INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
MARCH 27, 2012

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.

FRAUDULENT UTILITY BILL E-MAIL

The IC3 has received over 40 complaints since May 2011 reporting the receipt of an unsolicited e-mail purportedly from a specified utility company. The e-mail stated the recipient had a new bill which needed to be paid, and the bill was attached to the e-mail. The recipient was instructed to click on the attachment to view their bill. The attachment contained a zip file with a computer virus.

The e-mail concluded by stating the recipient received the e-mail message, because he/she receives e-bills from this utility company. Many of the recipients are located in areas of the United States that do not use this utility company as their electric provider.

BUSINESSES TARGETED WITH E-MAIL PURPORTEDLY FROM THE BETTER BUSINESS BUREAU (BBB)

The IC3 has received several complaints from businesses regarding an e-mail, purportedly from the BBB, which states the BBB has received a complaint from a customer regarding their business. The recipient is asked to review the complaint attached to the e-mail and respond to the BBB. The file attached to the e-mail contains a virus.

In one complaint received by the IC3, a business claimed their computer was infected with a virus after opening the attachment in the e-mail they received. As a result, the business lost nearly $100,000 when fraudsters successfully wired money from the company's bank account after the virus enabled them to capture passwords and other important banking information.

The BBB posted the following alert on December 7, 2011.
http://www.bbb.org/us/article/alert-malicious-complaint-email-claiming-its-from-bbb-30916

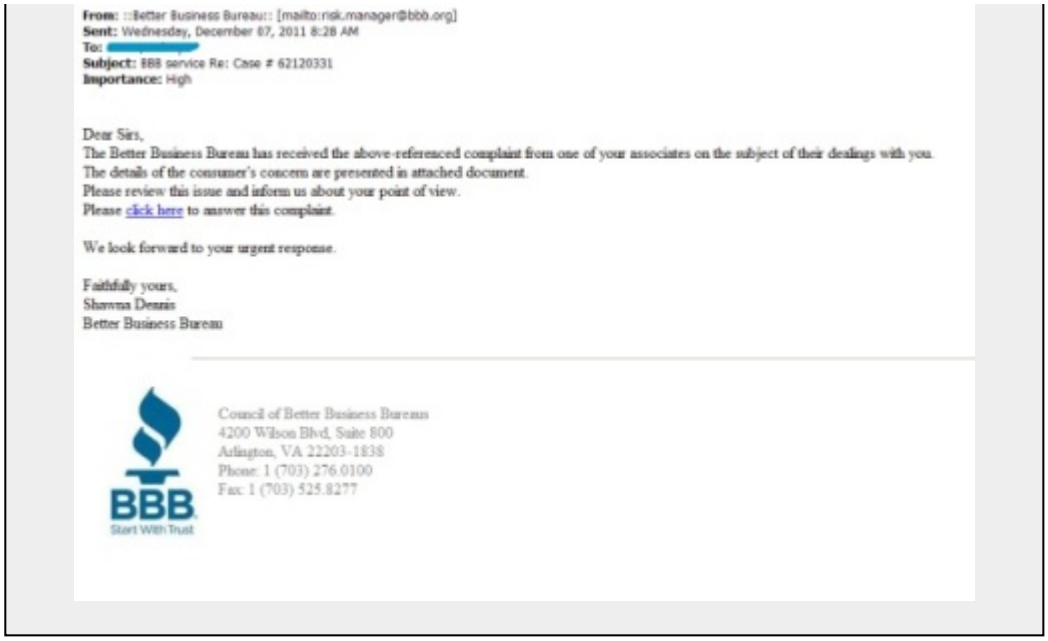
ALERT
Malicious Complaint E-mail Claiming It's From BBB

Better Business Bureau is issuing an urgent SCAM alert cautioning businesses and consumers about an email that looks like it is from BBB, with the subject line "Complaint from your customers." This e-mail is fraudulent; ignore its contents and delete it immediately. If you have already clicked on a link in the e-mail, run a full virus scan of your computer.

The e-mails have return addresses that BBB does not use (one example is riskmanager@bbb.org) and it is signed with the address of the Council of Better Business Bureaus, the national office of the BBB system. The e-mail contains a link to a non-BBB web site. Do NOT click on the link.

BBB is working with law enforcement to determine its source and stop the fraudulent campaign.

This is what the email looks like:



From: ::Better Business Bureau:: [mailto:risk.manager@bbb.org]
Sent: Wednesday, December 07, 2011 8:28 AM
To: [redacted]
Subject: BBB service Re: Case # 62120331
Importance: High

Dear Sirs,
The Better Business Bureau has received the above-referenced complaint from one of your associates on the subject of their dealings with you.
The details of the consumer's concern are presented in attached document.
Please review this issue and inform us about your point of view.
Please click here to answer this complaint.

We look forward to your urgent response.

Faithfully yours,
Shawna Dennis
Better Business Bureau

Council of Better Business Bureaus
4200 Wilson Blvd, Suite 800
Arlington, VA 22203-1838
Phone: 1 (703) 276.0100
Fax: 1 (703) 525.8277

BBB
Start With Trust

MOVING COMPANY SCAMS

The IC3 continues to receive complaints regarding moving company scams. The complaints received at the IC3 do not appear to be linked to each other. There are many individuals who take advantage of those posting moving services on-line, receive an estimate for the service, and hire the company. Scams include the company showing up, and the estimate suddenly doubles or additional fees are added; the counterfeit check scheme, where the victim is selling an item on-line, and the buyer claims a moving company has been hired to pick up the merchandise, and the buyer pays for the merchandise with a check written for more than the price of the merchandise; and after loading and driving away with the customer's property, the moving company later calls to inform the customer they must pay more if they want to see their belongings again, basically holding the property hostage. Often, even after paying the additional costs, deliveries were late and many of the customers' items were damaged or missing. Those who refused to pay the additional cost were told they would not receive a refund or their belongings.

BROWSER BOT INFECTION

What happens when your web browser becomes the "bot?" A look at a current Trojan infection campaign similar to the infamous Zeus malware makes open source web browser users a bit nervous.

The open source browser can now function like a bot and accept commands. It can process the content of the current page where it is located, redirect the user, halt the loading of particular pages, steal passwords, run executables, and even kill itself. Unfortunately, the kill function is a bit excessive and deletes critical system files, which in turn prevents users from logging in properly.

The way it builds the malicious code into the open source browser is notable, because it uses the design of the browser against itself. In the past, researchers have seen threats create malicious extensions. Users would have to disable that particular add-on, which would eradicate the threat. For this particular piece of malware, this is not the case. Since it is a component, it does not appear as an add-on in the browser's Add-ons Manager in the same manner other extensions and plugins appear. Furthermore, due to the design of the open source browser, the Trojan will be reinstalled every time the browser establishes a connection to the Internet.

HTML ATTACHMENTS USED TO SPREAD MALWARE

In the last month, security researchers have observed several large spam campaigns with malicious HTML attachments. A 2007 botnet is believed to be behind the spike in these attacks. Traditionally, HTML-based attachments were used for phishing attacks to entice HTML

victim to the desired spoofed web page. This current attack vector uses the HTML attachment with malicious javascript to redirect victims to the exploit kit. The exploit kit will then scan the target machine for vulnerabilities that can be exploited to install an information-stealing Trojan.

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