INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS APRIL 20, 2012

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

INVESTMENT SCAM

The IC3 continues to receive complaints involving subjects who have obtained the names and social security numbers of individuals for illegal purposes. Subjects use the information to defraud the U.S. government by electronically submitting a fraudulent tax return for a hefty refund. The prevalence of such complaints mirrors the recent surge in tax fraud cases involving identity theft.

Investment fraud is another scheme with an Internal Revenue Service (IRS) nexus, on which the IC3 has received complaints. Subjects are incorporating the use of bogus IRS documents to perpetrate this scheme. One example of how subjects are using bogus IRS documents to commit investment fraud and steal victims' identities is by the subjects posing as a tax consulting firm. The subjects engage potential victims via telephone and attempt to convince them to sell their underperforming shares in a company. The potential victim is advised to sell their corporate shares, applicable taxes must be paid. Some of the victims were also advised they had to buy other certain shares with their profit. Documents such as share certificates and invoices for federal and state taxes were exchanged via e-mail. After the funds were wired, the subjects became unresponsive to the victim's inquiries. An open source search also revealed multiple complaints concerning this scheme. It is unknown at this time how the subjects obtained knowledge that the victims actually owned underperforming stocks.

The loss amounts tend to be much higher with investment fraud complaints than in regular identity theft complaints.

BLACKHOLE EXPLOIT KIT 1.2.3 RELEASED

Blackhole is currently the most widely purchased exploit pack in the underground market. An exploit pack is a software toolkit that is injected into malicious and/or compromised websites, allowing the attacker to push a variety of exploits targeting vulnerabilities of popular applications like Java and Flash.

On March 25, 2012, the Blackhole Exploit Kit 1.2.3 was released. This kit included the latest critical vulnerability in Java, allowing the bypassing of Java's sandbox environment. Java's sandbox is designed to provide security for downloading and running Java applications, while preventing them access to the hard drive or network. New malware samples appearing in the wild have been highly successful at exploiting this flaw. It is estimated at least 60% of Java users have not yet patched against this latest flaw, *CVE-2012-0507*.

The table below illustrates the number of vulnerabilities loaded by type and the overall percentage:

EXPLOITS	LOADS	PERCENT OF TOTAL	
Java Array	14,982	82.94	
PDF LIBTIFF	1,960	10.85	
PDF ALL	681	3.77	
HCP	173	0.96	

EXPLOITS	LOADS	PERCENT OF TOTAL	
MDAC	141	0.78	
Flash	126	0.70	

TERMINATION OF YOUR CERTIFIED PUBLIC ACCOUNTANT (CPA) LICENSE SPAM CAMPAIGN CONTAINING MALWARE

Recently, unsolicited e-mails titled "[BULK] Termination of your CPA license" have been sent to numerous IC3 e-mail accounts. One example of the many e-mail addresses used was support@aicpa.org. The IC3 has also received complaints reporting this spam campaign.

The e-mails were purportedly from The American Institute of Certified Public Accountants concerning a complaint filed against the recipient for filing fraudulent tax refunds for their clients. A link was provided for the recipient to view the complaint. Recipients were advised to provide feedback within a specific period of time and threatened with possible termination of their accountant licenses if they failed to do so.

Analysis conducted by an IC3 Information Technology Specialist found the e-mails were pushing out a Blackhole exploit kit containing a Trojan redirector. It was also determined that the IP addresses used in this campaign have been involved in large volumes of DDoS activity from the same botnet and appear to have originated from Brazil.

WANT TO GET PAID TO DRIVE YOUR OWN CAR?

Several complainants reported a scam to the IC3 involving the advertising of a company's logo on their personal vehicle while they go about their normal daily routine. Although legitimate offers exist, those scammed reported to the IC3 that initial contact with the subject was mostly through online ad postings. The posting offered an easy way to earn extra income by allowing businesses to advertise their logo on the complainant's personal vehicle through a vinyl decal or "auto wrap." The fraudsters were using company names such as Coca Cola, Monster Energy drink, Carlsberg beer, Heineken Co., and Red Bull.

Individuals were advised they would be paid an average of $400-$600 per week in exchange for driving around with vinyl advertising signs wrapped around their vehicle. Those interested in participating were asked to provide their contact information and vehicle details. They were promised an up-front payment, which would be sent by check or money order.

The employment offer was, of course, entirely bogus. Those who fell for the scam received a check or money order for more than the promised amount. They were directed to cash it and wire the difference to a third party, who was supposed to be the graphics designer to pay for the cost of the design. The checks and money orders turned out to counterfeit and the criminals, once again, were able to convert fraudulent checks and money orders into untraceable cash, leaving the victim responsible for the bank's losses.

ONLINE PROPERTY RENTAL SCENARIOS

The IC3 continues to receive complaints regarding rental property scams from victims and real estate agencies. Several real estate agencies reported that their listings are being duplicated to perpetrate fraudulent online postings. These postings have been damaging to their companies reputations. These complaints make it evident that there are many who capitalize on people are looking to rent property and attempt to take advantage of those individuals, especially when they are in pressing situations in which they need to find a residence within a short amount of time.

Below are some scenarios of the scheme recently reported to the IC3:

- A fraudster posted rental property online. When the prospective renter inquired about the property via e-mail, the fraudster requested detailed personal information, as well as a security deposit of $1000 to hold the home. Payment, in the form of a money order, was requested because of the "online scams." After the deposit was received, the fraudster claimed that he mailed the keys and lease agreement for a hard copy to be signed. Later, the victim received an e-mail from an individual posing as the fraudster's "lawyer" stating a hold had been placed on the package containing the key until the full amount of the first and last month's rent is paid. The victim realized it was a scam after they contacted the realtor who advised the home had been foreclosed.

- Another victim also responded via e-mail to an online post advertising a house for rent. The victim was asked to submit an online credit report. The fraudster then provided a link in his e-mail, allowing the victim’s credit report information to be directly accessible to him.
- A complainant had inquired about a condo rental advertised online. The complainant was advised to go to the condo and call the fraudster so he could meet her with the keys. Upon placing the call, no one answered. Later, the fraudster provided the complainant an excuse for not being available and requested the deposit be made through an online payment service. After the deposit was made, the complainant realized it was a scam and contacted the online payment service. Upon an investigation, the receiver of the deposit advised they had been defrauded as well and was only acting as the "pay agent" for the true fraudster.

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