INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
JUNE 27, 2014

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.

BUSINESS E-MAIL COMPROMISE

For more than a year, the IC3 has been receiving complaints from businesses that were contacted fraudulently via legitimate suppliers' e-mail accounts. Recipients were asked to change the wire transfer payment of invoices. Businesses became aware of the scheme after the legitimate supplier delivered the merchandise and requested payment. This scam has been referred to as the "man-in-the-email scam." However, it was recently renamed the "business e-mail compromise."

A twist to this scam that is being reported pertains to the spoofed business e-mail accounts requesting unauthorized wire transfers. In the scheme, a business partner, usually chief technology officers, chief financial officers, or comptrollers, receives an e-mail via their business accounts purportedly from a vendor requesting a wire transfer to a designated bank account. The e-mails are spoofed by adding, removing, or subtly changing characters in the e-mail address that make it difficult to identify the perpetrator's e-mail address from the legitimate address. The scheme is usually not detected until the company's internal fraud detections alert victims to the request or company executives talk to each other to verify the transfer was made. The average dollar loss per victim is approximately $55,000. However, the IC3 has received complaints reporting losses that exceed $800,000.

Recently, the IC3 began receiving related complaints from companies that were alerted by their suppliers about spoofed e-mails received using the company's name to request quotes and/or orders for supplies and goods. These spoofed e-mails were sent to multiple suppliers at the same time. In some cases, the e-mails could be linked by Internet Protocol (IP) address to the original business e-mail compromise scams. Because this latest twist is relatively new, the dollar loss has not been significant. Also, victim companies have a greater chance of discovering the scheme because the e-mails go to multiple suppliers that often follow-up with the company.

Based on analysis of the complaints, the scam appears to be Nigerian-based. Complaints filed contain little information about the perpetrators. However, subject information that was provided has linked to names, telephone numbers, IP addresses and bank accounts reported in previous complaints, which were tied over the years to traditional Nigerian scams.

Some commonalities found among the complaints include:

> Victims are generally from the United States, England and Canada, although there have been complaints from other countries such as Belgium.
>
> Victim businesses often trade internationally, usually through China.
>
> Victim businesses that conduct high-dollar wire transfers, so requests for larger monetary amounts are not uncommon.
>
> Most, but not all, victims receive the fraudulent e-mail request through AOL, Gmail, or Hotmail addresses. A few companies have reported scammers were able to access the company's internal server.

Transactions were traced by the victim’s fraud department to mainly banks in China or Hong Kong. However, transactions with banks in South Africa, Turkey and Japan were also reported.

INCREASE IN FRAUDULENT TAX FILINGS

IC3 complaints reporting the fraudulent filing of victims' income taxes have doubled from 2013 to 2014. Complainants report their information was somehow compromised and used to file their taxes.

Some complainants reported that before filing their 2013 taxes, they were notified by the Internal Revenue Service (IRS) that they were being audited or under review. Others reported receiving a rejection notice from the IRS when they attempted to electronically file their taxes. They were told that someone else had already used their Social Security Number to file. These victims had to mail their tax returns into the IRS and file an identity theft report.

Some of the victims reported their information was also used to open several credit cards and lines of credit.

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