INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS
JULY 14, 2011

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.

DDOS ATTACKS — RISING TREND

Distributed denial of service attacks (DDoS) attacks in general are on the rise. One reason may be due to the availability of software tools like LOIC, Slow Loris and BE botnet, which allow anybody to participate in a distributed attack.

Gaming sites in particular have come under attack by multiple hacking groups. Open source of intelligence indicates that some of the attacks are supposedly in response to the company itself, while other attacks are in response to group rivalries.

It appears that social engineering of followers of some of these media-driven hacking groups have influenced others in participating in the attacks thus adding to the intensity of these DDoS attempts.

It is also worthy to note that some DDoS attacks have been used to distract the organization from other criminal activity. One group will cause the traffic disruption, while the others attempt to compromise servers and exfiltrate data.

The IC3 continues to receive complaints reporting DDoS attacks, often to smaller e-commerce based businesses. One reported attack was DNS based. The company reportedly had 165 million hits over a three-day period, which overloaded their network and crashed their site. They stated their web hosting company attempted multiple solutions over the course of the attack, which lasted approximately ten days.

Another reportedly exhausted every avenue available to combat an attack to their site, but was unable to stop it because of the overwhelming intensity. They reported the attack mainly concentrated on the Internet banking services segment of the site, and the attackers were not successful in penetrating the network, gaining access to any internal function. However, the attackers inundated the incoming communication lines with more than 8,000 hits per second to the bank's login screen, eliminating access to the bank by its clients.

The following are more examples of DDoS attacks reported to IC3:

- Subjects orchestrated a DDoS attack on a server used by a company to host servers for online games. Once the company addressed the attack, the fraudsters then hosted another attack on a different IP.
- Three DDoS attacks in one week targeted a company, hitting them with high volume of traffic, which saturated the uplinks of one of their Internet Service Providers.
- For more than 20 days in May 2011, a business's network and video game had been under DDoS attacks. The attacks targeted their master servers controlling access to all game servers and player logins. Through research, the company believed the attacker was in the United Kingdom and had also been extorting and threatening other individuals and committing credit card fraud. The company reported that their loss of revenue was approximately $50,000.
- Since March 2011, one company has filed six IC3 complaints, reporting multiple attacks. The most recent were two brute force attacks in May 2011 to their File Transfer Protocol (FTP) server using a non-existent user name and various passwords.
- Another company's site was recently attacked on two occasions. The attacker reportedly used at least 1,000 unique IPs to crash it.

EXTORTION EMAILS TARGETING PHYSICIANS

Since March 5, 2011, the IC3 has received over 50 complaints reporting extortion emails targeting professionals, mainly physicians. Victims were told complaints had been filed against them and posted online, claiming they were facing prison for sexual indecency. Also posted were the victims' names, addresses, telephone numbers, and email addresses. The victims were told "these types of comments will destroy your reputation and are permanently archived on search engine sites; you will lose thousands of dollars in revenue with a bad reputation." Victims were also told the sender could "convince the people who posted the comments to remove them"; however, the removal fee was $250 USD.

The IC3 also received complaints from individuals residing in Asia who claimed they were hired to write complaints, collect "complaint reports," and add them to website. Individuals reported that the subject also had job ads posted on Asian online classified job sites looking for writers for the website.

The complainants claimed they were promised $10 USD for each post on a weekly basis via an online payment service or check/money order. One reportedly did 150 posts in one week; however, the subject neither paid the complainants nor responded to their emails.

Workers also stated that the subject uses various aliases and hired another company, which they believe he owns, to remove the complaints.

SCAMS PROMISING LARGE WINNINGS AND THREATS IF VICTIMS DO NOT COMPLY

The IC3 has received numerous complaints advising of a spam email attachment circulating, which claimed to be from the FBI. The email appeared to be the typical Nigerian 419 type scam; however, this most recent attempt contained the FBI seal and the Economic and Financial Crimes Commission (EFCC) logo at the top, making it appear official.

The letter instructs the recipient to contact the EFCC in Lagos, Nigeria, at the email address provided to obtain "clearance documents" and asks that the recipient provide their full name, address, and telephone/cell number. Several different names, email addresses, and mailing addresses are used in this email scam, but the content of the letter remains consistent throughout.

The letter threatened that, if the recipient does not contact the EFCC immediately, Director Mueller "will have an agent come visit you at home for questioning." The letter emphasized the need to send $250 for issuing the clearance document, and then $1.5 million would be released to the individual. The letter attempted to coerce recipients into cooperating by advising that "failure to provide the above requirement in the next 24 hours, legal action will be taken immediately by arresting and detaining you." The letter was signed, "Faithfully Yours, Robert S. Mueller III, FBI Director." In addition, the letter contained cc's at the bottom to various agencies including the Supreme Court of the United States, U.S. Courts of Appeals, and U.S. District and Circuit Courts.

The social engineering technique of utilizing the FBI's name helps fraudsters intimidate, impress, and convince the recipient that the emails are legitimate. Several Public Service Announcements (PSA) have been posted on the www.fbi.gov, www.lookstoogoodtobetrue.com, and www.ic3.gov websites related to these types of schemes.

To view the letter, please refer to the appendix.

EMAIL IMPERSONATING THE FBI CONTAINING A TROJAN

Another fraudulent email campaign has begun claiming to be from the FBI telling recipients they have visited 40 illegal websites. The IC3 issued warnings about these particular email campaigns in 2005 and 2006 by releasing three PSAs on February 23, 2005, November 22, 2005, and July 24, 2006. The fraudulent email mentioned in the first PSA claimed the FBI logged the recipient's IP address on more than 40 illegal websites. The next two PSAs mentioned the emails that claimed the FBI logged the recipient's IP address on more than 30

illegal websites. All the emails instructed the recipient to answer questions in the attachment, which contained malware.

The PSA from February 23, 2005 stated the FBI has become aware of spam email fraudulently claiming to be from fbi.gov accounts. The email appeared to be sent from the email addresses of police@fbi.gov, fbi@fbi.gov, officer@fbi.gov, and web@fbi.gov. The recipients were told the FBI had logged their IP addresses on more than 40 illegal sites. The email instructed them to answer questions in the attachment, which contained a W32.Sober.K@mm worm.

In 2005, the IC3 began seeing complaints reporting fraudulent emails purportedly from the FBI claiming the recipient went to more than 30 illegal sites. The IC3 received over 5,300 related complaints in that year alone. The number of related complaints drastically dropped the following year to approximately 130 complaints. After 2006, the IC3 has only received two related complaints, one in 2007 and one in 2008.

Also in 2005, the IC3 began seeing complaints reporting fraudulent emails purportedly from the FBI claiming the recipient went to more than 40 illegal sites. That year, a total of approximately 1,600 related complaints were filed. No other complaints were reported until the beginning of this year, with more than 300 so far being filed.

As in the earlier email versions mentioned above, fraudsters are still using spoofed email addresses with an fbi.gov email extension. Recipients are still being told the FBI has logged their IP address on more than 40 illegal sites, and they need to answer the questions in the attachment, which contains malware.

THREATENING IC3 IMPERSONATION CALLS

The IC3 has received thousands of complaints pertaining to payday loan scams; however, recently some of the callers have claimed to be with the IC3. Recipients described the callers as "very nasty and could barely speak English." Victims were told a complaint had been filed against them regarding a payday loan and they must repay the loan as soon as possible to avoid court and jail time. The amount of the loans vary, but average around $600.

Other complainants reported that the caller claimed to be from the Attorney General's office and told the recipient they were being sued by the IC3 and private detectives for not repaying a payday loan.

In both scenarios, the caller had the recipient's social security account number and bank information. Some recipients reported that the checking account number was incorrect. Others reported receiving calls from individuals claiming to be "officers" with the IC3. Recipients reported being told they were being investigated and were threatened by claims that information would be used against them in court proceedings, but they did not provide any additional details about the calls. These callers were described as having an Indian accent, called the recipients multiple times, and used various names.

INCREASE IN ECOMMERCE FRAUD

A company who serves as a data sharing platform for merchants to stop on-line fraud, recently provided IC3 with the below information describing how there has been an increase in fraud attempts incurred by on-line merchants.

Since mid-March, merchants have experienced a serious increase in fraud attempts. The following four theories were studied and considered as explanations to the increased attempted fraud. The nature of the fraud attempts was that criminals had the complete identity information: name, address, email address, and IP address of the consumer.

- Theory One – "Stolen Data" – one of the recent major data breaches included credit card numbers, and the fraudsters are using the data.

  This theory is the least likely, because the fraudsters who attempted these attacks have more details than were included in the data breaches.

- Theory Two – "Spear Phishing" – a major recent data breach that compromised email accounts is being used by the criminals to target consumers with really good phishing emails, referred to as spear phishing. The fraudster knows the consumer conducts business with a specific company. The fraudster creates a targeted email from the company who conducts business with the consumer, and is able to collect enough information to compromise the consumer.

  To study this theory, the Anti-Phishing Working Group's (APWG) phishing map was researched. In the past 12 months, phishing in the U.S. was at a rate of 38%, and in the past 90 days, the site reports phishing attacks at 51.33%, which is a significant increase.

  While phishing may be a contributor to the increase in fraud attempts, this theory has been declined, because with phishing information, when eCommerce orders are placed, there is some degree of inaccurate information, and the information is often "tested."

- Theory Three – "Malware" – malware has spread and become more vicious. While the malware is more vicious, an impact on eCommerce has yet to be determined; although it may come in the future. Additionally, according to data on the APWG's website, malware for the past 12 months in the U.S. was 35.85%, and in the past 90 days was reported to be 25.48%. Based on these numbers, malware attacks are actually down according to the website.

  A study was conducted with merchants participating in a program associated with the data sharing platform company. No link was found in confirmed fraud from merchants and malware tools or any other recognizable pattern.

- Theory Four – "Fake eCommerce Donation Sites" – After researching this theory, it is believed the increase in fraud attacks is tied to fake donation sites that took advantage of the earthquakes and Tsunami in Japan. This belief is supported because the fraudsters have the exact information on the data elements for making purchases, and the accuracy rate is very good. Therefore, it is most likely the data is being collected from fraudulent sites that took donations from the devastating earthquakes and Tsunami in Japan. It is believed the fraudsters used social networks to promote the donation sites to expand their reach farther and faster than has been viewed in previous years.

  The timing is exactly right; other major tragedies have been viewed as the cause to increased fraud spikes – such as Hurricane Katrina. In fact, fake donation sites were such a problem for Katrina, the National Center for Disaster Fraud (NCDF) was originally established by the Department of Justice to investigate, prosecute, and deter fraud in the wake of Hurricane Katrina. Its mission has expanded to include suspected fraud from any natural or man-made disaster. More than 20 federal agencies, including the FBI, participate in the NCDF, allowing it to act as a centralized clearinghouse for information related to relief fraud.

  After the Tsunami in Japan, we immediately saw fraudulent donation sites and organizations. LooksToGoodToBeTrue.com and the IC3 posted consumer advisories on March 11, 2011 to advise the public about rogue websites that fraudulently seek charitable donations.

  According to a Websense threat report, "following the disasters in Japan, cybercriminals tried to utilize every possible underground technique to benefit from this occurrence. Apart from already known vectors such as phishing and malicious spam emails, criminals used Viral Facebook applications."

APPENDIX:

Screen shot of FBI and EFCC Letter:

FBI Headquarter in Washington, D.C.
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue,
NW Washington, D.C. 20535-0001

EFCC Headquarter in Lagos.
Economic and Financial Crimes Commission
15A, Awolowo Road, Ikoyi, Lagos,
Nigeria, 23401.

REF: US/29028/BA28/11

Attention:

BENEFICIARY,

You are to contact the ECONOMIC AND FINANCIAL CRIME COMMISSION (EFCC) Lagos, Nigeria to obtain the Clearance Documents, find below their contact information's:

Contact Person: Mr. Adewale Philbert

PRINCIPAL STAFF OFFICER ECONOMIC AND FINANCIAL CRIME COMMISSION (EFCC)

Mr. Philbert's Email: adewalephil@blumail.org

Lagos Office Address 15A Awolowo Road, Ikoyi, Lagos Nigeria

Ensure you contact them (EFCC) with your Full Name, Address and phone number/cell number.

Contact the EFCC via Email with the information above immediately, once you contact them i will get back to you or else i will have an agent come visit you at home for questioning.

Furthermore, be advised that according to the United State Law together with the FBI rules and regulations, you are to obtain the document from the EFCC of Lagos Nigeria where the funds were transferred from. Also Note that you are to take care of the cost of the Document, which will be issued in your name. Due to the content of the document and how important and secured the document is, you as the beneficiary will send to the EFCC of NIGERIA the sum of USD250 Dollars only for the issuing of the document right away and your USD1.5 Million will be released to you, that is the lay down rules for EFCC of NIGERIA to release such sensitive document, EFCC will issue you the authentic and original copy of the documents with seal on it for verification and approval.

You are here by advised to contact them through the email address above to make an enquiry concerning how you will send the official fee to them. Note that you are to observe this immediately, if you really want your funds to be credited to your personal bank account and to avoid any legal battle with the security operatives over this matter. We have already informed the EFCC of NIGERIA about the present situation, go ahead and contact them immediately. Your fund is under our custody and will not be released to you unless the required document is confirmed; after that, the fund will be released to you immediately without any delay.

NOTE: We have asked for the above document to make available the most completed and up-to-date records possible for no criminal justice purposes. The documents will clarify the intensity of this fund; exonerate it from money laundry, scam and terrorism.

WARNING: Failure to provide the above requirement in the next 24 hours, legal action will be taken immediately by arresting and detaining you as soon as international court of justice issues a warrant of arrest, if you are found guilty, you will be jailed as terrorism, drug trafficking and money laundering is a serious problem in our community today and the world at large. The F.B.I will not stop at any length in tracking down and prosecuting any criminal who indulges in this criminal act. FORWARD THE DOCUMENT TO US VIA EMAIL ATTACHMENT AS SOON AS YOU OBTAIN IT. Nobody is above the law and the law is not a respecter of anybody. We presumed you are law abiding citizen whom would not want have scuffles with the authority, in and outside America.

We are charged with the responsibility of implementing legal norms and our authority is irrevocable so do not dare dispute our instruction, just act as instructed. The person you know will not help you in this matter rather abide by this instruction. The funds in question were deposited by those people that contacted you.

Note: You are to contact EFCC with your full names, phone number/cell number and full address via their email stated above immediately for the processing of your Clearance Documents within the next 48 hours.

Faithfully Yours.
Robert S. Mueller III
FBI Director

Note contact the EFCC office: adewalephil@blumail.org

You have less than 24 hours to contact them.

CC. TO:
Supreme Court of the United States
U.S. Courts of Appeals
U.S. District Courts
U.S. Circuit Courts
Courts of Special Jurisdiction:
Bankruptcy Courts
Court of Claims, 1855 - 1982
U.S. Court of Federal Claims, 1982 -
Customs Court, 1890 - 1980
U.S. Court of Customs and Patent Appeals, 1910 - 1982
U.S. Court of International Trade, 1980 -
Commerce Court, 1910 - 1913
Territorial Courts
Courts of the District of Columbia
Temporary Emergency Court of Appeals
Judicial Panel on Multi-District Litigation
Foreign Intelligence Surveillance Court
Federal Courts Outside the Judiciary

ROBERT MUELLER
Director - **FBI.**

NSB SEAL ABOVE