INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
JUNE 19, 2013

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.

TECH SUPPORT CALLS PURPORTEDLY FROM A WIRE TRANSFER COMPANY

The IC3 has recently received complaints from businesses regarding telephone calls from individuals claiming to be with a wire transfer company's tech support. One complainant reported that the wire transfer company's name was displayed on their caller ID. The callers instructed the victims to go to a particular website to run an application which allows the caller to remotely access the victim's computer. Once remote access was established, the victims were instructed to open their wire transfer program and log-in to their accounts, so the callers could update the system. The victims were then told to turn off their monitors, to avoid interference with the update. The victims later discovered the subjects made wire transfers to NetSpend accounts. One victim noticed something downloading onto his computer once the caller gained remote access. This made the victim suspicious, so he turned off his computer. Later, he discovered the caller had loaded $950 on a prepaid credit card from the victim's account. Another victim reported money transfers were made to various states and individuals, but the caller reassured the victim that no transfers were actually being processed. No other details were provided.

WEBSITES POSTING MUG SHOTS AND EXTORTION

The IC3 has received hundreds of complaints from individuals claiming they located their mug shots on 20 different websites, all of which allegedly use similar business practices. Some victims reported they were juveniles at the time of the arrests and their records were sealed. Therefore, their information should not be available to the public. Others stated the information posted on the sites was either incorrect or blatantly false.

Complainants who requested to have their mug shot removed, had to provide a copy of their driver's license, court record and other personal identifying information. However, providing such information puts those at risk for identify theft.

Complainants were also subject to paying a fee to have their mug shot removed. Although they paid the fee, some of the mug shots were not removed. If they were removed, the mug shots appeared on similar websites.

If the victim threatened to report the websites for unlawful practice, the websites' owners threatened to escalate the damaging information against the victim.

ATTACKERS USE SKYPE, OTHER IM APPS TO SPREAD LIFTOH TROJAN

SC Magazine featured the following article on June 1, 2013

Users receiving shortened URLs in Skype instant messages, or similar IM platforms, should be wary of a new trojan, called Liftoh.

So far, it has primarily infected users in Latin America, said Rodrigo Calvo, a researcher at Symantec.

When targeted, victims receive a message in Spanish containing a shortened URL. The messages appear as if they are coming from someone on the user's Skype contact list who is linking to a photo. If clicked, the link redirects users to 4shared.com, which is hosting a URL,

which initiates a weaponized zip file containing Liftoh. The trojan is capable of downloading additional malware.

The malicious URLs have been clicked on more than 170,000 times, according to Symantec.

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