INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS

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.

SOCIAL NETWORK MISSPELLING SCAM

During December 2010, the IC3 discovered misspellings of a social network site being used as a social engineering ploy. Misspelling the domain name of this site would redirect users to websites coded to look similar to the actual website. The website users were redirected to answer three or four simple survey questions. Upon answering those questions, users were offered a choice of three free gifts. Multiple brands were observed as being offered as gifts, including gift cards to retail stores and various brands of laptops.

After clicking on one of the gifts, users were further redirected to other websites claiming to give free gifts for completing surveys. The surveys typically asked for name, address, phone number, and e-mail address. A user could spend hours filling out multiple surveys and never receive any of the gifts advertised.

FAKE ONLINE RECEIPT GENERATOR TARGETS UNSUSPECTING ONLINE MARKETPLACE MERCHANT

A new scam aims to swindle online marketplace sellers by generating fake receipts. This Receipt Generator is an executable file that has been circulating on hacking forums recently. This is a particularly interesting scam - because it does not target regular PC users, it targets the sellers on online marketplace websites. This is what the would-be social engineer sees when running the program:

The social engineer can fill in a variety of information, including item name, price, and the date the order was taken. Additionally, it allows them to choose between the .com, .co.uk, .fr, and .ca marketplace portals. When they hit "Generate," an HTML file is created in the program folder which looks like this:

The program produces what appears to be a genuine marketplace receipt and a copy of the "Printable Order Summary," similar to the documents resulting from legitimate marketplace purchases. Note the small details, such as "Total before tax," "Sales tax," and other particulars that make the receipt convincing.

Many sellers on these markets will ask the buyer to send them a copy of the receipt should the buyer run into trouble, have orders go missing, lose the license key for a piece of software, and so on. The scammer relies on the seller to accept the printout at face value without checking the details. After all, how many sellers would be aware someone went to the trouble of creating a fake receipt generator?

Sellers must remain ever vigilant about this scam, which has been a popular topic in recent hacker forums. The VirusTotal detection rate is currently 1/43 – detected as Hacktool.Win32.Amagen.A.

MALICIOUS CODE IN .GOV E-MAIL

A recent malware campaign, disguised as a holiday greeting from the White House, targeted government employees. The recipient received the below e-mail with links to what masqueraded as a greeting card, but when they clicked on the link, it attempted to download a file named "card.exe." The executable program proved to be an information-stealing Trojan, which would disable the recipient's computer security notifications, software updates, and firewall settings. The malware also installed itself into the computer's registry, enabling the code to be executed every time the computer was rebooted. At the time of review, this particular malicious code sample had a low antivirus detection rate of 20%, with only 9 out of 43 antivirus companies reporting detection.

```
From: sender@whitehouse.gov [mailto: sender@whitehouse.gov]
Sent: Wednesday, December 22, 2010 10:33 PM
To: recipient's name
Subject: Merry Christmas, recipient's name

Recipient's name here,

As you and your families gather to celebrate the holidays, we
wanted to take a moment to send you our greetings. Be sure that
we're profoundly grateful for your dedication to duty and wish
you inspiration and success in fulfillment of our core mission.

Greeting card:

hxxp://xtremedefenceforce.com/card/
hxxp://elvis.com.au/card/

Merry Christmas!


_____
Executive Office of the President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500
```

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