# INTERNET CRIME COMPLAINT CENTER'S (IC3)
# SCAM ALERTS
# MAY 2, 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.

## SEXTORTION SCAM

The IC3 has received numerous +complaints over the last couple of years regarding an online sextortion scam capitalizing on social media websites and technology. Contact between the subject and victim is initiated via social media websites and/or online dating websites. Once rapport has been established, victims are asked to engage in video chat where they are enticed to expose themselves in sexually compromising situations, while their images are secretly recorded. Subjects then threaten to make the videos available to all the victims' social networking friends and other online contacts unless funds, ranging in the amounts of $50 to $300, are wired to various destinations overseas.

---

## INCREASE IN ONLINE FRAUDULENT GUN SALES

Criminals capitalize on current events highlighted by the media, especially when the topic draws a significant amount of attention. The IC3 often sees evidence of this via complaints. One topic in particular that has continued to receive national attention is gun legislation reform. As a result, gun sales have skyrocketed. Consumers are not only purchasing firearms in stores, but online as well. The IC3 has seen an uptick in the number of complaints recently filed reporting fraudulent advertisements for firearms. Criminals entice victims into purchasing the firearms by using photos and descriptions hijacked from online firearm ads and advertise the firearms for below market value. The majority of the type of firearm that victims were attempting to purchase was a long gun.

In order to convince the buyer the transaction is legitimate, the criminal sometimes provides the victim a copy of a military photo ID via email, which they claim is theirs. Criminals also appear to know the procedures of transferring firearms by arranging for the firearm to be delivered to the victim's local Federal Firearm Licensee (FFL). Many of the complainants fell for the scam, losing hundreds to over a thousand dollars in each transaction.

---

## UNAUTHORIZED BANK ACCOUNT ACCESS IN THE PAYDAY LOAN SCAM

The payday loan scam involving threats and TDoS attacks was highlighted in the February 21, 2012 Public Service Announcement titled "New Variation On Telephone Collection Scam Related To Delinquent PayDay Loans" and in the January 7, 2013 IC3 Scam Alerts.

Based on IC3 complaint information, it appears the tactics used by the subjects continue to evolve. Information revealed subjects are now making unauthorized deposits for payday loans into victims' bank accounts. The proceeds range from $200 to $300. After the initial deposit, victims reported unauthorized withdrawals every two weeks in increments between $60 and $90. The withdrawals are applied to accrued interest only, making it impossible to pay the loan in full. Victims reported all efforts to return the unwanted loan proceeds or pay the loan in full were unsuccessful. Some reported closing their bank account and holding the loan proceeds to prevent further fraud to their account. It has yet to be determined how the subjects are obtaining the victims' bank account information, because some of the victims claim they have never applied for a payday loan.

---

## FAKE EMAILS FROM HSBC WITH ATTACHED PAYMENT_ADVICE.ZIP CONTAINS TROJAN

***MX Lab featured the following article on March 27, 2013***

MX Lab, started to intercept a new trojan distribution campaign by email with the subject "Payment Advice – Advice Ref:[B32454525694]". Please note that the numbers used in the subject and mail from may vary.

The email is sent from the spoofed address "payment.advice@hsbc.com.hk " and has the following body:

```
Sir/Madam
Upon your request, attached please find payment e-Advice for
your reference.
Yours faithfully
HSBC

*****************************************************************

We maintain strict security standards and procedures to prevent
unauthorised access to information about you. HSBC will never
contact you by e-mail or otherwise to ask you to validate
personal information such as your user ID, password, or account
numbers. If you receive such a request, please call our Direct
Financial Services hotline.
Please do not reply to this e-mail. Should you wish to contact
us, please send your e-mail to commercialbanking@hsbc.com.hk and
we will respond to you.
Note: it is important that you do not provide your account or
credit card numbers, or convey any confidential information or
banking instructions, in your reply mail.
Copyright. The Hongkong and Shanghai Banking Corporation Limited
2005. All rights reserved.

*****************************************************************
```

The attached ZIP file has the name Payment_Advice.zip and contains the 96 kB large file Payment_Advice.exe.

The trojan is known as W32/Trojan.IWRE-9169, PWS.Win32.Fareit.AMN (A), W32/Yakes.B!tr, Trojan.Agent.RVGen5.

At the time of writing, 11 of the 46 AV engines did detect the trojan at Virus Total. Virus Total and SHA256:

ea92af5486f6b8039b0f2193666ea8604d54d5cc9e7f37f7396a8b6f2baa3260.

---

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