FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

July 1, 2011
Volume 3 Issue 7

Federal Bureau of Investigation
5525 West Gray Street
Tampa, FL 33609, 813.253.1000

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

A few brief notes this month

In the interests of brevity, we are going to try something new here this month.

Our intent with these newsletters has always been to provide education through the use of the real world examples of espionage, economic espionage, hacking, export violations and other related counterintelligence news.

The myriad of methods and techniques used by foreign governments, unethical competitors, hackers, criminals and others seeking to steal information is vast. The monthly reporting we compile and forward to you each month fully demonstrates that the threat and the vulnerability are very real.

Our hope is always that someone will see a parallel in something that happened in one of articles, and recognizes a similar situation existing that the individual has observed. Then, noting the similarity, the individual will contact Security, Human Resources, Computer Security, or The FBI and Defense Security Service, as required by the NISPOM.

This month, rather than provide a link to the original article, as well as then including the entire original article, we are instead providing a link, a brief summary providing the flavor of the story, and in some cases a very brief summary of why this article might be important to you.

We are trying to provide what we think to be relevant news to many different recipients with a variety of interests. We think by doing this, we can still provide something of interest and relevance for everyone.

Please do remember, "links" are not forever, and obviously not available offline, so please do visit a link you deem of interest quickly, because in a week or a month, or a year it may be gone forever. If you find a link of interest that no longer works, one suggestion would be to do a Google search using similar words as included in the published article headline. More often than not you'll find a variant, and be able to obtain basically the same or similar content at the new link. One other potential source is the Internet Archive, often referred as the "Wayback Machine" (Mr. Peabody anyone?). This is an archive of the World Wide Web as it has changed and modified throughout much of the web's history.

If interested, the below link will take you to it:

http://www.google.com/url?sa=t&source=web&cd=8&sqi=2&ved=0CGIQFjAH&url=http%3A%2F%2Fwaybackmachine.org%2F&ei=CyPtTdzkMMHIgQeF4-3hCQ&usg=AFQjCNHIA4Q7TuWpvJ_3lU7C5dzGVOxmmg

Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education

Recently, the Counterintelligence Strategic Partnership Unit of the FBI drafted and published an excellent white paper captioned as above. This paper is unclassified in its entirety, and may be viewed in its entirety at:

http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-and-national-security

A very brief extract from this white paper follows:

Who tries to improperly obtain information from US campuses?

There are a variety of people and organizations within and outside the United States who may seek to improperly or illegally obtain information from US institutions of higher education: foreign and domestic businesses, individual entrepreneurs, competing academics, terrorist organizations, and foreign intelligence services.

Foreign and domestic businesses compete in a global economy. Some foreign governments provide resources and information, including competitive intelligence gathering and corporate espionage on behalf of their indigenous companies as a way to promote the overall economic well-being of their country.

Foreign intelligence services pursue restricted information and so may seek out people who have, or will eventually have, access to restricted information.

Individual entrepreneurs may capitalize on opportunities to bring new technology or services to their country in order to fill a niche currently supplied by non-native companies. To jump start business, they may steal research or products that would otherwise be costly to create or replicate. Academics may steal research and use it or claim it as their own for a variety of reasons. Terrorist

organizations may want information on products or processes they can use to inflict mass casualties or damage.

END OF EXTRACT
For those of you with ties to academia, we encourage you to visit the website hyperlinked above to view the entire white paper. Individuals involved with the development of intellectual property in an academic environment may well gain new insights and perspectives that shed light on the nature of the threat and how best to counter it.

Travel Advice for the Upcoming Vacation Season and for Business Travelers and Students

At the below web hyperlinks readers will find two pamphlets published by the FBI that provide detailed listings of best practices, safety tips and tips on protecting your business information when traveling overseas. In addition, there is an excellent publication providing similar tips for students traveling overseas. These documents are available as downloadable .pdf documents. Readers are encouraged to view these pamphlets and utilize them as appropriate.
Web links to the pamphlets follow:

http://www.fbi.gov/about-us/investigate/counterintelligence/business-travel-brochure
http://www.fbi.gov/about-us/investigate/counterintelligence/student-travel-brochure-pdf

ARRESTS, TRIALS AND CONVICTIONS

Two Chinese Nationals Charged with Illegally Attempting to Export Military Satellite Components to the PRC

NOTE: On 6/1/2011 the below named individuals pleaded guilty in federal court in Alexandria, Virginia, to attempted export of defense items.

FOR IMMEDIATE RELEASE April 4, 2011

ALEXANDRIA, Va. – Two Chinese nationals have been indicted by a federal grand jury in Alexandria, Va., for attempting to obtain radiation-hardened microchips, which are prohibited defense items used in the military and aerospace industry.

Neil H. MacBride, United States Attorney for the Eastern District of Virginia; Todd Hinnen, Acting Assistant Attorney General for National Security; John P. Torres, Special Agent in Charge for ICE, Office of Homeland Security Investigations (HSI)

in Washington, D.C.; and Robert E. Craig, Special Agent in Charge of the Defense Criminal Investigative Service's (DCIS) Mid-Atlantic Field Office, made the announcement after the indictment was unsealed.

Hong Wei Xian, a/k/a "Harry Zan," 32, and Li Li, a/k/a "Lea Li," 33, both from the People's Republic of China (PRC), were charged in a two-count indictment accusing them of conspiring to violate the Arms Export Control Act to smuggle goods from the United States and the attempted export of United States Munitions List items in violation of the Arms Export Control Act. If convicted, they face a maximum penalty of five years in prison for the conspiracy charge and 20 years in prison on the export violation charge. Xian and Li will make their initial appearance at 2:00 p.m. at the Alexandria federal courthouse.

According to the indictment, Xian is the president of Beijing Starcreates Space Science and Technology Development Company Limited (Beijing Starcreates), and Li is the company's vice president. Among other things, Beijing Starcreates engages in the business of importing and selling programmable read-only memory microchips to China Aerospace Science and Technology Corporation, which is controlled by the PRC government and plays a substantial role in the research, design, development and production of strategic and tactical missile systems and launch vehicles for the PRC.

Since 1990, the U.S. government has maintained an arms embargo against the PRC that prohibits the export, re-export, or re-transfer of any defense article to the PRC. Prohibited defense articles are placed on the United States Munitions List, which includes spacecraft systems and associated equipment. A programmable read-only memory microchip (PROM) serves to store the initial start-up program for a computer system and is built to withstand the conditions present in outer space.

According to the indictment, neither Xian nor Li applied for nor received a license from the United States to export defense articles of any description; however, from April 2009 to Sept. 1, 2010, the two are charged with contacting a company in the Eastern District of Virginia and seeking to export thousands of radiation-hardened PROMs from that company.

The indictment states that Xian and Li knew a license was required but did not seek to obtain one because it was difficult, time-consuming, and would require them to identify the end user and describe the end use. They are accused of conspiring to break up orders into multiple shipments and designate countries outside the PRC for delivery to avoid drawing attention to the orders.

On Sept. 1, 2010, the defendants were arrested in Hungary pursuant to a United States provisional arrest warrant and were transferred into the custody of

U.S. Marshals on April 1, 2011, after they waived extradition. They arrived in the Eastern District of Virginia late April 1, 2011.

This case was investigated by ICE HSI and DCIS, with assistance from ICE HSI Office of International Affairs and the Department of Justice's Office of International Affairs. Assistant United States Attorney James P. Gillis of the Office's National Security and International Crime Unit and Trial Attorney Brandon L. Van Grack of the Justice Department's National Security Division are prosecuting the case on behalf of the United States.

Criminal indictments are only charges and not evidence of guilt. A defendant is presumed to be innocent until and unless proven guilty.

A copy of this press release may be found on the website of the United States Attorney's Office for the Eastern District of Virginia at http://www.justice.gov/usao/vae . Related court documents and information may be found on the website of the District Court for the Eastern District of Virginia at http://www.vaed.uscourts.gov or on http://pacer.uspci.uscourts.gov.

Iranian National Pleads Guilty in Plot to Illegally Export Missile Components and Radio Tests Sets to Iran

http://www.justice.gov/usao/iln/pr/chicago/2011/pr0531_01.pdf

FOR IMMEDIATE RELEASE

TUESDAY MAY 31, 2011

AUSA Patrick Pope

(312)353-1980

www.usdoj.gov/usao/iln

Randall Samborn

(312)353-5318

CHICAGO — An Iranian national who maintained a residence and business in California pleaded guilty today in Federal Court here to two felony charges stemming from his efforts to illegally export missile components and radio test sets from the United States to Iran, via the United Arab Emirates.

The defendant, Davoud Baniameri, 38, of Woodland Hills, Calif., pleaded guilty to one count of conspiring to export goods and technology to Iran without a license or approval from the U.S. Department of Treasury, in violation of the International Emergency Economic Powers Act (IEEPA) and one count of attempting to export defense articles on the U.S. Munitions List from the United States without a license or approval from the U.S. Department of State in violation of the Arms Export Control Act (AECA).

U.S. District Judge Samuel Der-Yeghiayan set sentencing for Aug. 4. Baniameri, who remains in federal custody, faces a maximum penalty of 10 years in prison for violating IEEPA and a maximum of 20 years in prison for violating AECA and a maximum fine of $250,000 on each count. A written plea agreement contemplates a sentencing guideline range of 46 to 57 months imprisonment. The guilty plea was announced by Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois; Gary J. Hartwig, Special Agent in Charge of the U.S. Immigration and Customs Enforcement (ICE) Office of Homeland Security Investigations HSI); Richard D. Zott, Special Agent-in-Charge of the Defense Criminal Investigative Service Central Field Office in St. Louis; Ronald B. Orzel, Special Agent-in-Charge of the Chicago office of the Department of Commerce's Office of Export Enforcement; and Alvin Patton, Special Agent-in-Charge of the Criminal Investigation Division of the Internal Revenue Service. The Chicago Police Department also assisted in the investigation.

Baniameri, also known as "Davoud Baniamery," David Baniameri," and "David Baniemery," was arrested on a criminal complaint on Sept. 9, 2009, and indicted in December 2009, along with co-defendant Andro Telemi, 40, of La Tuna Canyon, Calif., a naturalized U.S. citizen from Iran. A superseding indictment in July 2010 charged Baniameri, Telemi and a third defendant, Syed Majid Mousavi, an Iranian citizen living in Iran. Telemi, also known as "Andre Telimi" and "Andre Telemi," was released and is awaiting trial in Federal Court in Chicago. Mousavi, also known as "Majid Moosavy," remains a fugitive and is believed to be in Iran.

According to the plea agreement and other court records, sometime before Oct. 10, 2008, Mousavi, based in Iran, contacted Baniameri in California and requested that he purchase and export radio test sets from the United States to Iran, through Dubai. Baniameri agreed and over the next few months negotiated the purchase of three Marconi radio test sets from a company in Illinois.

Ultimately, Baniameri arranged for the radio test kits to be sent to him in California, where he shipped them to Dubai, for ultimate transshipment to Iran. At no time did Baniameri obtain or attempt to obtain a license from the U.S. government for the export of the radio test sets.

The plea agreement also states that, sometime before Aug. 10, 2009, Mousavi contacted Baniameri and requested that he purchase and export to Iran via Dubai 10 connector adapters for the TOW and TOW2 missile systems. Baniameri agreed to purchase the items on behalf of Mousavi, and over the next few months, he admitted that he and his co-defendants attempted to purchase 10 connector adaptors from a company in Illinois, which unbeknownst to them, was in fact a company controlled by law enforcement. In September 2009, Baniameri admitted that he directed Telemi to take possession of the connector adaptors in California after having paid $9,450 to a representative of the Illinois company. To further facilitate the export of these items to Iran, Baniameri arranged to fly from the United States to Dubai and then from Dubai to Iran. At no time did Baniameri obtain or attempt to obtain a license from the U.S. government for the export of the connector adaptors. He was arrested before leaving the United States.

The government is being represented in court by Assistant U.S. Attorney Patrick C. Pope.

Department of Justice Disrupts International Cybercrime Rings Distributing Scareware

http://www.justice.gov/opa/pr/2011/June/11-opa-820.html

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, June 22, 2011

WASHINGTON – Today the Department of Justice and the FBI, along with international law enforcement partners, announced the indictment of two individuals from Latvia and the seizure of more than 40 computers, servers and bank accounts as part of Operation Trident Tribunal, an ongoing, coordinated enforcement action targeting international cybercrime. The operation targeted international cybercrime rings that caused more than $74 million in total losses to more than one million computer users through the sale of fraudulent computer security software known as "scareware."

Scareware is malicious software that poses as legitimate computer security software and purports to detect a variety of threats on the affected computer that do not actually exist. Users are then informed they must purchase what they are told is anti-virus software in order to repair their computers. The users

are then barraged with aggressive and disruptive notifications until they supply their credit card number and pay for the "anti-virus" product, which is, in fact, fake.

Warrants obtained from the U.S. District Court for the Western District of Washington and elsewhere throughout the United States led to the seizure of 22 computers and servers in the United States that were involved in facilitating and operating a scareware scheme. In addition, 25 computers and servers located abroad were taken down as part of the operation, including equipment in the Netherlands, Latvia, Germany, France, Lithuania, Sweden and the United Kingdom.

The first of the international criminal groups disrupted by Operation Trident Tribunal infected hundreds of thousands of computers with scareware and sold more than $72 million worth of the fake antivirus product over a three-year period. The scareware scheme used a variety of ruses to trick consumers into unknowingly infecting their computers with the malicious scareware products, including web pages featuring fake computer scans. Once the scareware was downloaded, victims were notified that their computers were infected with a range of malicious software, such as viruses and Trojans and badgered into purchasing the fake antivirus software to resolve the non-existent problem at a cost of up to $129. An estimated 960,000 users were victimized by this scareware scheme, leading to $72 million in actual losses. Latvian authorities also executed seizure warrants for at least five bank accounts that were alleged to have been used to funnel profits to the scam's leadership.

A second international crime ring disrupted by Operation Trident Tribunal relied on online advertising to spread its scareware products, a tactic known as "malvertising." An indictment unsealed today in U.S. District Court in Minneapolis charges the two operators of this scareware scheme with two counts of wire fraud, one count of conspiracy to commit wire fraud and one count of computer fraud. The defendants, Peteris Sahurovs, 22, and Marina Maslobojeva, 23, were arrested yesterday in Rezekne, Latvia, on the charges filed in the District of Minnesota. According to the indictment, the defendants created a phony advertising agency and claimed that they represented a hotel chain that wanted to purchase online advertising space on the Minneapolis Star Tribune's news website, startribune.com. The defendants provided an electronic version of the advertisement for the hotel chain to the Star Tribune, and technical staff at startribune.com tested the advertising and found it to operate normally.

According to court documents, after the advertisement began running on the website, the defendants changed the computer code in the ad so that the computers of visitors to startribune.com were infected with a malicious software

program that launched scareware on their systems. The scareware caused users' computers to "freeze up" and then generate a series of pop-up warnings in an attempt to trick users into purchasing purported "antivirus" software, which was, in fact, fake. Users' computers "unfroze" if the users paid the defendants for the fake antivirus software, but the malicious software remained hidden on their computers. Users who failed to purchase the fake antivirus software found that all information, data and files stored on the computer became inaccessible. The scam allegedly led to at least $2 million in losses. If convicted, the defendants face penalties of up to 20 years in prison and fines of up to $250,000 on the wire fraud and conspiracy charges, and up to 10 years in prison and fines of up to $250,000 on the computer fraud charge. The defendants also face restitution and forfeiture of their illegal profits. An indictment is merely a charge and defendants are presumed innocent until proven guilty.

"Today's operation targets cybercrime rings that stole millions of dollars from unsuspecting computer users," said Assistant Attorney General Lanny A. Breuer of the Justice Department's Criminal Division. "These criminal enterprises infected the computers of innocent victims with malicious scareware, and then duped them into purchasing fake anti-virus software. Cybercrime is profitable, and can prey upon American consumers and companies from nearly any corner of the globe. We will continue to be aggressive and innovative in our approach to combating this international threat. At the same time, computer users must be vigilant in educating themselves about cyber security and taking the appropriate steps to prevent dangerous and costly intrusions."

"This case shows that strong national and global partners can ensure there is no sanctuary for cyber-crooks," said U.S. Attorney Jenny A. Durkan of the Western District of Washington. "We will continue to work with the public and the computer industry, to fortify our cyber defenses. A combination of safe online habits and smart technology will help reduce the threat posed by these organized criminal groups."

"The global reach of the Internet makes every computer user in the world a potential victim of cybercrime," said U.S. Attorney B. Todd Jones of the District of Minnesota. "Addressing cybercrime requires international cooperation; and in this case, the FBI, collaborating with our international law enforcement and prosecution partners, has worked tirelessly to disrupt two significant cybercriminal networks. Their efforts demonstrate that no matter the country, Internet criminals will be pursued, caught and prosecuted."

Assistant Director Gordon M. Snow of the FBI's Cyber Division said, "Scareware is just another tactic that cyber criminals are using to take money from citizens and businesses around the world. This operation targeted a sophisticated business enterprise that had the capacity to steal millions. Cyber threats are a global

problem, and no single country working alone can be effective against these crimes. The FBI thanks the participating foreign law enforcement agencies for their ongoing partnership and commitment in disrupting this threat."

Operation Trident Tribunal was conducted by the FBI's Cyber Division, Seattle Field Office and Minneapolis Field Office; the Computer Crime and Intellectual Property Section and the Asset Forfeiture and Money Laundering Section of the Justice Department's Criminal Division; the U.S. Attorney's Office for the District of Minnesota; and the U.S. Attorney's Office for the Western District of Washington. Operation Trident Tribunal was the result of significant international cooperation and substantial assistance from the Criminal Division's Office of International Affairs. Multiple foreign law enforcement partners provided invaluable assistance in this operation, including the Cyprus National Police in cooperation with its Unit for Combating Money Laundering (MOKAS); German Federal Criminal Police (BKA); Latvian State Police; Security Service of Ukraine; Lithuanian Criminal Police Bureau; French Police Judiciare; the Netherlands' National High-Tech Crime Unit; the Cyber Unit of the Swedish National Police; London Metropolitan Police; Romania's Directorate for Combating Organized Crime; and the Royal Canadian Mounted Police.

To avoid falling victim to a scareware scheme, computer users should avoid purchasing computer security products that use unsolicited "free computer scans" to sell their products. It is also important for users to protect their computers by maintaining an updated operating system and using legitimate, up-to-date antivirus software, which can detect and remove fraudulent scareware products.

Additional tips on how to spot a scareware scam include:

Scareware advertising is difficult to dismiss. Scareware purveyors employ aggressive techniques and badger users with pop-up messages into purchasing their products. These fake alerts are often difficult to close and quickly reappear;

Fake anti-virus products are designed to appear legitimate, and can use names such as Virus Shield, Antivirus or Virus Remover. Only install software from trusted sources that you seek out. Internet service providers often make name-brand anti-virus products available to their customers for free;

Become familiar with the brand, look and functionality of the legitimate anti-virus software that is installed on your computer. This will assist you in identifying scareware.

Computer users who think they have been victimized by scareware should file a complaint with the FBI's Internet Crime Complaint Center, www.ic3.gov .

11-820 Office of Public Affairs

Former NSA Senior Executive Pleads Guilty to Unauthorized Access of Government Computer

http://www.justice.gov/opa/pr/2011/June/11-crm-760.html

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, June 10, 2011

WASHINGTON - Former National Security Agency (NSA) senior executive Thomas A. Drake pleaded guilty today in U.S. District Court in Baltimore to a one-count criminal information charging him with unauthorized access of an NSA computer, announced Assistant Attorney General Lanny A. Breuer of the Justice Department's Criminal Division.

Drake, 54, pleaded guilty before U.S. District Court Judge Richard D. Bennett to the misdemeanor offense of intentionally exceeding the authorized access of a computer. Sentencing is scheduled for July 15, 2011, at 3:00 p.m. EDT. "Today, Thomas Drake admitted that he illegally accessed classified NSA computer systems to obtain information that he then provided to another person who had no authorization to receive it. As today's guilty plea shows, in cases involving classified information, we must always strike the careful balance between holding accountable those who break our laws, while not disclosing highly-sensitive information that our intelligence agencies conclude would be harmful to our nation's security if used at trial," said Assistant Attorney General Breuer. "Individuals who are granted special access to our nation's most sensitive information cannot unilaterally decide to disregard the law and agreements they make with the government on how that information may be handled."

According to the statement of facts, Drake worked as an employee of the NSA from August 2001 through April 2008. In connection with his employment, Drake was granted a Top Secret clearance and had access to classified computer

systems, such as the NSA's internal intranet or NSA Net. Drake received various security briefings regarding the handling restrictions and requirements involving official NSA information, and knew that the NSA restricted the use of and access to its computers and NSA Net for official use only.

According to the statement of facts, from approximately February 2006 through March 2007, Drake intentionally accessed NSA Net, obtained NSA information and provided the information to another person not permitted or authorized to receive it.

Also today, in exchange for the defendant's guilty plea, the government filed a motion to dismiss, at the time of sentencing, the pending indictment against Drake. Drake was charged in an April 2010 indictment with willful retention of classified information, obstruction of justice and false statements.

According to the government's motion, pre-trial rulings by the court under the Classified Information Procedures Act (CIPA) would have required that highly classified information appear, without substitution, in exhibits made publicly available at trial. The NSA concluded that such disclosure would harm national security. According to the filing, in CIPA litigation, the parties indicate what classified information they reasonably expect to disclose thorough evidence, and the court makes determinations on how and what classified information may be used at trial. The government then must make a determination whether the disclosure of that classified information could harm national security, and accordingly how the prosecution is impacted.

The case is being prosecuted by Senior Litigation Counsel William M. Welch II of the Criminal Division and Trial Attorney John P. Pearson of the Criminal Division's Public Integrity Section. This case was investigated by the FBI and the NSA Office of Security & Counterintelligence. The National Security Division also provided assistance in this matter.

11-760 Criminal Division

Members of International Procurement Network Indicted for Supplying Iran with U.S. Military Aircraft Components

http://www.justice.gov/opa/pr/2011/June/11-nsd-826.html

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, June 23, 2011

Total of 12 Defendants in U.S., France, U.A.E. and Iran Charged

MACON, Ga. – Seven individuals and five corporate entities based in the United States, France, the United Arab Emirates (U.A.E.) and Iran have been indicted in the Middle District of Georgia for their alleged roles in a conspiracy to illegally export military components for fighter jets and attack helicopters from the United States to Iran. One of the defendants and his company were sentenced yesterday, with the individual receiving nearly five years in prison. Another defendant and his company have admitted their illegal conduct and also pleaded guilty in the investigation.

Federal prosecutors today unsealed a superseding indictment in Macon, Ga., charging eight of the defendants with conspiring to violate and violating the Arms Export Control Act (AECA), the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions Regulations, as well as conspiracy to defraud the United States, money laundering and false statement violations. Charges against the four other defendants, who have pleaded guilty in the case, are contained in the original indictment in the investigation that was filed previously.

The indictment and other enforcement actions were announced by Todd Hinnen, Acting Assistant Attorney General for National Security; Michael J. Moore, U.S. Attorney for the Middle District of Georgia; Brock Nicholson, Special Agent-in-Charge of the U.S. Immigration and Customs Enforcement, Homeland Security Investigations (ICE-HSI) office in Atlanta; Brian D. Lamkin, Special Agent-in-Charge of the FBI's Atlanta Field Division; and Robert Luzzi, Special Agent-in-Charge of the Commerce Department, Office of Export Enforcement (OEE) Miami Field Office.

The Defendants

Thus far, four defendants based in the United States have been charged as part of the investigation. They are The Parts Guys LLC, a company in Port Orange, Fla., that maintains a warehouse at the Middle Georgia Municipal Airport in Macon, as well as the president of The Parts Guys, Michael Edward Todd, who is a U.S. national. In addition, Galaxy Aviation Services, a company in St. Charles, Ill., and its president, Hamid Seifi, also known as Hank Seifi, an Iranian-born U.S. national, have been charged.

Todd was arrested last year in Atlanta based on the original indictment in the case. Todd and his company, The Parts Guys, pleaded guilty to conspiracy to violate the AECA on May 9, 2011, and have yet to be sentenced. Federal agents arrested Seifi in Atlanta earlier this year, also based on the original indictment.

Seifi and his company, Galaxy Aviation, pleaded guilty on Feb. 24, 2011, to conspiracy to violate the AECA and violating the IEEPA. Yesterday, Seifi was sentenced to 56 months in prison followed by three years of supervised release, a fine of $12,500 and forfeiture of $153,950, while Galaxy Aviation, which is now defunct, received a $400 special assessment.

Three defendants based in France have also been indicted as part of the investigation. They are Aerotechnic, a company in Pinsaguel, France, and its president, Philippe Sanchez, a French national, as well as Luc Teuly, a French national and the sales manager of Aerotechnic. Each of these defendants remains a fugitive.

Two defendants based in the U.A.E. have also been indicted in the case. They are Aletra General Trading, a company in Dubai doing business as "Erman & Sultan Trading Co," and Syed Amir Ahmed Najfi, an Iranian national and purchaser for Aletra. Najfi remains a fugitive.

Three defendants based in Iran have also been charged in the case. They are Sabanican Company, a company in Tehran, and its president, Hassan Seifi, an Iranian national, as well as Reza Seifi, an Iranian national and the managing director of Sabanican Company. Each of these defendants remains at large. As part of the U.S. government's coordinated action against this procurement network, the Commerce Department announced today that it will add the eight defendants in France, Iran and the U.A.E. to its "Entity List." The Entity List provides notice to the public that certain exports, re-exports and transfers (in-country) to parties identified on the Entity List require a license from the Commerce Department, and that availability of license exceptions in such transactions is limited. All eight parties will be added to the Entity List with a licensing requirement for all items subject to the Commerce Department export regulations and with a presumption of denial.

The Charges

According to the charges, the defendants conspired to export components for attack helicopters and fighter jets to Iran without obtaining the required U.S. export licenses. These components included military parts for the Bell AH-1 attack helicopter, the UH-1 Huey attack helicopter, as well as the F-5 and F-4 fighter jets.

Defendant Najfi and his firm in the U.A.E. are alleged to have placed orders and purchased military aircraft parts, including those for the Bell AH-1 attack helicopter, from Todd and his company, The Parts Guys, in the United States. Todd and other conspirators then attempted to and did cause the export of the aircraft parts to the U.A.E.

Defendant Hank Seifi and his firm in Illinois also allegedly placed orders and purchased U.S. aircraft parts from Todd and his company in Georgia -- on behalf of Hassan Seifi, Reza Seifi and their company in Iran. According to the charges, Todd and other conspirators then caused these aircraft parts to be exported to Iran via the defendants in France: Sanchez, Teuly and their company, Aerotechnic.

The charge of conspiracy carries a maximum penalty of five years in prison, while violating the AECA carries a maximum penalty of 20 years in prison, and violating IEEPA carries a maximum penalty of 20 years in prison. Money laundering carries a maximum 20 years in prison, while making false statements carries a maximum of five years in prison.

"The defendants in this case are alleged to have conspired to defraud the United States by illegally acquiring and exporting fighter jet and attack helicopter components. Keeping such advanced weaponry, which is designed to protect the men and women of our Armed Forces and to defend our national interests, from falling into the hands of state sponsors of terror has never been more important," said Todd Hinnen, Acting Assistant Attorney General for National Security.

"Through coordinated law enforcement efforts, we have cut off more than a branch of this illegal supply tree; we have cut off the tree at its trunk. These parts have a military purpose, and I am determined to see that they are not used to harm the United States, its soldiers, citizens or friends. This type of criminal activity should remind each of us that we must be ever vigilant in our efforts to protect our national security. The threat is very real, and comes from even the least suspected places, including middle Georgia," said U.S. Attorney Michael Moore.

"The illegal export of U.S. weapons and military technology presents a direct threat to our national security," said Brock Nicholson, Special Agent-in-Charge of ICE-HSI in Atlanta. "This investigation demonstrates the importance of preventing our military equipment from falling into the wrong hands, where it could potentially be used against our military members, our homeland and our allies. Enforcing U.S. export laws is one of our top priorities, and we will continue working with our law enforcement partners to ensure that those who put our country at risk are discovered and brought forward for prosecution."

Brian D. Lamkin, Special Agent-in-Charge, FBI Atlanta, stated: "The cooperative efforts among the FBI, ICE and U.S. Commerce was critical in bringing this case forward for prosecution by the U.S. Department of Justice. The enforcement of U.S. laws that prohibit the acquisition of specified defense related items is paramount to national security and is a daunting task when back dropped against the vast movement of legitimate international trade that occurs every day in the U.S. The FBI is pleased with the role that it has played in this multi-agency enforcement effort."

"The Commerce Department's Office of Export Enforcement (OEE) dedicates one hundred percent of its resources to enforcing export laws, and today's case is the result of ongoing cooperation with Immigration and Customs Enforcement and the FBI to protect our national security," said Robert Luzzi, Special Agent-in-Charge of OEE's Miami Field Office. "Parties who export to embargoed destinations such as Iran will be pursued and prosecuted to the fullest extent of the law."

This case was investigated by ICE Homeland Security Investigations in Atlanta, FBI Atlanta Field Division and the Department of Commerce's OEE.
The prosecution is being handled by Assistant U.S. Attorneys Jennifer Kolman and Danial E. Bennett from the U.S. Attorney's Office for the Middle District of Georgia and Trial Attorneys Ryan P. Fayhee and Brandon L. Van Grack from the Counterespionage Section of the Justice Department's National Security Division.
The public is reminded that an indictment contains mere allegations and that defendants are presumed innocent unless and until proven guilty.

11-826 National Security Division

The Economic Espionage Case Against Hanjuan Jin

Located at the link below is the Memorandum Opinion and Order dated 6/14/2011, signed by Judge Ruben Castillo of the United States District Court Northern District of Illinois, Eastern Division. Judge Castillo is the presiding judge in the trial of Hanjuan Jin.

http://www.courthousenews.com/2011/06/24/Jin.pdf

Hanjuan Jin was a software engineer for Company A, a Chicago-area company that sells telecommunications products and services around the world. The government alleges that while Jin was on medical leave from Company A in 2006, she negotiated and accepted employment with Company B, a

telecommunications company based in China that has provided telecommunications technology and products to the Chinese military.

The government also alleges that after accepting employment with Company B, Jin returned to work at Company A on February 26 2007, and did not advise anyone at Company A that she had accepted employment with Company B.

That day, she downloaded over 200 technical documents belonging to Company A on the secure internal computer network, and removed other documents and materials belonging to Company A. The next day she informed her manager at Company A that she was resigning. That same night, Jin downloaded additional technical documents belonging to Company A.

The following day, February 28, 2007, Jin was stopped at O'Hare International Airport as she attempted to depart for China. She had previously purchased a one way ticket to China. When she was stopped, Jin had in her possession over 1000 technical electronic and paper documents belonging to Company A. She also possessed Company B documents containing Chinese military applications for certain telephonic communications technology.

On December 9, 2008, the Grand Jury returned a superseding indictment. The indictment charges Jin with violating the Economic Espionage Act of 1996. Counts I-III charge Jin with possessing trade secrets with intent to convert them to the economic benefit of someone other than the owner, intending and knowing that the offense would injure the owner, in violation of 1832 (a) (3). Counts IV-VI charge Jin with possessing trade secrets, knowing the trade secrets were stolen, appropriated, obtained and converted without authorization, intending and knowing that the offense would benefit a foreign government, in violation of 1831 (a) (3).

In sum, the indictment alleges that Jin stole trade secrets pertaining to telecommunications technology from Company A, and intended to convert those trade secrets to the benefit of a telecommunications competitor in China, Company B, and the Chinese military.

For more on this fascinating case, please visit the hyperlink located toward the beginning of this article.

TECHNIQUES, METHODS, TARGETS

Espionage and Foreign Interference

http://www.csis-scrs.gc.ca/prrts/spng/index-eng.asp (NOTE: THIS LINK IS TO THE CANADIAN WEB SITE FOR CSIS)

Espionage

Canada's national and economic security continues to be threatened by espionage and foreign-influenced activity. CSIS's counter-intelligence activities are aimed at investigating such threats and reporting on them to the Canadian government and law enforcement agencies.

In their quest for political and military intelligence, foreign intelligence services constantly attempt to infiltrate key Canadian government departments.

Increasing global economic competition is leading many governments-both those representing traditionally "hostile" countries as well as those from countries considered "friendly" to Canada-to shift the focus of their intelligence collection from traditional political and military matters to the illicit acquisition of economic and technological information. Such information can include trade and pricing information, investment strategies, contract details, supplier lists, planning documents, research and development data, technical specifications and drawings, as well as computer databases.

Economic espionage-defined as illegal, clandestine, or coercive activity by foreign governments in order to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage-costs the economy billions of dollars each year. Because Canada is a world leader in many technology-intensive fields (including aerospace, biotechnology, chemicals, communications, information technology, mining and metallurgy, in addition to nuclear, oil and gas, and environmental technologies), Canadian companies have been targeted by foreign governments to obtain economic or commercial advantages. The damage to Canadian interests results in lost contracts, jobs and markets, and a diminished competitive advantage.

While espionage can occur on Canadian territory, Canadian businesspeople travelling abroad may also be vulnerable. A foreign government can operate more easily and with greater impunity within its own borders, making hotel rooms, restaurants, offices, and telecommunications systems vulnerable to espionage activities.

CSIS also investigates threats posed by foreign-influenced activities including transnational criminal activity, cyber-related attacks, and activities directed against Canada's expatriate communities.

Expatriate communities in wealthy countries such as Canada are often well-organized and well-funded, making them attractive targets for foreign governments and dissident groups. Certain countries use methods of coercion and manipulation that threaten Canada's national interests. In investigating these activities, CSIS strives to send the message that targeting Canadian citizens is unacceptable.

The CSIS Annual Report can be accessed at below link.
NOTE: THIS LINK IS TO CSIS ITSELF FOR DOWNLOAD OF THE DOCUMENT…THE DOCUMENT IS 14 MEGABITS IN SIZE

http://beta.images.theglobeandmail.com/archive/01286/Canadian_Security__1286526a.pdf

Canada swarming with foreign spies: CSIS head

http://www.montrealgazette.com/news/Canada+swarming+with+foreign+spies+CSIS+head/4941021/story.html

The above is a news article summarizing the findings stated in the CSIS Annual report.

5 top social media security threats

http://www.networkworld.com/cgi-bin/mailto/x.cgi?pagetosend=/news/2011/053111-social-media-security.html&pagename=/news/2011/053111-social-media-security.html&pageurl=http://www.networkworld.com/news/2011/053111-social-media-security.html&site=printpage&nsdr=n

Enterprises need to take precautions to make sure employees practice safe social media

This article, by Chris Nerney, Network World, identifies the top five social media security threats, and ranks them in descending order as below

5. Mobile apps
4. Social engineering
3. Social networking sites
2. Your employees
1. Lack of a social media policy

Please visit the original article at the above link for all the details.

Cop accused of lying about citizenship to join FBI

http://www.beaumontenterprise.com/news/article/Cop-accused-of-lying-about-citizenship-to-join-FBI-1413462.php

By Guillermo Contreras, San Antonio Express-News

Updated 02:02 p.m., Tuesday, June 7, 2011

A Fair Oaks Ranch police officer who wanted to join the FBI has been charged with lying about his citizenship to get a job there.

The FBI Joint Terrorism Task Force opened a full-blown investigation last year of Pejman Amrollah Majdabadi, 30, for his "aggressiveness" in wanting to join the FBI and his e-mailed request to the agency seeking to attend weapons of mass destruction training being taught by the JTTF, according to a criminal complaint affidavit unsealed Monday.

The Iranian-born officer…

EDITORIAL COMMENT: Green Card Fraud (fake marriages) has been successfully utilized more times than we care to think, to successfully gain citizenship and subsequent access to classified information.

Please read the rest of the above article by following the link included at the beginning of this article.

Gmail phishers stalked victims for months

http://www.theregister.co.uk/2011/06/03/gmail_users_stalked_for_months/

Senior gov officials data mined for future attacks

By Dan Goodin in San Francisco

Posted in Security, 3rd June 2011 00:20 GMT

Spear phishers who targeted the personal Gmail accounts of senior government officials painstakingly monitored incoming and outgoing email for almost a year, a researcher who helped uncover the campaign said.

In some cases, the attackers sent the victims emails designed to originate from friends or colleagues in hopes of getting responses that detailed the targets' schedules, contacts, and job responsibilities, Mila Parkour, a Washington, DC-based system administrator who does security research on the side, told The Register. The attackers also employed web-based scripts that caused earlier versions of Microsoft's Internet Explorer browser to divulge detailed information about the software used [1] by the compromised account holder.
The ultimate goal, Parkour speculated, was to assemble an arsenal of personal information that could be used…

Please view this article in its full detail by visiting the website at the link above.

Microsoft warns on support scams

Original URL:

http://www.theregister.co.uk/2011/06/16/tech_support_scam_calls/

Thousands still falling for old-school tech support swindle

By John Oates

Posted in Crime, 16th June 2011 08:59 GMT

A survey from Microsoft reveals just how widespread the fake tech support call scam is becoming.

The crooks cold-call people at home and claim to be calling from Microsoft or a well-known security firm and offering "free security checks"…

Please read the rest of the article by connecting to the article via the above hyperlink.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

Intellectual Property Law Enforcement Efforts

In addition to the protection of classified information, many recipients of this newsletter are responsible for the protection of intellectual property. This intellectual property can take many forms, be it trade secrets, copyrights, trademarks, patents, etc. This could be in the form of paper and electronic documents, a label on clothing, a particular design feature or logo, etc.

The below congressional testimony by FBI Assistant Director Gordon Snow provides insight into some of the threats we all face, as well as some of the solutions the FBI and government are taking to address these threats, often times in partnership with the organizations, businesses, and other entities you, the readers represent and belong too.

http://www.fbi.gov/news/testimony/intellectual-property-law-enforcement-efforts

Gordon M. Snow

Assistant Director, Cyber Division

Federal Bureau of Investigation

Statement Before the Senate Judiciary Committee

Washington, D.C.

June 22, 2011

Good afternoon Chairman Leahy, Ranking Member Grassley, and members of the Committee. I'm pleased to appear before you today to discuss the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO IP Act) and the FBI's efforts, activities, and successes relating to intellectual property rights (IPR) crimes to date.

The enforcement of U.S. laws protecting IPR is critical to protecting the U.S. economy, our national security, and the health and safety of American citizens. The increasing accessibility of the Internet and improvements in manufacturing and transportation have led to the expansion of the global market. With increasing competition, innovation, and divisions of labor, more digital content is instantaneously distributed to the global market than ever before. Businesses now have extraordinary opportunities to market and distribute their goods and services all around the world. Unfortunately, the expansion in worldwide trade has led to growth in the number of criminals and organizations that seek to

exploit and misappropriate the intellectual property of others for profit. These criminals have developed complex and diverse methods of committing IPR crime.

The Nature of the Threat

IPR violations which include theft of trade secrets, digital piracy, and the trafficking of counterfeit goods, result in billions of dollars in lost profits annually. Failure to protect IPR undermines confidence in the economy, removes opportunities for growth, erodes the U.S.'s technological advantage, and disrupts fairness and competitiveness in the marketplace. In short, a robust system for protecting IPR is critical to economic prosperity.

However, some IPR violations pose a more far-reaching and serious threat to the U.S. than just economic loss to the rights holder. Such violations put public safety at risk through the sale of counterfeit pharmaceuticals, electrical components, aircraft and automobile parts, and the funding of organized crime. Some IPR violations also threaten our critical infrastructures and our national security. Counterfeit computer and networking devices undermine the reliability of our communications and transportation networks and create national security vulnerabilities. In addition, nation states target U.S. civilian industries for trade secret theft to obtain information that can be used to advance domestic industries and military capabilities.

The focus of my remarks today is the important role the FBI plays in protecting IPR, our efforts to coordinate with other federal agencies to ensure that intellectual property is rigorously protected, and our successes in this battle thus far.

The Role of the FBI

The FBI's strategic objective is to detect and disrupt state sponsored groups and international and domestic criminal organizations that manufacture counterfeit and pirated goods or steal, distribute or otherwise profit from the theft of intellectual property. The highest priorities for our investigations are counterfeit products affecting health and safety, the theft of trade secrets, and violations with a significant economic impact. The FBI aggressively pursues intellectual property enforcement through traditional investigative methods, intelligence initiatives and coordinated efforts with private industry and domestic and foreign law enforcement partners.

The FBI partners closely with the National Intellectual Property Rights Coordination Center (the IPR Center), which is hosted by U.S. Immigration and Customs Enforcement (ICE). The IPR Center serves as a centralized, multiagency

entity to coordinate, manage, and advocate the U.S. government's criminal enforcement of intellectual property laws.

The FBI moved its Intellectual Property Rights Unit (IPRU) to the IPR Center in April 2010. It includes five dedicated FBI agents, as well as management staff, intelligence analysts and professional support staff who work full time at the IPR Center. The IPRU has a dual focused mission. First, it provides effective national program management for the FBI IPR program by aggressively advocating program awareness, coordinating and deconflicting investigative activity, and proactively developing relationships to address current and emerging threats to U.S. intellectual property. Second, it initiates and conducts IPR investigations that are complex, multi-jurisdictional and/or international in nature.

The IPRU is the coordination center for field office efforts to investigate IPR violations and other FBI divisions that conduct investigations with an IPR nexus. For example, the Criminal Investigative Division's Organized Crime Unit investigates cases involving counterfeit health products. The Counterintelligence Division's Economic Espionage Program focuses on the theft of trade secrets by foreign agents, governments and instrumentalities as defined by the Economic Espionage Act of 1996. Collaboration with these two divisions on IPR cases functions as a force multiplier and leads to broader criminal charges and higher penalties for offenders.

The FBI and the PRO IP Act

As a result of the PRO IP Act, the FBI Cyber Division has 51 dedicated IPR special agents placed in 21 field offices and the IPRU. The first enhancement under the Act, in April 2009, resulted in the allocation of 26 positions in the field and five at the IPRU. A second enhancement in May 2010 led to the allocation of an additional 20 positions in the field. Of these 51 positions, 44 special agents were placed in 20 field offices where United States Attorneys' Office (USAO) had Computer Hacking and Intellectual Property (CHIP) Units. The FBI office in Houston was allocated two IPR agents, even thought there is not a CHIP unit there, for a total of 46 agents in the field.

As part of this allocation, the field offices in Los Angeles, New York, San Francisco, and Washington, D.C. received an enhancement to establish dedicated IPR squads. Each of these offices has established IPR task forces or working groups to coordinate IPR enforcement efforts and conduct outreach to industry and rights holders.

This distribution of investigative resources maximizes the nationwide reach and ability of the FBI to disrupt and dismantle international and domestic manufacturers or distributors of counterfeit and pirated goods, and criminal

organizations engaged in IPR crime. The locations for the distribution of these resources were selected based on a regional domain analysis of the threat to intellectual property, intellectual property threat intelligence reporting, input from the IPR Center, and an understanding that the geographically-dispersed nature of IPR violations and subject locations made it possible to establish venues regionally. The placement of the special agents was coordinated with and approved by the Office of the Deputy Attorney General and the Executive Office of the United States Attorneys.

As of May 31, 2011, the FBI had 471 pending IPR investigations with 46 special agent positions dedicated to working IPR matters in the field. In FY 2010, the number of new FBI initiated theft of trade secrets and health and safety cases increased by 42 percent over FY 2009. The use of sophisticated investigative techniques increased by 50 percent in IPR cases.

In addition to the placement of IPR dedicated agent resources, in the spring of 2010, the IPRU management team conducted a case review of all pending IPR cases to support the shift of resources to priority investigations.

Strategic Initiatives and Successes

Capitalizing on the resources from the PRO IP Act, the FBI has enhanced its engagement on a number of significant strategic initiatives. This engagement has sharpened the focus of the FBI's IPR program on priority threats, increased awareness of the threat landscape, and strengthened relationships with community partners.

The FBI established and leads the Intelligence Fusion Group (IFG) at the IPR Center. Together the partner agencies define the IPR threat picture, share tactical and strategic intelligence, produce joint intelligence products, and develop the national strategy to address IPR crimes. Through the IFG, the FBI led a comprehensive analysis of the global threat to U.S. interests from criminal IPR violations. The report, entitled "Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad," is the culmination of a year-long joint effort led by the FBI and ICE with contributions from IPR Center partners. As part of this effort, agents and analysts interviewed 126 IPR experts from corporate security offices, industry associations, government agencies, and academic institutions in the U.S., India, and China regarding IPR threats. A survey accompanying the report will solicit feedback and additional information to help determine additional targeted analysis opportunities.

To address the problem of counterfeit aircraft parts entering the commercial and military repair or manufacturing supply chain, the FBI, Department of

Transportation Office of Inspector General and Federal Aviation Administration jointly coordinated the "Fractured Skies" initiative. As part of this effort, the IPRU has engaged the National Cyber-Forensics & Training Alliance, located in Pittsburgh, PA, for analytical review and target package development.

In an effort to improve international relationships on IPR investigations, conduct threat assessments, and make recommendations on the strategic plan in high threat countries, the IPRU embedded a dedicated IPR team comprised of an analyst and an agent in the FBI's Legal Attaché offices in Beijing and New Delhi to work directly with local and regional authorities on IPR matters for 60 days. Based upon the results of this effort and the threat emanating from these regions, the IPRU is currently in the process of embedding a fulltime IPR dedicated agent in Beijing for a year.

To capitalize on private sector partnerships, the FBI created a working group consisting of corporate security officers from Fortune 100 companies to focus on bolstering relationships of trust between law enforcement agencies and industry and improving information-sharing regarding intellectual property theft. In February 2011, the FBI hosted key industry Chief Security Officers to kick-off the Intellectual Property Threat Small Working Group. The goal of this working group is to build liaison among industry peers in an effort to generate high priority IPR cases. To this end, the FBI is currently developing targeted education and awareness presentations for corporate executives and general counsels.

Additionally, the FBI has taken over the hosting of the IPR Center's website, www.IPRCenter.gov. Phase two of this project will kick off later this year and involved a significant redesign of the site so that it includes training, education, enforcement activities and a reporting mechanism for IPR tips. The FBI is working in concert with the IPR Center partners to ensure comprehensive coverage of IPR issues and make this site the "go to" site for all IPR enforcement.

Training and Capacity Building

In order to promote high standards of IPR protection and the enforcement of laws protecting intellectual property, the FBI places a heavy emphasis on meaningful training and capacity building. The FBI provides training on IPR enforcement to an increasing number of individuals each year. In FY 2009, the FBI provided IPR training to 782 individuals from the federal government, the domestic private sector, foreign governments, and the overseas private sector. In FY 2010, the FBI trained 1678 such individuals. As of May 2011, the FBI has already trained 1064 individuals. As described below, the FBI provides training to its own personnel and its domestic and international counterparts in a number of

different ways. Resources from the PRO IP Act have made these ambitious and important training programs possible.

In September 2010 the IPRU provided its second annual, comprehensive IPR program training for IPR dedicated special agents. Additionally, special agents new to the IPR program received an introductory basic training course, and all IPR special agents participated in an advanced course to build upon existing skill sets and share the latest investigative techniques and technological methods. IPR program coordinators in offices currently without funded IPR positions also received this annual training to ensure maximum regional coverage and to provide support to the CHIP units. The training session explored the forensic aspects of IPR investigations, to include the mechanisms necessary to identify counterfeits, the utilization of undercover operations, and IPR evidentiary procedures. Training topics also covered statutory authorities, DOJ enforcement efforts, major case initiatives, case studies, intelligence analysis for IPR cases, and federal partnering efforts. Industry subject matter experts from the International Anti-Counterfeiting Coalition, Underwriters Laboratories, Eli Lilly, Cisco Systems, the Motion Picture Association of America, and Microsoft made presentations.

All cyber career path designated special agents receive supplemental IPR training during a two-week New Agent Training (NAT) program. This training consists of an IPR program overview, a PRO IP Act overview, IPR case initiation/investigative techniques, and guidance regarding the importance of interagency partnerships, and the benefits of industry coordination efforts. The agents also receive forensic training from the Computer Analysis Response Team (CART) of the Operational Technology Division at FBI.

The IPRU recently developed a comprehensive web based training module specifically designed for agents working on IPR investigations. This module will be placed on our online training academy in the very near future.

The FBI also provides cross-program IPR training to organized crime and counterintelligence special agents and training on organized crime and counterintelligence to IPR dedicated special agents. This cross-program training was designed to ensure that agents pursue all avenues of investigation in cases that involve organized crime, counterintelligence and IPR issues.

The FBI provides IPR training to domestic and international law enforcement officials. The FBI is collaborating with its partner agencies to develop more comprehensive and advanced intellectual property training curriculum. The curriculum will ensure a uniform foundation across law enforcement agencies conducting IPR investigations and provide state and local law enforcement and industry liaisons with information about how to most effectively partner with the

federal government on IPR investigations. For example, the FBI contributed training material and support to INTERPOL's new Intellectual Property Crime College, an online resource available to law enforcement officers and industry partners worldwide.

Over the last two years, the FBI, through the IPRU, provided training on IPR to law enforcement officials from 15 different countries. For example, in September 2010, the FBI provided training during the 6th INTERPOL and Korea Copyright Commission Conference in Seoul, South Korea. It was the first to be held in the INTERPOL Asia and Pacific Region and was delivered with the support of the INTERPOL Liaison Office Bangkok for Asia and Pacific Region. The target audience included regional police middle managers with responsibility for investigating transnational organized intellectual property crime. The training provided attendees with a common understanding of the nature and extent of regional and increasingly global transnational organized intellectual property crime and investigative best practices techniques. It illustrated the benefits of working together with industries affected by intellectual property crime.

Additionally, the FBI provided training to the U.S. Patent and Trademark Office and its international attachés. The FBI's use of PRO IP Act resources has permitted an increased focus on training in high priority areas; this has directly contributed to increases in the quantity and quality of IPR cases.

Investigative Accomplishments

Pro IP Act resources have directly contributed to the FBI's development of strategic initiatives, training of its agents and counterparts, and increased capacity to combat high priority IPR crime. As a result, over the past year, the FBI and its partners have successfully investigated major IPR violations that resulted in millions of dollars in losses and unquantifiable harm to human health and safety. The following are but a few examples.

Earlier this year, a former Apple employee pled guilty to his role in a scheme to defraud Apple, Inc. while he was employed with the company from 2005 through 2010. The FBI investigation began in April 2010, when Apple found evidence of a kickback scheme on the employee's laptop. The employee transmitted Apple's confidential information, such as product forecasts, roadmaps, pricing targets, product specifications, and data obtained from Apple's business partners, to suppliers and manufacturers of Apple parts. In return, the suppliers and manufacturers paid kickbacks, including payments determined as a percentage of the business they did with Apple. The scheme enabled the suppliers and manufacturers to, among other things, negotiate more favorable contracts with Apple than they would have been able to obtain without the confidential information.

A joint investigation with an FBI counterintelligence squad revealed that General Motors (GM) was allegedly the victim of a conspiracy by a former GM employee and spouse to steal GM's hybrid vehicle technology with the intent to sell it to a Chinese automaker. The stolen GM documents were valued at over $40 million. The couple was arrested on July 22, 2010. Last year, the FBI initiated a case involving the theft of trade secrets at Societe Generale (SocGen). On November 19, 2010, the former employee was found guilty of theft of trade secrets and interstate transportation of stolen property for stealing the proprietary computer code used in SocGen's high-frequency trading system; he was sentenced to three years in prison.

Similarly, a former employee of Goldman Sachs was convicted for theft of trade secrets in 2010. The defendant, a computer programmer, was accused of stealing trading software by uploading a proprietary trading platform program for equity products to a server in Germany. The FBI was able to seize the server in question and block access to the site. Goldman Sachs could not put an exact dollar amount on the software taken, but media reports have indicated that Goldman made in excess of $300 million in one year through its use of high frequency program trading and would not license the software for anything less than $1 billion. In December 2010, a federal jury found the defendant guilty of theft of trade secrets; in March 2011, he was sentenced to 97 months in prison. Highlighting the potential for safety risks associated with some IPR violations, a Canadian man was sentenced to 33 months in prison for selling fake cancer medication on the Internet. Initial investigation into the sale and distribution of copyrighted media revealed that the subject was marketing fake cancer treatment drugs, which he admitted to selling to at least 65 cancer patients. In addition to his prison sentence, he was ordered to pay a $75,000 fine and $53,724 in restitution.

In January of this year, Wayne Chih-Wei Shu pled guilty to six counts of mail fraud, one count of trafficking in counterfeit goods, and one count of trafficking in counterfeit labels, illicit labels, or counterfeit documentation or packaging. The case was initially based on intelligence provided by Microsoft's Anti-piracy group which identified Shu as one of the most prolific distributors of counterfeit Microsoft server and Office software in Washington state. The investigation resulted in the seizure of the counterfeit evidence, as well as a forfeiture judgment for the sum of $1,750,396.98, for real and personal property, cash, and illicit proceeds.

Conclusion

As the Committee knows, law enforcement faces significant challenges in our efforts to protect IPR, thereby protecting U.S. IP right holders and the health and safety of American citizens.

With the support of the PRO IP Act, however, the FBI is in a position to aggressively investigate the domestic and international criminal organizations that profit from the theft of intellectual property. The PRO IP Act has enabled the FBI to dedicate increased numbers of special agents and analysts to IPR matters, ensure quality training, and support effective interagency collaboration.

Combined with our ongoing efforts to strengthen our relationships with industry, partner with our counterparts in the IPR Center and improve our collaboration with our international law enforcement partners, these efforts will enhance our ability to identify and neutralize those who perpetrate IPR crimes. We look forward to working with the Committee and Congress as a whole to continue on a successful course forward for the nation that protects intellectual property and its citizens. Thank you for the opportunity to be here. I would be happy to take any questions.

New Zeus emails cloaked as Fed, IRS messages

http://www.scmagazineus.com/new-zeus-emails-cloaked-as-fed-irs-messages/article/205920/

Small and midsize organizations may want to take note: There is a particularly large Zeus spam campaign making the rounds. The e-mails piggyback on two trusted names — the Federal Reserve and the Internal Revenue Service (IRS) — to incite recipients to take unwise actions.

Researchers at Barracuda Labs first spotted the huge uptick in the malicious messages June 20, when the e-mails were blocked before reaching some 120,000 users within 10 minutes. In particular, the e-mails claiming to originate from the Federal Reserve appear to target individuals in charge of an organization's finances. The body of the messages encourage recipients to click on a malicious link for more information about a wire fund transfer that was not processed. Users who click on the link are asked to install an executable, which actually is the data-stealing Zeus trojan, notorious for keylogging the corporate banking credentials belonging to small and midsize businesses, school districts, and charities.

On June 22, the fraudsters switched their tactics to leverage the IRS name in their e-mails. The messages contained the same payload, but victims were told their federal tax payment was canceled by their bank, and they were encouraged to click on the malicious link for further details.

Please see full details at the web site connected to the above hyper-link.

JULY IN COUNTERINTELLIGENCE HISTORY

- July 1st, 1963: Gennadiy Sevastyanov, Cultural Attache at the Soviet Embassy, Washington DC, was declared persona non grata by the State Department when it was learned that he had tried to use the brother of a defector to contact the defector who was then working for a U.S. government security agency.
- July 1st, 1988: Eighty-seven Soviet observers took up residence at U.S. military nuclear facilities in connection with the Intermediate Nuclear Force Treaty, thus increasing the FBI's foreign counterintelligence responsibilities.
- July 12th, 1966: Retired U.S. Army Lieutenant Colonel William Henry Whalen was arrested on this date in Alexandria, VA for conspiracy to commit espionage on behalf of the Soviet Union. He was subsequently sentenced to 15 years in prison.
- July 17th, 1950: On this date Julius Rosenberg was arrested for atomic espionage. He and his wife Ethel were subsequently convicted, sentenced to death, and executed on June 19th, 1953.
- July 24th, 1950: Noting previous presidential directives from 1939 and 1943 directing the FBI to take charge of investigative work in matters relating to espionage, sabotage, subversive activities and related matters, President Truman on this date reconfirmed the FBI's authority to investigate domestic security matters.

PRESENTATIONS AND OUTREACH

The CI Strategic Partnership Newsletter is a product of the FBI's Counterintelligence Program Coordination Section which plays a key role in protecting our sensitive technologies from our adversaries.

The Challenge: to protect United States sensitive information, technologies and thereby competitiveness in an age of globalization.

Our Solution: to foster communication and build awareness through partnerships with key public and private entities, by educating, and enabling our

partners to identify what is at counterintelligence risk and how to protect it. We call it "knowing your domain"—identifying the research, information and technologies that are targeted by our adversaries, and establishing an ongoing dialog and information exchange with partners, the goal of which is to change behaviors and reduce opportunities that benefit the opposition's efforts.

The United States is a world's leader in innovation. Consider the breakthrough research and development that's taking place on the nation's campuses and in research facilities—often on behalf of the government. Sensitive research, much of which occurs in the unclassified realm, is the key to our nation's global advantage, both economically and militarily.

The Counterintelligence (CI) Program Coordination Section is responsible for determining and safeguarding those technologies which, if compromised, would result in catastrophic losses to national security. Through our partnerships with businesses, academia, and US Government agencies, the FBI and its counterintelligence community partners are able to identify and effectively protect projects of great importance to the U.S. Government. This provides the first line of defense inside facilities where research and development occurs and where intelligence services are focused.

The FBI's outreach efforts continue to evolve. This newsletter is one way we hope to expand our outreach to the elements of our "CI Domain." We continue in contacting businesses and organizations with which we have not yet made personal contact. In support of its Counterintelligence Domain/Strategic Partnership Program, the Federal Bureau of Investigation hosts an annual Research and Technology Protection (RTP) Conference for Facility Security Officers and RTP Professionals. Unclassified presentations address specific country threats to your technology, industrial and economic espionage, counterintelligence threat issues, and computer intrusion/cyber threat matters. The annual RTP Conference is offered in two locations during the year: Orlando and Clearwater.

The FBI's Domain/Strategic Partnership Program seeks to interface with private industry, high tech companies, research institutes, any stakeholder and/or

contractor that design, develop, produce, and distribute critical information and technologies. Our job is to establish contact with these "Domain entities" in our territory, and assist them to better understand the foreign intelligence threat, and improve their ability to institute protective mechanisms. In addition to hosting an annual Research Technology Protection (RTP) Conference for security professionals, we also provide security awareness threat briefings to our defense contractor partners, high tech companies and research institutes. To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

James "Pat" Laflin (James.Laflin@ic.fbi.gov) 813.253.1029

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000