



## **Internet Crime Complaint Center's (IC3) Scam Alerts January 7, 2013**

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

### **NEW TWIST TO ONLINE TECH SUPPORT SCAM**

The IC3 continues to receive complaints reporting telephone calls from individuals claiming to be with Tech Support from a well-known software company. The callers have very strong accents and use common names such as "Adam" or "Bill." Callers report the user's computer is sending error messages, and a virus has been detected. In order to gain access to the user's computer, the caller claims that only their company can resolve the issue.

The caller convinces the user to grant them the authority to run a program to scan their operating system. Users witness the caller going through their files as the caller claims they are showing how the virus has infected their computer.

Users are told the virus could be removed for a fee and are asked for their credit card details. Those who provide the caller remote access to their computers, whether they paid for the virus to be removed or not, report difficulties with their computer afterwards; either their computers would not turn on or certain programs/files were inaccessible.

Some report taking their computers to local technicians for repair and the technicians confirmed software had been installed. However, no other details were provided.

In a new twist to this scam, it was reported that a user's computer screen turned blue, and eventually black, prior to receiving the call from Tech Support offering to fix their computer. At this time, it has not been determined if this is related to the telephone call or if the user had been experiencing prior computer problems.

---

### **TDOS ATTACKS TO EMERGENCY SERVICES**

As some are aware, reports of pay day loan phone scams have been occurring for the last three years or more. The scam involves victims being relentlessly contacted at their residences and places of employment regarding claims they are delinquent on a payday loan. Various coercion techniques have been used by the subjects in an attempt to persuade the victim to send money. Such techniques have evolved from repeated annoying phone calls to abusive language, threats of bodily harm, and arrests.

The IC3 has become aware of increased coercion tactics used by the subjects, which have created a threat to emergency services across the nation. The threats have now escalated into a Telephony Denial of Service (TDoS) attacks against the victims' employers, which some have been emergency service agencies. The TDoS attacks have tied up the emergency services' telephone lines, preventing them from receiving and responding to legitimate emergency calls.

The other tactic the subjects are now using in order to convince the victim that a warrant for their arrest exists is by spoofing a police department's telephone number when calling the victim. The subject claims there is a warrant issued for the victim's arrest for failure to pay off the loan. In order to have the police actually respond to the victim's residence, the subject places repeated, harassing calls to the local police department while spoofing the victim's telephone number.

---

## MOST POPULAR 2012 PASSWORDS REVEALED

[SplashData.com](http://SplashData.com) recently published the following information regarding the most popular 2012 passwords on the web. The ranking was based on password information from compromised accounts posted by hackers online. The article was also featured on [blogs.avg.com](http://blogs.avg.com).

This year, the list is back! So it's time to see how, if at all, users have learned their lessons about what makes a strong password.

Here's the full list and how it compares to last year's:

#	Password	Change from 2011
1.	password	Unchanged
2.	123456	Unchanged
3.	12345678	Unchanged
4.	abc123	Up 1
5.	qwerty	Down 1
6.	monkey	Unchanged
7.	letmein	Up 1
8.	dragon	Up 2
9.	111111	Up 3
10.	baseball	Up 1
11.	iloveyou	Up 2
12.	trustno1	Down 3
13.	1234567	Down 6
14.	sunshine	Up 1
15.	master	Down 1
16.	123123	Up 4
17.	welcome	New
18.	shadow	Up 1
19.	ashley	Down 3
20.	football	Up 5
21.	jesus	New
22.	michael	Up 2
23.	ninja	New
24.	mustang	New
25.	password1	New

As you can see, people haven't changed their password habits a whole lot in a year.

**If your password is included on that list, or is a close variation of these passwords, it's really important to take action now!**

Fixing your password problem can be very simple;

**Long is strong:** The longer the password, the more difficult it will be for someone to try and crack it using brute force. So, instead of a single word, with a jumble of symbols, numbers and characters, try a string of words. Use a line of your favorite poem, song or just something memorable. Feel free to add your lucky number at the end if you like.

Something like: "withnodirectionhome1085".

A famous Dylan lyric like this will always be easy to remember, and say you were born in October 1985. This means that you've suddenly got a 23 character password, which is much harder to crack than something much harder to remember such as "Phu!R7tRjX".

**Variety is the spice of life:** The trouble with smaller, complex passwords is that they can be a real hassle to remember, often forcing you to use the same password for multiple accounts which is never a good idea. So another benefit of having long, easy to remember passwords is that you keep many passwords.

---

## JAVA ZERO-DAY EXPLOIT ON SALE FOR 'FIVE DIGITS'

Miscreants in the cyber underground are selling an exploit for a previously undocumented security hole in Oracle's Java software that attackers can use to remotely seize control over systems running the program, [KrebsOnSecurity](#) has learned.

The flaw, currently being sold by an established member of an invite-only Underweb forum, targets an unpatched vulnerability in Java JRE 7 Update 9, the most recent version of Java (the seller says this flaw does not exist in Java 6 or earlier versions).

According to the vendor, the weakness resides within the Java class "MidiDevice.Info," a component of Java that handles audio input and output. "Code execution is very reliable, worked on all 7 version I tested with Firefox and MSIE on Windows 7," the seller explained in a sales thread on his exploit. It is not clear whether Chrome also is affected. "I will only sell this ONE TIME and I leave no guarantee that it will not be patched so use it quickly."

The seller was not terribly specific on the price he is asking for this exploit, but set the expected offer at "five digits." The price of any exploit is ultimately whatever the market will bear, but this is roughly in line with the last Java zero-day exploit that was being traded and sold on the underground. In August, I wrote about a newly discovered Java exploit being folded into the BlackHole exploit kit, quoting the author of that crimeware tool as saying that "the price of such an exploit if it were sold privately would be about \$100,000."

I have repeatedly urged readers who have no use for Java to remove it from their systems entirely. This is a very complex program that is widely installed (Oracle claims that some 3 billion devices run Java), and those two qualities make it a favorite target for attackers. What's more, Java is a cross-platform technology, meaning that applications written to run in Java can run seamlessly across multiple operating systems. Indeed, some 650,000 Mac users discovered this the hard way earlier this year, when the Flashback worm took advantage of an unpatched vulnerability that was present in Apple's version of Java.

Apple has since taken steps to unplug Java from the browser in OS X, and this is the very approach I've recommended for users who need Java for specific Web sites or applications (see: <http://krebsonsecurity.com/how-to-unplug-java-from-the-browser>), I would suggest a two-browser approach. If you normally browse the Web with Firefox, for example, consider disabling the Java plugin in Firefox, and then using an alternative browser (Chrome, IE9, Safari, etc.) with Java enabled to browse only the site that requires it.

---

## **FAKE ORDER CONFIRMATION EMAILS FROM AMERICAN AIRLINES LEADS TO MALWARE**

[MX Lab](#), <http://www.mxlab.eu>, intercepted some samples of fake order confirmation emails from American Airlines that will lead the user to a host with an embedded Javascript that will download the malicious payload.

The email is send from the spoofed address "American Airlines" and has the following body (single image email):



In this case, the URL `hxxp://egiser-ingenieros.com/FAHSIENFHE.html` brings us to an HTML page with an embedded Javascript that will start the download of the malicious ZIP file:

```
<html>(CR)(LF)
<body>(CR)(LF)
<script language="JavaScript">(CR)(LF)
<!--(CR)(LF)
window.location="AA_Electronic_Ticket.zip";(CR)(LF)
//-->(CR)(LF)
</script>(CR)(LF)
</body>(CR)(LF)
</html>
```

The ZIP file has the name `AA_Electronic_Ticket.zip` and contains the 60 kB large file `AA_Electronic_Ticket.exe`.

The trojan is known as `Spyware/Win32.Zbot`, `Win32/TrojanDownloader.Zortob.B`, `Trojan.Generic.KDV.783582`, `W32/Kryptik.BWW`.

At the time of writing, 13 of the 44 AV engines did detect the trojan at Virus Total.

Virus Total [permalink](#) and SHA256:

`df95ea18dd12805419f71d33e7e8e2bd7a9c013b9799559ef288b609cc56e84f`.

---

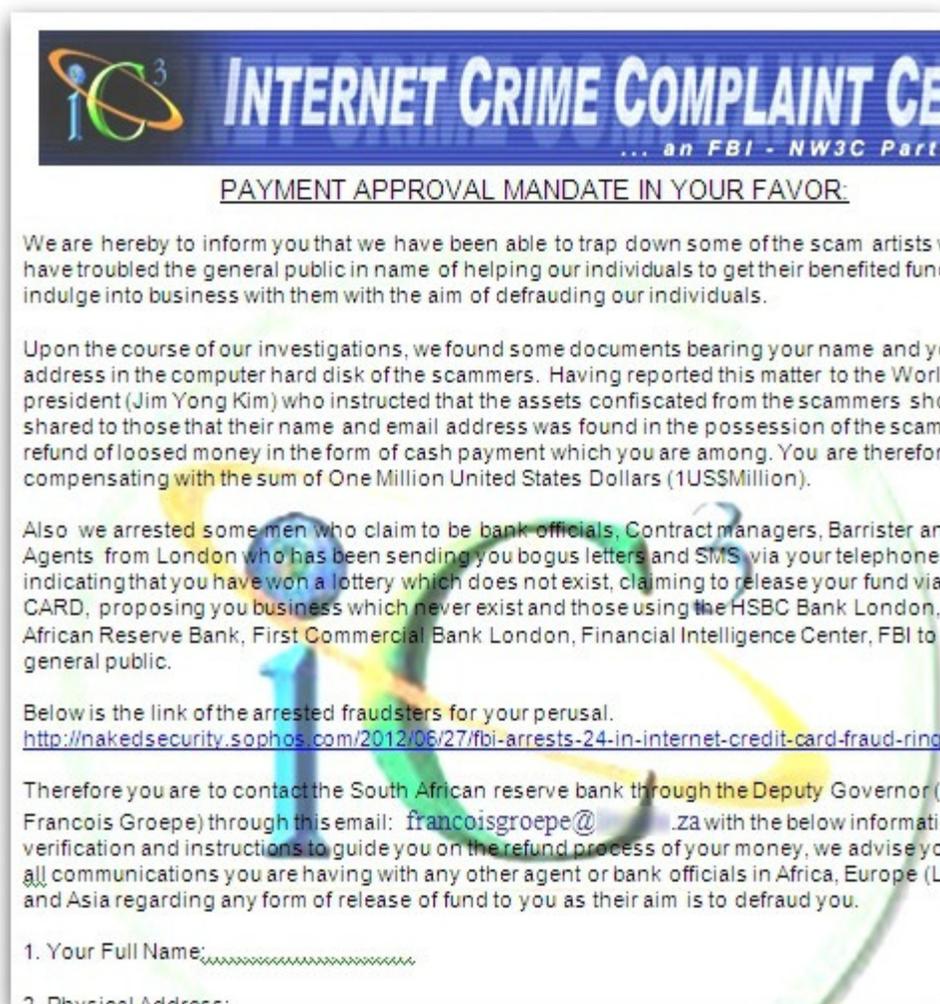
## **A MILLION DOLLARS, THE INTERNET CRIME COMPLAINT CENTER AND NAKED SECURITY — THE INGREDIENTS FOR A SCAM**

[Naked Security](#) released the following article on November 7, 2012.

An email scam is using a Naked Security news story about the arrest of a gang of suspected credit card fraudsters, in an attempt to scam innocent internet users.

The scam emails have the subject line "We have mandated your payment, kindly view below attachment", and claim to come from the Internet Crime Complaint Center (IC3).

Attached to the emails is a file (`DETAILS.doc`) which presents itself as an official communication from the IC3, explaining that criminal proceeds have been confiscated from scammers, and as the recipient's name and email address was found in the criminals' possession one million dollars in compensation is available.



Part of the Word document, which uses the genuine IC3 logo, reads as follows:

We are hereby to inform you that we have been able to trap down some of the scam artists which have troubled the general public in name of helping our individuals to get their benefited fund or to indulge into business with them with the aim of defrauding our individuals.

Upon the course of our investigations, we found some documents bearing your name and your email address in the computer hard disk of the scammers. Having reported this matter to the World Bank president (Jim Yong Kim) who instructed that the assets confiscated from the scammers should be shared to those that their name and email address was found in the possession of the scam artists as refund of loosed money in the form of cash payment which you are among. You are therefore to be compensating with the sum of One Million United States Dollars (1US\$Million).

Also we arrested some men who claim to be bank officials, Contract managers, Barrister and Lottery Agents from London who has been sending you bogus letters and SMS via your telephone numbers indicating that you have won a lottery which does not exist, claiming to release your fund via ATM CARD, proposing you business which never exist and those using the HSBC Bank London, South African Reserve Bank, First Commercial Bank London, Financial Intelligence Center, FBI to scam the general public.

The email then goes on to request that the recipient send over their name, address and

phone number to an email address, allegedly belonging to the deputy governor of a South African bank.

It doesn't take a super-sleuth to realise that this is going to end up as a 419 scam, with the potential victim encouraged to pay a logistical fee in advance for the release of the funds. In short, anyone who falls for the ruse is going to end up out of pocket.

What caught our eye, however, was the news story link that the scammers are using to give credence to their story that funds are available after the capture of cybercriminals.



Yes, it points to a Naked Security story from earlier this year about [an FBI arrest of 24 people](#) in a suspected credit card fraud ring.

I guess we should be flattered..

Don't forget — just because you think it's unlikely that anyone would ever fall for an email scam like this, doesn't mean they don't succeed. There are people out there who are vulnerable or elderly who could be tricked into believing that the offer is real — and end up losing a lot of money as a result.

---

For more information regarding online scams visit our Press Room page for the most current Public Service Announcements. <http://www.ic3.gov/media/default.aspx>