Cyber Sweep

Executive Summary:

Operation Cyber Sweep represents a coordinated initiative targeting an expansive array of Cyber Crime schemes victimizing individuals and industry worldwide. This initiative highlights numerous investigations that have been successfully advanced through cooperation and coordination of law enforcement, and a growing list of industry partners.

Cases included in Operation Cyber Sweep exemplify the growing volume and character of Internet facilitated crimes confronting law enforcement, and also underscores the continuing commitment of law enforcement to aggressively pursue cyber criminals, both domestically and abroad. Historically, Cyber criminals abroad have perceived themselves as beyond the reach of U.S. authorities, and in some instances, untouchable by their own country's law enforcement. Until recently, law enforcement and industry were consistently frustrated with the inability to effectively pursue matters in certain countries. That situation is rapidly changing, due to a concerted emphasis within DOJ to train and equip law enforcement in many of these countries, including Ghana, Nigeria and Romania. Due in large part to these efforts, certain noteworthy international successes included in Operation Cyber Sweep became possible.

Criminal schemes included in this initiative include: International re-shipping schemes, auction fraud, spoofing/phishing, credit card fraud, work at home schemes, cyber-extortion, Intellectual Property Rights (IPR), Computer Intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of "traditional crimes" that have migrated on-line.

The substantial accomplishments included in this initiative are attributable to the growing number of joint cyber-crime task forces established across the U.S. Over the past year, more than 50 such task forces have either been established or significantly augmented with resources from numerous federal, state and local agencies. Enhanced industry partnerships developed in coordination with associations such as the Merchants Risk Council (MRC), the Business Software Alliance (BSA), the Software and Information Industry Association (SIIA) and the Motion Picture Association of America (MPAA) also contributed significantly to the success of this initiative. Operation Cyber Sweep has been coordinated at the Federal level with the Department of Justice, the FBI, the U.S Postal Inspection Service, the U.S. Secret Service, the Federal Trade Commission and the Bureau of Immigration and Customs Enforcement. Numerous state and local law enforcement agencies contributed significantly to this initiative as well. State & Local participation in this effort was amplified in coordination with The National White Collar Crime Center (NW3C).

Operation Cyber Sweep includes more than 100 investigations, in which more than 125,000 victims lost more than $100 million dollars. Through these investigations more than 350 subjects were targeted, resulting in 125 arrests/convictions, 70+ indictments and the execution of more than 90 search/seizure warrants. Although significant in number, these investigations represent only a fraction of the cyber crime problem, underscoring not only the

need for sustained law enforcement focus, but the continuing development of expanded industry partnerships as well.

Common Internet Fraud Schemes

Advance-Fee Fraud Schemes

The victim is required to pay significant fees in advance of receiving a substantial amount of money or merchandise. The fees are usually passed off as taxes, or processing fees, or charges for notarized documents. The victim pays these fees and receives nothing in return. Perhaps the most common example of this type of fraud occurs when a victim is expecting a large payoff for helping to move millions of dollars out of a foreign country. The victim may also believe he has won a large award in a nonexistent foreign lottery.

Business/Employment Schemes

Typically incorporate identity theft, freight forwarding, and counterfeit check schemes. The fraudster posts a help-wanted ad on popular Internet job search sites. Respondents are required to fill out an application wherein they divulge sensitive personal information, such as their date of birth and Social Security number. The fraudster uses that information to purchase merchandise on credit. The merchandise is sent to another respondent who has been hired as a freight forwarder by the fraudster. The merchandise is then reshipped out of the country. The fraudster, who has represented himself as a foreign company, then pays the freight forwarder with a counterfeit check containing a significant overage amount. The overage is wired back to the fraudster, usually in a foreign country, before the fraud is discovered.

Counterfeit Check Schemes

A counterfeit or fraudulent cashier's check or corporate check is utilized to pay for merchandise. Often these checks are made out for a substantially larger amount than the purchase price. The victims are instructed to deposit the check and return the overage amount, usually by wire transfer, to a foreign country. Because banks may release funds from a cashier's check before the check actually clears, the victim believes the check has cleared and wires the money as instructed. One popular variation of this scam involves the purchase of automobiles listed for sale in various Internet classified advertisements. The sellers are contacted about purchasing the autos and shipping them to a foreign country. The buyer, or person acting on behalf of a buyer, then sends the seller a cashier's check for an amount several thousand dollars over the price of the vehicle. The seller is directed to deposit the check and wire the excess back to the buyer so they can pay the shipping charges. Once the money is sent, the buyer typically comes up with an excuse for canceling the purchase, and attempts to have the rest of the money returned. Although the seller does not lose the vehicle, he is typically held responsible by his bank for depositing a counterfeit check.

Credit/Debit Card Fraud

Is the unauthorized use of a credit/debit card to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in an identity theft scheme.

Freight Forwarding/Reshipping

The receiving and subsequent reshipping of on-line ordered merchandise to locations usually abroad. Individuals are often solicited to participate in this activity in chat rooms, or through Internet job postings. Unbeknownst to the reshipper, the merchandise has been paid for with fraudulent credit cards.

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an email solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

Investment Fraud

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.

Non-delivery of Goods/Services

Merchandise or services that were purchased or contracted by individuals on-line are never delivered.

Online Auction/Retail

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Phony Escrow Services

In an effort to persuade a wary Internet auction participant, the fraudster will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware the fraudster has spoofed a legitimate escrow service. The victim sends payment or merchandise to the phony escrow and receives nothing in return.

Ponzi/Pyramid Schemes

Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits. However, no investments are actually made by the so called "investment firm." Early investors are paid returns with the investment capital received from subsequent investors. The system eventually collapses and investors do not receive their promised dividends and lose their initial investment.

Spoofing/Phishing

A technique whereby a fraudster pretends to be someone else's email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster's newly created fraudulent web site. Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dupe the victim into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim, usually via email is provided with a hyperlink that directs him/her to a fraudster's web site. This fraudulent web site's name (Uniform Resource Locator) closely resembles the true name of the legitimate business. The victim arrives at the fraudulent web site and is convinced by the sites content that they are in fact at the company's legitimate web site and are tricked into divulging sensitive personal information. Spoofing and phishing are done to further perpetrate other schemes, including identity theft and auction fraud.