.com
Malicious IP Address	IP Address	66.226.79.71
Malicious IP Address	IP Address	80.77.95.236
Malicious IP Address	IP Address	80.77.95.237
Malicious IP Address	IP Address	80.77.95.238
Malicious IP Address	IP Address	80.77.95.239
Malicious IP Address	IP Address	216.55.190.208
Malicious IP Address	IP Address	88.214.208.44
Malicious IP Address	IP Address	195.189.226.168
Malicious IP Address	IP Address	216.55.147.72
Malicious IP Address	IP Address	216.255.178.122
Malicious IP Address	IP Address	76.19.248.173

**For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).**



<b>Signature</b>	<b>Type</b>	<b>Raw Details</b>
Malicious IP Address	IP Address	66.226.64.3
Malicious IP Address	IP Address	194.186.220.12
Malicious IP Address	IP Address	65.13.18.216
Malicious IP Address	IP Address	216.55.190.208
Malicious IP Address	IP Address	65.113.119.152
Malicious IP Address	IP Address	24.253.85.84
Malicious IP Address	IP Address	192.216.198.4
Malicious IP Address	IP Address	80.6.2.124
Malicious IP Address	IP Address	83.97.194.100
Malicious IP Address	IP Address	24.188.192.235
Malicious IP Address	IP Address	83.97.194.100
Malicious IP Address	IP Address	86.122.97.223
Malicious IP Address	IP Address	217.121.209.201
Malicious IP Address	IP Address	216.255.178.122
Malicious IP Address	IP Address	66.36.229.210
Malicious IP Address	IP Address	66.148.74.113
Malicious IP Address	IP Address	38.101.105.44
Malicious IP Address	IP Address	69.60.120.99
Malicious IP Address	IP Address	64.62.137.150
Malicious IP Address	IP Address	90.15.59.86
Malicious IP Address	IP Address	194.146.248.7
Malicious IP Address	IP Address	85.221.196.131

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



Signature	Type	Raw Details
Malicious IP Address	IP Address	64.247.58.239
Malicious IP Address	IP Address	85.221.138.252
Malicious IP Address	IP Address	83.4.164.214
Malicious IP Address	IP Address	89.37.241.180
Malicious IP Address	IP Address	72.36.215.253
Malicious IP Address	IP Address	202.71.103.77
Malicious IP Address	IP Address	85.17.105.34
Malicious IP Address	IP Address	91.193.63.15
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	89.43.45.232
Malicious IP Address	IP Address	89.37.240.118
Malicious IP Address	IP Address	62.21.81.104
Malicious IP Address	IP Address	216.55.169.234
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	89.38.40.54
Malicious IP Address	IP Address	74.138.172.183
Malicious IP Address	IP Address	12.210.14.103
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

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



Signature	Type	Raw Details
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	66.36.241.45
Malicious IP Address	IP Address	209.160.73.236
Malicious Host Name	IP Address	66.226.76.119
Malicious IP Address	IP Address	64.62.137.150
Malicious IP Address	IP Address	204.13.160.28
Malicious IP Address	IP Address	66.148.74.113
Malicious IP Address	IP Address	66.36.231.45
Malicious Traffic Signature	String	-----7d33188e01e4
Malicious Traffic Signature	UserAgent String	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.11) Gecko/20071121 Firefox/2.0.0.11
Malicious Traffic Signature	String	GET //go/open.php?
Malicious Traffic Signature	String	/stat?uptime=%d&downlink=%d&uplink=%d&id=%s&statpass=%s&comment=%s
Malicious IP Address	IP Address	66.36.229.201
Malicious IP Address	IP Address	216.197.96.131
Malicious IP Address	IP Address	58.65.239.58
Malicious IP Address	IP Address	67.80.100.210
Malicious IP Address	IP Address	24.0.67.192
Malicious IP Address	IP Address	24.147.127.2
Malicious IP Address	IP Address	24.184.17.157

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



Signature	Type	Raw Details
Malicious IP Address	IP Address	24.199.106.221
Malicious IP Address	IP Address	24.94.52.194
Malicious IP Address	IP Address	58.65.239.42
Malicious IP Address	IP Address	64.62.137.150
Malicious IP Address	IP Address	65.13.18.216
Malicious IP Address	IP Address	66.226.76.119
Malicious IP Address	IP Address	66.226.77.20
Malicious IP Address	IP Address	66.235.183.207
Malicious IP Address	IP Address	66.235.184.222
Malicious IP Address	IP Address	66.235.184.35
Malicious IP Address	IP Address	66.36.229.201
Malicious IP Address	IP Address	66.36.229.201
Malicious IP Address	IP Address	66.36.244.102
Malicious IP Address	IP Address	66.36.244.22
Malicious IP Address	IP Address	66.36.244.22
Malicious IP Address	IP Address	68.230.96.99
Malicious IP Address	IP Address	68.44.1.54
Malicious IP Address	IP Address	68.83.200.176
Malicious IP Address	IP Address	69.114.209.137
Malicious IP Address	IP Address	69.114.38.212
Malicious IP Address	IP Address	69.115.231.178
Malicious IP Address	IP Address	69.122.152.134
Malicious IP Address	IP Address	70.143.53.160
Malicious IP Address	IP Address	70.252.194.125
Malicious IP Address	IP Address	72.36.215.253
Malicious IP Address	IP Address	72.36.215.253
Malicious IP Address	IP Address	74.72.104.249
Malicious IP Address	IP Address	76.10.128.170
Malicious IP Address	IP Address	80.89.128.150
Malicious IP Address	IP Address	81.169.137.209
Malicious IP Address	IP Address	81.169.183.122
Malicious IP Address	IP Address	81.19.70.3

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).



Signature	Type	Raw Details
Malicious IP Address	IP Address	82.165.187.34
Malicious IP Address	IP Address	83.217.63.251
Malicious IP Address	IP Address	84.51.21.60
Malicious IP Address	IP Address	85.25.147.96
Malicious IP Address	IP Address	87.234.154.82
Malicious IP Address	IP Address	87.236.198.84
Malicious IP Address	IP Address	88.212.196.70
Malicious IP Address	IP Address	88.251.228.98
Malicious IP Address	IP Address	88.255.90.234
Malicious IP Address	IP Address	88.255.90.234
Malicious IP Address	IP Address	88.85.72.9
Malicious IP Address	IP Address	91.149.90.80
Malicious IP Address	IP Address	128.36.233.87
Malicious IP Address	IP Address	147.202.44.42
Malicious IP Address	IP Address	172.16.1.42
Malicious IP Address	IP Address	195.71.90.10
Malicious IP Address	IP Address	204.13.160.28
Malicious IP Address	IP Address	206.126.82.188
Malicious IP Address	IP Address	206.225.87.160
Malicious IP Address	IP Address	206.225.87.160
Malicious IP Address	IP Address	206.225.90.14
Malicious IP Address	IP Address	206.225.95.98
Malicious IP Address	IP Address	209.160.73.236
Malicious IP Address	IP Address	216.55.147.91
Malicious IP Address	IP Address	216.55.160.23
Malicious IP Address	IP Address	216.55.168.211
Malicious IP Address	IP Address	216.55.168.39
Malicious IP Address	IP Address	216.55.169.234
Malicious IP Address	IP Address	217.106.233.187
Malicious IP Address	IP Address	217.8.249.162
Malicious IP Address	IP Address	add.83673hour.biz
Malicious IP Address	IP Address	cakirgroup.com

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).

Signature	Type	Raw Details
Malicious IP Address	IP Address	come.digg00igg.biz
Malicious IP Address	IP Address	keeper.ws
Malicious IP Address	IP Address	me.24next24.biz
Malicious IP Address	IP Address	www.om7890.com
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	24.10.208.205
Malicious IP Address	IP Address	64.39.30.124
Malicious IP Address	IP Address	24.155.37.177
Malicious IP Address	IP Address	216.55.142.88
Malicious IP Address	IP Address	216.55.147.91
Malicious IP Address	IP Address	66.36.229.201
Malicious IP Address	IP Address	66.36.244.38
Malicious IP Address	IP Address	66.235.184.35
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	65.31.75.62
Malicious IP Address	IP Address	65.97.139.242
Malicious URL	URL	<a href="http://www.narod.ru">www.narod.ru</a>
Malicious URL	URL	<a href="http://www.uploads.narod.ru">www.uploads.narod.ru</a>
Malicious IP Address	IP Address	212.43.222.170

For information on securing cardholder data, please visit [www.visa.com/cisp](http://www.visa.com/cisp).