FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

May 1, 2011
Volume 3 Issue 5

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

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

ECONOMIC ESPIONAGE; NATIONAL SECURITY DIVISION ANNOUNCES FARA EFILE FOR FOREIGN AGENTS REGISTRATION ACT ELECTRONIC FILING

Economic Espionage

Many of the arrests, trials and convictions highlighted in our monthly newsletters do not involve classified, U.S. Government information. Rather often, the targeted information involves the trade secrets, the proprietary information, the intellectual property powering our businesses and industries.

In the mid 1990's, much like it is today, the theft of intellectual property was occurring with growing frequency. In one particular case, a small Colorado software company had developed a software product, at the cost of approximately ten million dollars. When an employee stole the source code by copying it onto a floppy disk, and then sent the code out of the country to a foreign competitor, the only criminal charges that could be filed were for the interstate transportation of stolen property (ITSP) (i.e. the physical removal of the disk containing the source code, not the source code itself).

When the ITSP charges were filed, the prosecutors discovered that even ITSP could not be charged. Why? Because the item stolen must have a physical value of a minimum of five thousand dollars. The intellectual property contained on the disk might have been worth millions of dollars, but the disk it was contained on was worth maybe a dollar. Hence, the criminal behind this theft faced no criminal charges.

Because of incidents such as this, then FBI Director Louis Freeh pushed for the enactment of a law that allowed for the protection of intellectual property. In October, 1996, the Economic Espionage Act was signed into law.

When we go out to give our presentations, we discuss the theft of trade secrets. As noted in the article below, trade secrets must be protected: "… the owner has taken reasonable measures to protect…" to be considered trade secrets. Taking some of the proactive steps laid out in this article can be useful in protecting your trade secrets, as well as protecting the potential for civil or criminal charges to be filed if your trade secrets have been stolen.

Economic Espionage
http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage

Introduction

The Cold War is not over, it has merely moved into a new arena: the global marketplace. The FBI estimates that every year billions of U.S. dollars are lost to foreign and domestic competitors who deliberately target economic intelligence in flourishing U.S. industries and technologies, and who cull intelligence out of shelved technologies by exploiting open source information and company trade secrets. Foreign competitors who criminally seek economic intelligence generally operate in three ways:

1. They aggressively target and recruit insiders (often from the same national background) working for U.S. companies and research institutions;

2. They conduct economic intelligence through operations like bribery, cyber intrusions, theft, dumpster diving (in search of discarded intellectual property or prototypes), and wiretapping; and,

3. They establish seemingly innocent business relationships between foreign companies and U.S. industries to gather economic intelligence, including trade secrets.

In an effort to safeguard our nation's economic secrets, the Economic Espionage Act (EEA) was signed into law on October 11, 1996.

How to Protect Your Business from Espionage: Six Steps

1. Recognize there is an insider and outsider threat to your company.

2. Identify and valuate trade secrets.

3. Implement a proactive plan for safeguarding trade secrets.

4. Secure physical and electronic versions of your trade secrets.

5. Confine intellectual knowledge on a "need-to-know" basis.

6. Provide training to employees about your company's intellectual property plan and security.

Definitions

Economic Espionage is (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent. (Title18 U.S.C., Section 1831).

Trade secrets are all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing, which the owner has taken reasonable measures to protect; and has an independent economic value. "Trade secrets" are commonly called classified proprietary information, economic policy information, trade information, proprietary technology, or critical technology.

Theft of trade secrets occurs when someone (1) knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to (2) knowingly benefit anyone other than the owner. Commonly referred to as Industrial Espionage. (Title 18 U.S.C., SECTION 1832).

A Foreign Agent is any officer, employee, proxy, servant, delegate, or representative of a foreign government.

A Foreign Instrumentality is defined as: (1) any agency, bureau, ministry, component, institution, or association; (2) any legal commercial or business organization, corporation, firm, or entity; and, (3) substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government.

Statutory authority: The Economic Espionage Act (EEA) of 1996
TERRITORIAL LIMITS: EEA protects against theft that occurs either (1) in the United States, or (2) outside the United States and (3) an act in furtherance of the offense was committed in the United States, or (4) the violator is a US person or organization.

Frequently Asked Questions

What are some methods of targeting or acquiring trade secrets?

1. Steal, conceal, or carry away by fraud, artifice, or deception;

2. Copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey; and,

3. Receive, buy, or possess a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

Does the Economic Espionage Act of 1996 apply if the offender is a foreign person?

Yes. The Act states that (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit anyone other than the owner. Other elements will apply for prosecution.

Does the Economic Espionage Act of 1996 apply if it occurs outside the United States?

Yes. However, the violator must be (1) a US person or organization; or (2) an act in furtherance of the offense was committed in the United States.

Are there other statutes that can apply if trade secrets are not classified and therefore cannot be prosecuted under the Economic Espionage Act of 1996 Title 18 U.S.C. Section 1831 and 1832?

Yes. The following is a list of violations that may apply: mail fraud, wire fraud, interstate transportation of stolen property, export control, and misuse of a computer system. Contact your local FBI for further assistance.

Is the FBI proactive in its approach to economic espionage?

Yes. FBI Director Robert Mueller has designated counterintelligence as the FBI's number two priority, second only to counterterrorism. The Economic Espionage Unit is dedicated to countering the economic espionage threat to include developing training and outreach materials; participating in conferences; visiting private industry; working with the law enforcement and intelligence community on requirement issues; and providing specific classified and unclassified presentations.

National Security Division Announces FARA eFile for Foreign Agents Registration Act Electronic Filing

Department of Justice
Office of Public Affairs

http://www.justice.gov/opa/pr/2011/April/11-nsd-484.html

FOR IMMEDIATE RELEASE Friday, April 15, 2011

New Online Portal for FARA Registration and Payment Process

WASHINGTON – The Justice Department's National Security Division today announced the launch of a system for the electronic filing of registration statements and supplements with the Justice Department under the Foreign Agents Registration Act (FARA). Called FARA eFile, the system enables FARA registrants to electronically file documents with the FARA Registration Unit, which is part of the Counterespionage Section of the Justice Department's National Security Division.

Under FARA, which was amended by the Honest Leadership and Open Government Act of 2007, FARA registrants shall file registration statements and supplements in electronic form. FARA eFile is an intuitive online shopping cart process that allows registrants to register and pay the required registration fees online, 24 hours a day, seven days a week, demonstrating another enhancement to the department's FARA website. FARA eFile will result in more timely public disclosure and transparency while promoting more efficient practices.

Passed by Congress in 1938, FARA is a public disclosure statute that requires all persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities.

The purpose of FARA is to protect the national defense, internal security and foreign relations of the United States by requiring public disclosure by persons engaged in certain activities on behalf of foreign principals to ensure the American public and its lawmakers know the source of the information intended to sway public opinion, policy and laws. The law facilitates evaluation by the government and the American people of the statements and activities of such persons in light of their associations.

FARA eFile can be accessed at www.fara.gov and is linked through the home page of the National Security Division at www.usdoj.gov/nsd/ . Additional information about FARA eFile can also be found at www.fara.gov/efile-faq.html.

ARRESTS, TRIALS AND CONVICTIONS

Chinese National Sentenced Today For Stealing Ford Trade Secrets

http://www.justice.gov/usao/mie/news/2011/2011_4_12_xyu.html

FOR IMMEDIATE RELEASE

April 12, 2011

Former Ford employee, Xiang Dong Yu, aka Mike Yu, 49, of Beijing, China, was sentenced today to 70 months in federal prison and ordered to pay a fine of $12,500 as a result of having pleaded guilty in federal court to two counts of theft of trade secrets, announced Barbara L. McQuade, United States Attorney for the Eastern District of Michigan. McQuade was joined in the announcement by Andrew G. Arena, Special Agent in Charge of the FBI. In addition to his custodial sentence, Chief Judge Gerald E. Rosen ordered that Mr. Yu be deported from the United States upon completion of his sentence.

According to the plea agreement in this case, Yu was a Product Engineer for the Ford Motor Company from 1997 to 2007 and had access to Ford trade secrets, including Ford design documents. In December 2006, Yu accepted a job at the China branch of a U.S. company. On the eve of his departure from Ford and before he told Ford of his new job, Yu copied some 4,000 Ford documents onto an external hard drive, including sensitive Ford design documents. Included in those documents were system design specifications for the Engine/Transmission Mounting Subsystem, Electrical Distribution system, Electric Power Supply, Electrical Subsystem and Generic Body Module, among others. Ford spent millions of dollars and decades on research, development, and testing to develop and continuously improve the design specifications set forth in these documents.

The majority of the design documents copied by the defendant did not relate to his work at Ford. On December 20, 2006, the defendant traveled to the location of his new employer in Shenzhen, China, taking the Ford trade secrets with him. On January 2, 2007, Yu emailed his Ford supervisor from China and informed him that he was leaving Ford's employ.

The plea agreement further states that in November 2008, the defendant began working for Beijing Automotive Company, a direct competitor of Ford. On October 19, 2009, the defendant returned to the United States, flying into Chicago from China. Upon his arrival, the defendant was arrested on a warrant issued upon the indictment in this case. At that time, the defendant had in his possession his Beijing Automotive Company laptop computer. Upon examination

of that computer, the FBI discovered that forty-one Ford system design specifications documents had been copied to the defendant's Beijing Automotive Company work computer. The FBI also discovered that each of those design documents had been accessed by the defendant during the time of his employment with Beijing Automotive Company.

"We will vigilantly protect the intellectual property of our U.S. automakers, who invest millions of dollars and decades of time in research and development to compete in a global economy," McQuade said. "Those who do not play by the rules will be brought to justice."

Special Agent Arena stated, "Michigan, as well as the rest of the United States, is significantly impacted by the auto industry. Theft of trade secrets is a threat to national security and investigating allegations involving theft of trade secrets is a priority for the FBI. The FBI will continue to aggressively pursue these cases."

The investigation of this case had been conducted by the Federal Bureau of Investigation. This case is being prosecuted by Assistant U.S. Attorney Cathleen Corken.

Ex-Army analyst pleads guilty to theft

http://newsok.com/ex-army-analyst-pleads-guilty-to-theft/article/3551538

Liangtian Yang, a former U.S. Army analyst who tried to board a flight to China with electronic files containing restricted Army documents, pleaded guilty to theft of government property in U.S. District Court in Lawton and was sentenced to three years of probation.

By The Associated Press Associated Press

Published: March 25, 2011

LAWTON — A former U.S. Army analyst who tried to board a flight to China with electronic files containing restricted Army documents pleaded guilty Thursday to theft of government property in a case the defense insisted was about carelessness, not espionage.

Liangtian Yang entered the plea in U.S. District Court in Lawton and was sentenced to three years of probation by U.S. Magistrate Shon T. Erwin. Yang faced up to a year in prison and a $100,000 fine on the misdemeanor charge. Assistant U.S. Attorney Robert Gifford II had asked for five years of probation but did not seek a fine.

'Really bad mistake'

Afterward, defense attorney John Zelbst said Yang, also known as Alfred Yang, made a mistake when he tried to take the manuals out of the country without the required permission.

"It was careless," Zelbst said. "Alfred did some things that were probably irresponsible. It's not an espionage case. It's a case of a really bad mistake." Yang, a 26-year-old former field artillery analyst at Fort Sill, entered the guilty plea seven months after he was detained on Aug. 24 at the Minneapolis-St. Paul International Airport following a security screen before a Tokyo-bound flight with China as its final destination. Investigators found copies of Army field manuals on multiple launch rocket systems on his computer equipment.

"There were several manuals," Gifford told Erwin during a sentencing hearing. Although none were classified as top secret, they were restricted, he said.

Yang, who was dressed in casual clothes and was almost inaudible as he spoke to the magistrate, admitted he obtained the manuals through his employment at Fort Sill and that they were still on his computer as he tried to leave the U.S. Yang lost his security clearance on Aug. 16 after Army officials learned he had not reported getting married as required. Yang's wife is a Chinese citizen.

Defense attorney David Butler compared the case to one of shoplifting and said Yang had cooperated with government investigators as they tried to determine whether he was a threat to national security.

"He's done everything he possibly could," Butler said. He asked Erwin to give Yang credit for the 70 days he spent in pretrial detention in Grady County and impose just one year of probation.

Erwin indicated he believes the case was more serious.

"This is not garden-variety theft of government property case," Erwin said. "Five years is too long. One year is not enough."

Probation terms

Erwin said Yang will be bound by the terms of a plea agreement during his three-year probationary period, including a requirement that he not seek employment to do anything that requires a security clearance. Yang, who has surrendered his passport, also agreed not to contest any discharge he receives from the Oklahoma Army National Guard that is less than honorable.

Authorities have said Yang, of Lawton, has lived in the U.S. since 2001 and became a U.S. citizen in 2006. Zelbst said Yang, his wife and their 18-month-old son were returning to China so he could complete his doctoral degree. Yang received a bachelor's degree in business at the University of Oklahoma and a master's degree at Cameron University in Lawton, he said.

Zelbst said Yang and his wife, who holds a doctoral degree in engineering, are currently unemployed.

Read more: http://newsok.com/ex-army-analyst-pleads-guilty-to-theft/article/3551538#ixzz1IIq0RxOP

News reports allowed in NSA espionage trial

http://articles.baltimoresun.com/2011-03-31/news/bs-md-drake-hearing-20110331_1_nsa-employee-jury-trial-national-security-agency

Ex-employee accused of giving information to reporter

March 31, 2011|By Tricia Bishop, The Baltimore Sun

A federal judge said Thursday that he would allow Baltimore Sun articles about program and management problems at the National Security Agency to be admitted as evidence in the June trial of Thomas Drake, a former NSA employee accused of retaining classified documents to give to a reporter.

But the judge stopped short of allowing the reporter, identified in court papers as former Sun journalist Siobhan Gorman, to be called to the witness stand. District Judge Richard D. Bennett said that path could end in a "deep, dark hole," and that he's not inclined to jail reporters for refusing to reveal sources. Bennett's statements came in a four-hour hearing to determine how the two-week jury trial will proceed.

Drake, who worked as a contractor at the NSA from 1991 to 2001 and later as an agency employee until mid-2008, was indicted last April under the Espionage Act. Drake has pleaded not guilty to the 10 felony counts of illegally retaining national defense information, obstructing justice and lying to the FBI.

Drake is not charged with leaking the information, though the accusation is central to the government's case against him. As Bennett noted, sections of the indictment detail Drake's alleged interactions with Gorman, identified as "Reporter A."

The indictment alleges that they exchanged hundreds of email messages through encrypted accounts and met a half-dozen times at Washington-area locations. Gorman wrote a series of articles published in The Sun in 2006 and 2007 that revealed flaws in expensive anti-terrorism technology programs embraced by the NSA.

"We can't get away from the fact that this is more than a simple possession case. The government is making Tom's contact with the reporter an issue," said Maryland Federal Public Defender James Wyda, who represents Drake.

Defense attorneys want to introduce the articles to show that the classified information found in Drake's custody was not included, indicating that he never leaked it to Gorman. Prosecutors say that would prove nothing, however, because journalists select the content they use and she could simply have omitted the details.

"He brought the documents home because he was asked to do research by the reporter. … What ultimately happens with that information is simply not relevant," said William M. Welch II, a Justice Department lawyer.
Bennett told Welch he was free to argue that before the jury but that the articles could be used as evidence at the trial.

Drake has acknowledged showing two documents to Gorman that he believed were not classified, said Wyda, who described the documents as a meeting schedule and an email about an NSA success. Three other, allegedly classified documents found in his possession were there because Drake was a witness in a whistle-blower investigation by the Defense Department's inspector general, Wyda said.

"I'm not conceding [Drake] did anything wrong," Wyda said, adding that his client "went to the reporter because" some of Drake's other whistle-blower efforts had failed to get results.

"Nothing changed," Wyda said, so Drake "took the risk to give [information] to a reporter in violation of NSA regulations."

The judge rejected a defense request challenging the Espionage Act and parts of the Classified Information Procedures Act, which sets protocols for dealing with sensitive information, as unconstitutional. Bennett said he will present written opinions discussing his rulings on both motions.

Chinese Nationals Charged with Illegally Attempting to Export Military Satellite Components

http://www.outlookseries.com/A0997/Security/3454_Hong_Wei_Xian_Harry_Zan_Li_Li_Lea_Li_Chinese_Nationals_Charged_Indicted_Export_Military_Satellite_Components_PRC.htm

April 5, 2011

Hong Wei Xian, aka "Harry Zan," & Li Li, aka "Lea Li Chinese Nationals Charged with Illegally Attempting to Export Military Satellite Components to the PRC
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.

Hong Wei Xian, aka "Harry Zan," 32, and Li Li, aka "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 and to smuggle goods from the United States and the attempted export of U.S. 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 U.S. 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 of the PRC for delivery to avoid drawing attention to the orders.

On Sept. 1, 2010, the defendants were arrested in Hungary pursuant to a U.S. 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 U.S. 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.

'Supreme Commander' of phony army unit that recruited Chinese nationals charged

http://newsfeedresearcher.com/data/articles_n16/deng-military-unit.html#hdng3

The 51-year-old El Monte man allegedly recruited other Chinese nationals, primarily in the San Gabriel Valley, to join. He is accused of providing recruits with phoney U.S. Army uniforms, fake documents and military ID cards and charging them initiation fees ranging from $300 to $450, with renewal fees set at $120 a year.

A California man allegedly recruited more than 100 other Chinese nationals, gave them phony uniforms and documents, and charged them initiation dues, CNN reported. He declared himself "supreme commander" of the unit and told the recruits it was a path to U.S. citizenship. He even offered them a chance to buy a higher rank -- by paying him cash.

An El Monte man has been arrested and charged for allegedly recruiting 100 Chinese nationals to join a phony Army special forces unit that he led as "Supreme Commander," authorities said Tuesday.

The self-styled Supreme Commander of a phoney U.S. Army special forces unit was arrested and charged for allegedly recruiting 100 Chinese nationals to join the fake squad.

A Chinese national living in El Monte was arrested Tuesday for allegedly creating a phony U.S. Army special forces unit out of an office in Temple City, officials said.

As part of an immigration scam, a 51-year-old man from El Monte set up a phony Army recruitment office and charged Chinese nationals to become part of what he claimed was the U.S. Armed Forces, reports the Pasadena Star News.

"Going to the army is a way for people to get status in the U.S.," Choi said. Choi said APALC has experienced instances of groups posing as them and offering immigration workshops, including one recently in Rosemead. Choi said the group is making it a priority to be more proactive in identifying scams and encouraged those seeking immigration advice to use trusted resources, such as APALC. Deng also was charged on April 6 with one count of possession of child pornography after an earlier search of his home turned up items on his home computer, officials said.

If convicted Deng faces up to eight years, four months in prison. Deng was also charged on April 6 with one count possession of child pornography after an earlier search of his home. The pornography was found on his home computer, officials said.

Deng is to be arraigned Wednesday in Pomona Superior Court. If convicted as charged, he would face up to eight years and four months in state prison. In a separate case, Deng also was charged last week with one count of possession of child pornography, stemming from a search warrant executed at his home.

Authorities investigating the document case allegedly found child pornography on a computer, prosecutors said. He is set for arraignment in that case April 18 and would face up to three years in state prison if convicted.

Deng got a trip to jail. He's scheduled to appear in court for an arraignment hearing on Wednesday. If a jury convicts him, he faces more than eight years in state prison.

The California State Military Reserve (CSMR) is the State Defense Force of California authorized by United States Code (32 USC 109c) and the California Military and Veterans' Code (CM&VC 550). We augment the California National Guard during times of peace and war when they are activated and sent out of the state. He wanted to have a steady source of income from the overthrow of

Chinese Restaurants in the San Gabriel Valley. What I cannot believe is his being eligible for only 6 to 8 years of state prison.

The group seemed to have some type of rank system designated with striped insignias, with Deng as the "supreme commander." While prosecutors said they found evidence of more than 100 recruits, some in the Chinese American community said there appeared to be several branches of the "special forces reserve" with up to 800 members.

Recruits were allegedly charged initiation fees ranging from $300 to $450, with annual renewal fees of $120, according to Deputy District Attorney Richard Ceballos. Authorities said, recruits could increase their rank in the fraudulent unit by making cash donations to Deng. [2] Deng is suspected of charging recruits between $300 and $450, along with renewal fees of $120 each year, to be part of the unit. Recruits could move up in rank if they paid higher fees, officials said.

The unit began in October 2008 and was run out of Deng's office on Las Tunas Drive in Temple City, which was made to look like a legitimate Army recruitment office, officials said. [10] The recruits were also instructed to report to the defendant's office in Temple City, made up to look like an official U.S. military recruiting center, to undergo military training and indoctrination.

Deng allegedly provided each recruit with phony U.S. Army uniforms, fake documents and fraudulent military ID cards. [6] Most were from the L.A. area, but there were also recruits from as far away as Georgia, officials said. They were provided with fake documents and military ID cards as well as phony uniforms, apparently purchased at military surplus stores.

At the office, recruits were required to meet with Deng "to undergo military training and indoctrination," officials said. [7] Deng gave himself the title of "supreme commander" of the fake military unit, officials said.

What an alien won't do for a green card these days. For an initiation fee of up to $450 -- and $120 in annual dues -- Deng reportedly promised the "recruits" they would eventually earn U.S. citizenship. They also had the option of making cash donations to the unit in exchange for a better rank among the troops.

Deng, who is also known as Yupeng Deng, was arrested Tuesday. He was being held in lieu of $500,000 bail and was scheduled to be arraigned Wednesday at Los Angeles County Superior Court in Pomona.

Deng, 51, was arrested by Los Angeles County Sheriff's Department deputies assisting the investigation, which is being conducted by the FBI and the Department of Defense Criminal Investigative Services.

Last week, Deng was also charged with possession of child pornography. The charge stemmed from a search warrant executed on his home, the Los Angeles Times reported.

Last year, one Chinese-language newspaper reported that an Alhambra taxi driver was arrested near Los Angeles International Airport after producing counterfeit military identification while trying to get out of a traffic stop.

There have been several other cases in recent years of Chinese Americans posing as U.S. military officials.

Investigators learned that the recruits were told that the military IDs could be used to avoid getting traffic tickets and to receive certain types of military benefits and discounts, Eimiller said. Some of the recruits were so convinced that they were part of the U.S. military that they actually visited real Army recruiting centers and tried to pay their monthly dues directly to the U.S. government, Eimiller said. That was another tipoff when investigators began looking into the group. Local Chinese American leaders on Wednesday said they were shocked that a group that was such a familiar presence in the community is now being accused of being a fraud.

The Chinese-language media reported recently about a Rosemead man who went to China claiming to be a major general in the U.S. Army. The papers reported that he was treated like a dignitary in his hometown and received an audience with a Chinese military commander. Lim, the Walnut councilman, said there should be a lesson in this and other cases. "The people in the community should know this is totally illegal and not patriotic at all," he said.

4 Tennessee men plead guilty in international arms trafficking case

http://www.mmdnewswire.com/guilty-in-international-arms-trafficking-case-34778.html

NASHVILLE, Tenn. (MMD Newswire) April 1, 2011 -- Four former officers of Nashville arms manufacturer Sabre Defence Industries, LLC (SDI-US), pleaded guilty Monday to conspiring to defraud the United States and to violations of the Arms Export Control Act (AECA), following an investigation by U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

SDI-US Corporate President Charles Shearon, 55, of Ashland City, Tenn.; Chief Financial Officer Elmer Hill, 64, of Brentwood, Tenn.; Director of Marketing and Sales Michael Curlett, 44, of Hermitage, Tenn.; and International Shipping and

Purchasing Manager Arnold See, Jr., 54, of Antioch, Tenn., entered guilty pleas before Chief U.S. District Court Judge, Todd J. Campbell. Sentencing is set for Aug. 1 at 10 a.m.

The four men, along with co-conspirators SDI-US and Guy Savage 42, a citizen of the United Kingdom and owner of SDI-US, were indicted in January for conspiracy to defraud the United States, conspiracy to commit mail fraud and wire fraud, making false statements on export and import documents, and for conspiracy to violate the AECA.

"The national security implications of this case cannot be underestimated," said Raymond R. Parmer, Jr., special agent in charge of ICE HSI in New Orleans. "HSI agents in Nashville foiled a potentially dangerous smuggling scheme. In the wrong hands, technology like this could be used to inflict harm upon America or its allies."

"The illegal import, export and transfer of firearms and related components poses a great risk to America and our allies," said U.S. Attorney Jerry Martin. "Those who engage in such irresponsible and illegal activity will come to realize the commitment of our law enforcement partners to safeguarding America and the high priority given to this issue by the Department of Justice."

According to the indictment, Shearon, Hill, See, and Curlett conspired with Savage to illegally import and export regulated firearms and firearm components and technology to and from the United States.

During the plea hearings, Shearon, Hill, See, and Curlett stated that Savage directed their illegal activities from his personal residences in the United Kingdom, as well as from a related company, Sabre Defence Industries, LTD (SDI-UK), a licensed manufacturer, distributor, and importer of firearms and firearms components, also owned by Savage and headquartered in the United Kingdom. All defendants admitted that they had conspired to export firearms components, which are listed as defense articles on the United States Munitions List (USML), from the United States to an international location, without first obtaining a license or written authorization from the Directorate of Defense Trade Controls (DDTC) of the United States Department of State, as required.

They further admitted that they had conspired to import into the United States from international sources, suppressors, also known as silencers, which are also defense articles listed on the USML, without having first obtained the required license and authorization from the ATF.

The import and export of defense articles, such as firearms or firearms components or other military items on the USML, are strictly controlled by the

AECA and its attendant regulations, the International Trafficking in Arms Regulations (ITAR).

At the hearing, Shearon, Hill, and See admitted that, since 2003, they had conspired with Savage to falsify shipping records, conceal unlicensed firearms components in false bottoms of shipping cartons, and mislabel and undervalue shipments of firearm components, in an effort to avoid scrutiny by U.S. Customs and Border Protection control officers.

Curlett admitted that his participation in the conspiracy began with his employment with SDI-US in 2007. Each of the four defendants admitted that they had used email accounts and other forms of electronic communication to communicate with each other, and with Savage and other individuals located in the United States, the United Kingdom, and elsewhere, to ship firearms components from the United States to SDI-UK, without first obtaining an export license or permission and that they used international common carriers to ship the restricted items to and from the United States.

Shearon, Hill and See further admitted that, at the direction of Savage, they sought to conceal their illegal import and export activities by maintaining two sets of business books to record the company's accounts and balances, and its export and import activities. On Feb. 8, 2011, Savage was arrested in the United Kingdom with assistance from the London Metropolitan Police Service-International Assistance Unit, and the Department of Justice-Office of International Affairs. Searches were conducted in conjunction with the arrest and the Department of Justice is seeking Savage's extradition from the United Kingdom to the United States to stand trial.

Undercover agent thwarts conspiracy to export jet engines from Miami to Iran

http://www.winknews.com/Local-Florida/2011-03-23/Undercover-agent-thwarts-conspiracy-to-export-jet-engines-from-Miami-to-Iran

Story Created: Mar 23, 2011 at 7:48 PM America/New York
MIAMI, Fla. - A major crime operation is busted right here in Florida. What one group was selling inside a Miami warehouse could have threatened the nation's safety, had it not been intercepted by Homeland Security.

Four Colombian men were indicted by a Federal Grand jury in Miami for illegally trying to export 22 F-5 jet fighter engines to Iran. While it's unusual to see these kinds of items offered for sale online - which is where investigators found them -

we've learned it's not unusual for buyers around the world to try to supply our U.S. technology to other governments and even terrorists.

It was an online ad that caught the attention of Homeland Security Investigations. "That is not something we normally see," Anthony Mangione, Special Agent in Charge of Immigration and Customs Enforcement of Homeland Security Investigations in Miami.

For sale: J-85-CAN-15 aircraft engines used primarily in F-5 fighter jets. F-5s are currently used in the two countries of Venezuela and Iran. The only place you can get these parts, Mangione said, is the black market. According to the complaint affidavit, Iran produces an aircraft named "Saegeh," which is compatible with the F-5 fighter engines.

"We are seeing more and more individuals trying to get stuff to Iran," Mangione said.

On January 20th, an undercover agent responded to the ad, posing as a broker. "We met in an undercover capacity, made an offer for the engines, and that offer was then accepted," Mangione said.

The undercover agent said Iranian buyers were willing to purchase the 22 engines for $320,000.

Arrangements were made to ship them from Miami to Panama to Iran, a violation of the International Emergency Economic Powers Act banning exports to Iran.

"There is an entire industry built upon people roaming the world, literally, with sheets of information, with wish lists of governments and people who want our technology," Mangione said. "It's the best in the world and people want to do one of two things. They either want it or they want to do what we call retrofit it - figure out how it works and then try to organize defenses against it."

March 8th, Felipe Echeverry, Diego Echeverri, Amparo Echeverri Valdes, and Carlos Alfredo Pantoja-Coral were charged in the conspiracy, and the 22 engines were seized.

"People who sell these parts, people who buy these types of parts, they don't care who buys it," Mangione said. "It was a good thing it was undercover agents who bought them as opposed to representatives of the government of Iran or somebody else for that matter."

Right now, investigators are trying to figure out where these engines came from. They've had similar cases of individuals trying to get Generation 3 night vision goggles over to the Iranian army. The 4 men involved face 5 different charges, each charge carrying penalties of 5 to 20 years in prison if they're convicted.

Read more: http://www.winknews.com/Local-Florida/2011-03-23/Undercover-agent-thwarts-conspiracy-to-export-jet-engines-from-Miami-to-Iran#ixzz1IIiZnz8Q

TECHNIQUES, METHODS, TARGETS

Russian spy stiffs Yonkers on property taxes

9:22 PM, Apr. 25, 2011

The home at 17 Clifton Ave. is on the city's list of tax liens that it will sell May 11.

Written by Ernie Garcia

Westchester County, New York

Two Yonkers-based spies on the Russian payroll apparently didn't earn enough to pay their property taxes.

Former El Diario/La Prensa columnist Vicky Pelaez owes the city $10,889.60 for property taxes dating to 2009 on her home at 17 Clifton Ave. On May 11, the city will auction a lien on that property for the amount due, along with hundreds of other liens for unpaid taxes on properties throughout the city.

Pelaez and her husband, Juan Lazaro, whose real name is Mikhail Vasenkov, were arrested by the FBI in June with eight others suspected as Russian spies. Pelaez and Lazaro were accused of working for a Russian intelligence service, and federal authorities alleged that they received tens of thousands of dollars in payments in South America from their handlers, including $80,000 in February 2003.

Pelaez is listed as the home's owner on a tax sale notice published by Yonkers last week, and the couple admitted to authorities last year that the Russians paid for the house. She was forced to forfeit the house to the U.S. government when she pleaded guilty to conspiracy to act in the United States as a foreign agent of a foreign government.

A U.S. Department of Justice spokeswoman said Monday that there is no final order of forfeiture yet, so the property technically still belongs to Pelaez. Once the order is finalized, the property will be sold and outstanding taxes will be paid with proceeds from the sale.

Yonkers' website indicates that the single-family house, which sits on a 0.11-acre lot, has a full market value of $371,336. On Monday the southwest Yonkers home appeared to be unoccupied and the front door was padlocked.
Online property records indicate that Pelaez acquired the home in 1995 and paid $255,000 for it.

Pelaez is not the only noteworthy person on the city's tax lien list. Former city Councilman Stephen Kubasek owes $17,641.89 on three properties at 2, 4 and 6 Garfield St., while his relatives owe on two other properties in that vicinity.

FBI to Conduct Joint Cyber Investigations With China

http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=358

3/31/2011

NATIONAL HARBOR, Md. — Chinese hackers are suspected of perpetrating a number of cyber attacks on U.S. networks. The FBI is hoping that by working alongside cybersecurity experts in China, it can begin to gather useful intelligence about network intruders in that nation and elsewhere.

The bureau recently dispatched a cybersecurity expert to China, in an effort to work more cooperatively with Chinese authorities who oversee information networks, assistant director and head of the FBI's cyber division Gordon Snow said March 31 at the Air Force Association's "CyberFutures" conference.

FBI teams work with law enforcement and cyber agencies around the world, including in such places as Estonia, Romania and Colombia. But this is the first time an agent will be part of joint cybersecurity efforts with China, Snow said. China has been under political fire over the past couple of years for being suspected of initiating attacks on networks of U.S. government agencies, defense contractors and corporate giants like Google. Unlike other U.S. agencies tasked with cyber-related missions, the FBI does not defend a network. The bureau focuses on the difficult problem of determining the source of the attacks.

"I'm trying to find the person behind the keyboard," Snow said. "I want to know his plans and intentions."

The FBI's National Cyber Investigative Joint Task Force has three arms — an information operations group working out of Northern Virginia, an analysis branch in Maryland and a law enforcement operation also in the Washington, D.C. area. The task force works with 18 other organizations across the federal government, including NASA and the State Department.

The FBI tracks down cyber terrorists and hackers, Snow said. The bureau also collects intelligence on extremists who are using the Internet to communicate with, recruit and radicalize like-minded individuals. Or, it may investigate hackers who are increasingly showing themselves to be as sophisticated as state-sponsored organizations and large corporations, Snow said.

In addition to attributing attacks, the FBI must identify victims and notify them of intrusions.

Snow offered advice to those in charge of protecting critical networks. He said they must accept three things: They will be hacked, they might not know who did it and they have to be prepared to operate without access to critical information.

Espionage Via Spoofed White House eCard

http://www.networkworld.com/community/print/70268

By *Ms. Smith*
Created *Jan 3 2011 - 3:57pm*

When many people were caught up in the warm fuzzy feeling of peace on earth and goodwill toward man, it may have felt rewarding to receive a Christmas eCard from The White House. The bad news is that the spoofed whitehouse.gov seasons greetings contained malware aimed at espionage and sucked up several gigabytes of sensitive government documents. Some of the victims worked on cybersecurity as government employees and contractors.

It is currently unknown how many people received the following message on Dec. 23:

Figure 1. Screenshot of spammed message

Figure 2. Screenshot of malicious HTML page [1]

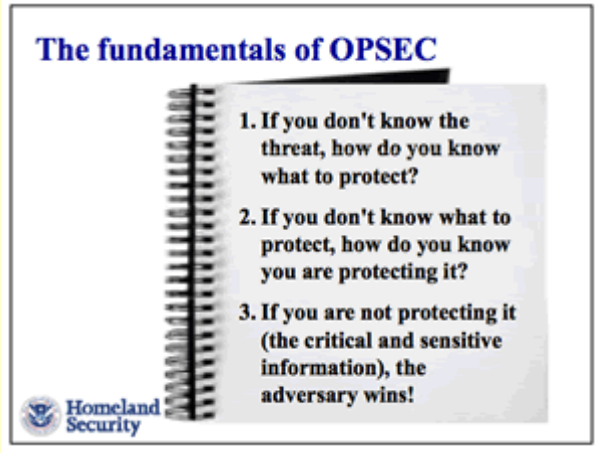
"As you and your families gather to celebrate the holidays, we wanted to take a moment to send you our greetings. Be sure that we're profoundly grateful for your dedication to duty and wish you inspiration and success in fulfillment of our core mission."

Regarding this Zeus banking Trojan variant, security blogger Mila Parkour wrote [2], it "appears to be designed for stealing documents as opposed to stealing passwords and banking information. This places this particular trojan in the category of malware designed for data theft and political/corporate espionage."

Any recipient who clicked on the links and opened the card.zip file were then infected with a Zeus Trojan variant that snatched documents and passwords and then uploaded the stolen data to a server in Belarus.

Security expert Brian Krebs wrote [3] in "White House eCard Dupes Dot-Gov Geeks" that he "analyzed the documents taken in that attack, which hoovered up more than 2 gigabytes of PDFs, **Microsoft Word** and **Excel** documents from dozens of victims."

Krebs identified some of the victims who fell for the scam e-mail as employees for various governments. These three stood out the most to me:



[3]-An intelligence analyst in **Massachusetts State Police** gave up dozens of documents that appear to be records of court-ordered cell phone intercepts. Several documents included in the cache indicate the victim may have recently received top-secret clearance. Among this person's cache of documents is a Department of Homeland Security tip sheet called "Safeguarding National Security Information."

-An employee at the **National Science Foundation's Office of Cyber Infrastructure**. The documents collected from this victim include hundreds of NSF grant applications for new technologies and scientific approaches.

Financial Action Task Force, an intergovernmental body dedicated to the development and promotion of national and international policies to combat money laundering and terrorist financing.

It is believed by Alex Cox, research analyst at security firm NetWitness, that this government spear phishing attack involves the same guy behind the "Hilary Kneber" Zeus botnet from last year that infected "some 75,000 PCs on a wide range of government and private sector networks." Krebs reports that Cox said, "It's either the same guy, or someone is using this guy's exact same technique."

For now, this Merry Christmas eCard attack is thought to be for espionage purposes and that may very well prove true. This goes to show that anyone, regardless of *expertise*, can fall for a scam. Over 2 gigs were stolen and the damage is done, but will any policies or information be changed now that they are compromised?

What if, later on, any of this "secret" information were to be published by someone such as WikiLeaks? Is a breach only truly considered serious if that information were to be made public? Case in point is Bank of America which may be the major American bank that Julian Assange intends to "take down" and reveal an "ecosystem of corruption."

As Bank of America's share price falls, The New York Times reported [4] on the bank's counterespionage work as it gears up for possible published data. A team of 15 to 20 Bank of America top officials are investigating, "scouring thousands of documents in the event that they become public, reviewing every case where a computer has gone missing and hunting for any sign that its systems might have been compromised."

From a security and privacy perspective, it seems like missing computers should have been very important at the time . . . not just if that information might be made public by WikiLeaks. Perhaps computers gone missing were important at the time, but now Bank of America has consulted with top attorneys in case legal problems spring up after a public disclosure, "including the bank's potential liability if private information was disclosed about clients."

If the possibility of espionage was not enough, is a breach considered red-alert important only if the stolen information becomes public knowledge?

Entrepreneurial Espionage – Made in China

http://blogs.forbes.com/williampentland/2011/01/22/entrepreneurial-espionage-made-in-china/?boxes=businesschannelsections

Jan. 22 2011 - 8:23 pm

By WILLIAM PENTLAND

China's President Hu Jintao promoted the emerging spirit of American-style entrepreneurialism during his visit to Washington D.C. this week for the highly-scripted U.S.-China Summit.

Jintao has not yet commented on the status of Chinese government's home-grown brand of "shadow innovation," which began nearly 30 years ago and is evolving today into an insidious and dangerous trend called "entrepreneurial espionage."

In 1986, Deng Xiao Peng established "Program 863," a sort of academy of sciences and technologies charged with closing the scientific gap between China and the world's advanced economies in a very short period of time. The 863 program and its institutional derivatives not only sponsored actual research, they also promoted the acquisition of advanced technologies from other countries legally or illegally.

Today, counter-intelligence activities in the United States that have a nexus with China typically involve the illegal acquisition of U.S. technologies. Unlike Russian intelligence officers looking to exploit ego, greed, or other personal weaknesses, China has not normally paid agents for classified documents or engaged in clandestine activity like 'dead drops.'

While some of the recent espionage cases brought against China have ties to China's intelligence services, the vast majority are linked to other state organizations, particularly the factories and research institutes of China's military-industrial complex. Multiple Chinese state entities are engaged in an active effort to acquire restricted U.S. technologies. Unlike other foreign governments, China has a history of encouraging and rewarding private individuals to obtain technology on its behalf.

Chinese intelligence practices rely on nonprofessional collectors motivated by profit, patriotism or other factors and acting either independently or on behalf of the Chinese government to gather science and technology intelligence.

Nonprofessional intelligence collectors—including government and commercial researchers, students, academics, scientists, business people, delegations, and visitors—also provide China with a significant amount of sensitive U.S. technologies and trade secrets," according to reports by the Office of the Director of National Intelligence. "[I]n many cases, the collection efforts of these private-sector players are driven entirely by the opportunity for commercial or professional gain and have no affiliation with [PRC intelligence]."

This practice has led to a vast amount of "entrepreneurial" economic and industrial espionage conducted by Chinese students, trade delegations, businessmen and educational and research institutions, according to reports by the U.S.-China Economic And Security Review Commission.

The Chinese government encourages such efforts and has benefited from them. In 2009, the Commission quoted testimony provided by former FBI Special Agent I.C. Smith that:

the Ministry of State Security sometimes places pressure on Chinese citizens going abroad for educational or business purposes and may make pursuit of foreign technology a quid pro quo for permission to travel abroad. However, this phenomenon of "entrepreneurial espionage" appears to be particularly common among businessmen who have direct commercial ties with Chinese companies and who seek to skirt U.S. export control and economic espionage laws in order to export controlled technologies to the PRC. In such instances, profit appears to be a primary motive, although the desire to "help China" can intersect in many cases with the expectation of personal financial gain.

"Espionage entrepreneurs" are not focused solely on obtaining state-of-the-art, high-tech data and equipment. In many cases there is no obvious direct state involvement in the theft or illegal export of controlled technology. These entrepreneurial efforts frequently take the form of "mom-and-pop" companies—many of them nothing more than a titular business registered at a residential address—that legally purchase older military technology from U.S. manufacturers or through a secondary market of defense industrial equipment auctions, or even from the Internet, and then look for customer institutions back in China.

"There are pieces of technology . . . that the Chinese are trying to acquire that are 20, 25 years old, [and] that are mainstays of existing U.S. defense systems but come nowhere close to being considered state-of-the-art, and yet a means-ends test would correctly identify those as critical gaps in the Chinese system," said Dr. James Mulvenon, a specialist on the Chinese military at the Defense Group, Inc., stated during testimony before the Commission in 2009.

DOJ Defending Grand Jury Subpoenas in Trade Secrets Theft Investigation

http://legaltimes.typepad.com/blt/2011/03/doj-defending-grand-jury-subpoenas-in-trade-secrets-theft-investigation.html

Federal prosecutors today were scheduled to participate in a closed-door hearing in a Richmond federal appeals court over the propriety of grand jury subpoenas in a trade secrets theft investigation.

Lawyers for Kolon Industries Inc., which makes a high-strength fiber that competes with Kevlar brand technology, lost their effort last year to quash U.S. Justice Department subpoenas in U.S. District Court for the Eastern District of Virginia.

Senior Judge Robert Payne's decision in July affirming the subpoenas is not public, and the briefs in the appeals court are under seal.

Yesterday evening, the U.S. Court of Appeals for the 4th Circuit announced it was closing hearing to the public, abandoning the court's general practice of keeping grand jury subpoena hearings open and using pseudonyms to protect the secrecy of the proceedings.

Kolon's lawyers at Paul, Hastings, Janofsky & Walker and Richmond's LeClairRyan urged the court to prohibit the public from attending the hearing. Large portions of Kolon's motion (PDF) are blacked out.

The Justice Department deferred to the court on whether it should keep the hearing open. An assistant U.S. attorney in Richmond, Richard Cooke, said in court papers (PDF) filed March 18 that pre-indictment disclosure could cause prospective witnesses to hesitate before they voluntarily testify before the grand jury.

But Cooke also noted secrecy is no longer necessary when the contents of grand jury matters have become public.

The government's ongoing grand jury investigation of Kolon is noted in a parallel civil case that is pending in Richmond federal district court. There, Kolon is defending against trade secrets claims that a rival company, E.I. du Pont de Nemours, filed in February 2009.

The suit, based in part on the prosecution of a former DuPont engineer named Michael Mitchell, alleges Kolon conspired to steal DuPont's Kevlar brand technology. Mitchell, who'd worked for DuPont for more than 25 years, was sentenced last year on trade secrets charges to 18 months in prison. Mitchell was accused of proving Kolon confidential information from DuPont.

Kolon's attorneys said in the parallel civil case that prosecutors were unfairly piggybacking on DuPont in the civil action, using subpoenas to try to grab documents outside of the grand jury's power. Lawyers for Kolon argue DOJ used DuPont's suit to revive a criminal investigation that the government had declared "dead" in early 2009. (DuPont, represented by McGuireWoods and Crowell & Moring, denies it had any improper relationship with the Justice Department.) In arguing the grand jury subpoenas were improper, Kolon's lawyers also point to a decision last year in San Francisco federal district court, where a trial judge quashed DOJ subpoenas in an investigation of price-fixing in the liquid crystal display market. In that case, documents entered the United States from overseas. Prosecutors served grand jury subpoenas on several law firms. Last December, the U.S. Court of Appeals for the 9th Circuit reversed Judge Susan Illston's decision in the LCD investigation and ordered the law firms to produce certain documents.

Toshiba Corp.'s attorneys at White & Case, one of the firms that received subpoenas, have asked the U.S. Supreme Court to review the 9th Circuit's decision. White & Case lawyers, including Washington partner Eric Grannon, argue federal appeals courts are split over whether grand jury subpoenas trump civil protective orders.

Paul Hastings partner Stephen Kinnaird was expected to argue the appeal for Kolon in the 4th Circuit this morning. Kinnaird earlier declined to comment, citing

the fact the case is under seal and the litigation is ongoing. Cooke was scheduled to argue for the government.

For Kinnaird, the argument marks the second time he's been in front of the 4th Circuit for Kolon in civil and criminal trade secret litigation.

Earlier this month, the 4th Circuit unanimously upheld Kolon's antitrust counterclaim that DuPont has monopolized the United States market for para-aramid fiber, a foundation for, among other products, body armor and fiber optic cables. Kinnaird argued the case for Kolon.

In the civil action in the appeals court, the Justice Department and Federal Trade Commission backed Kolon in its effort to revive its monopoly claims. Neither agency, however, took a position on the merits of Kolon's allegations.

Ex-U.S. official warns Taiwan on Chinese espionage, military

http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?ID=201103310048&Type=aIPL

2011/03/31 22:12:08

Taipei, March 31 (CNA) Taiwan is advised to be vigilant over China's espionage activities and its increasing military capability directed toward the country, a visiting former U.S. official said Thursday.

China has been extremely active in its collection of intelligence around the world, and Taiwan should be very careful with regard to China's espionage activities, given that an average of 4,000 tourists arrive in Taiwan from there every day, said former U.S. Deputy Assistant Secretary of State for East Asian and Pacific Affairs Randall Schriver.

Schriver, who is now president and chief executive officer of the Project 2049 Institute, a think tank focused on Asia-Pacific affairs, made the comment while referring to an espionage case last month in which an army general was detained to become the highest-ranking Taiwanese military official caught spying for China in more than two decades.

The former official spoke to reporters at the mid-point of a March 27-April 2 visit on a wide range of issues related to the triangular relations between the U.S., China and Taiwan.

Schriver expressed disagreement with the recommendation in a recent roundtable discussion in the U.S. that said the U.S. should re-examine its arms sales to Taiwan to seek better relations with China.

Joseph Prueher, former Commander-in-Chief of the U.S. Pacific Command and a former U.S. ambassador to China, said Tuesday in the roundtable titled "A Way Ahead with China " organized by the University of Virginia's Miller Center of Public Affairs that the U.S. should take a fresh look at its involvement with Taiwan "outside of a military context."

On the bright side however, said Schriver, the seminar could turn out to be productive by reminding people about Taiwan and spur discussion.

He also said the throw-Taiwan-off-the-bus arguments were "pretty swiftly followed by a lot of negative responses from the policy community" and received bipartisan criticism in Washington.

Taiwan has to figure out what it wants to do to address the increasing cross-Taiwan Strait military imbalance, he said, adding that "the threat is there. It's clear. It's real."

While China said in its 2010 Defense White Paper released that same day that its military deployment is not directed toward the people of Taiwan, Schriver said the claim "does not appear to me to be factually correct."

The relationship between the U.S. and Taiwan is in "a very good state" and one that is "warm and mutually respectful, " Schriver said, adding that he could not think of any major obstacle in the future, despite the soured bilateral ties over the beef issue.

Schriver urged the U.S. to hold high-level talks with Taiwan to resolve the beef dispute because suspending talks is "counterintuitive." Meanwhile, he went on, "there are things we can do (to improve bilateral relations) notwithstanding our disagreement over beef."

Looking to the future, Schriver said that regardless of the outcome of Taiwan's 2012 presidential election, the U.S. will seek an opportunity to re-engage with Taiwan and put more energy into bilateral exchanges. (By Chris Wang)

Lab halts Web access after cyber attack

http://www.knoxnews.com/news/2011/apr/19/lab-halts-web-access-after-cyber-attack/?print=1

By Frank Munger

Tuesday, April 19, 2011

OAK RIDGE — A highly sophisticated cyber attack — known as Advanced Persistent Threat — forced Oak Ridge National Laboratory to shut down all Internet access and email systems over the weekend.

Those restrictions will remain in place until lab officials and others investigating the attack are sure the situation is well controlled and manageable, ORNL Director Thom Mason said Monday.

Mason said he expects that email functions may be restored today on a limited basis, with no attachments allowed and restrictions on length.
"We made the decision (at about midnight Friday) to close down the connection to the Internet to make sure there was no data exfiltrated from the lab while we got the system cleaned up," he said.

The lab's cyber specialists had been monitoring the attack and recommended further action after it looked like efforts were under way to remove data from ORNL systems, Mason said.

Mason said the APT threat at ORNL is similar to attacks in recent times on Google, a security company known as RSA and other government institutions and corporations.

"In this case, it was initiated with phishing email, which led to the download of some software that took advantage of a 'zero day exploit,' a vulnerability for which there is no patch yet issued," he said. The vulnerability involved Internet Explorer, he said.

Mason said the lab has not, to this point, detected any large-scale exfiltration of data, and the decision to shut down Internet access was made to prevent that or anything similar to a 2007 cyber attack at ORNL in which large amounts of data were stolen. Following that event, the lab sent 12,000 letters to former lab visitors, informing them that their Social Security numbers may have been compromised (although there were no subsequent reports of identity thefts or major problems).

"We haven't really completed the post-mortem on what happened, so it would be foolish to kind of speculate on where things were going," Mason said, when asked about a report that the attack may have originated in China.
"There was no significant exfiltration of data that we detected," he said. "There were attempts and small volumes of things that were suspicious in terms of Internet traffic."

ORNL has solicited help from throughout government, including other Department of Energy labs. He confirmed that some outside experts had arrived

in Oak Ridge to participate in the investigation.
In addition, he said virtually all of the lab's information technology staff (about 200 people) was involved, either in the investigation or maintaining the functionality of internal systems.

Mason confirmed that some computers were confiscated and quarantined. He also confirmed that the phishing email messages in this case were disguised as coming from the lab's human resource department.
He said that some lessons learned from the 2007 attack helped lab officials with the current situation, but he said this is a much more advanced attack that the event four years ago.

"Well, if you look at this APT, it is much more sophisticated than what was being used a few years ago," he said. "Certainly what we've seen is very consistent with the RSA attack. … Whoever is doing this attempts to get a foothold in the network system, works patiently and relatively quietly to try to expand that and is looking for specific types of information."

Without email or Internet access, thousands of ORNL employees weren't able to do business as usual on Monday.

"It hampered our normal communications," said Mason, who was out of town and could not check his email. "It means we're dusting off some fax machines."
Senior writer Frank Munger may be reached at 865-342-6329.

Ministry of Defence fails at redacting nuclear sub secrets

http://www.h-online.com/security/news/item/Ministry-of-Defence-fails-at-redacting-nuclear-sub-secrets-1229523.html

The UK's Ministry of Defence is reported to have failed to correctly redact PDF files it released under the Freedom of Information Act. Redaction is the process of removing classified information from documents; on paper documents, this is

done by using a black marker to cross out the text. The report in question, "SUCCESSOR SSBN - SAFETY REGULATORS ADVICE ON THE SELECTION OF THE PROPULSION POLANT IN SUPPORT OF THE FUTURE DETERRENT REVIEW NOTE" was published as a PDF file on the parliamentary site, the Daily Star revealed the MoD had originally "redacted" the document by changing the background colour of the text to black.

This meant that the document could be read by simply selecting the "redacted" areas and copy-and-pasting the still present text into a text editor. According to Cryptome, the text was also revealed by Google as it automatically scanned the document and converted it into HTML. In this case the document contained information about emergency procedures on UK nuclear submarines and the equivalent procedures on US submarines.

Graham Cluley of Sophos was quoted as asking "If this document is like this, who knows what else is?" The answer came on Sunday when a report in the Daily Telegraph revealed that other documents from the MoD, Department for Trade and Investment, Department of Health and the Department of Communities and Local Government suffered from incorrectly or insufficiently applied redaction. The MoD has started a review of currently published documents to fix the bad redactions. A guide on properly redacting PDF documents is available from Adobe.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

Cyber Crime Now An Industry

http://blogs.wsj.com/tech-europe/2011/04/19/cyber-crime-now-an-industry/?mod=google_news_blog

April 19, 2011, 4:01 AM GMT

By Ben Rooney

Another day, another conference on cyber-security, another report. The latest two were: the Symantec Cyber Security Cabinet, held yesterday rather melodramatically in the Churchill War Rooms underneath the heart of London's government center; and published today Verizon's 2011 Data Breach Investigations Report.

Both pointed to the increasing threat, and both would agree that the nature of the threat has changed. If anyone still believed that the average cybercriminal is a gifted computer-programming—though socially—awkward teenager working alone in his bedroom, then you can be disabused of that idea.

But what is interesting is how these two different expert groups do characterize cybercrooks. Detective Superintendent Charlie McMurdie, head of the Scotland Yard's e-crime police unit, one of the panelists at the Symantec event, was keen to stress the "organised" nature of the criminals, suggesting there was almost a co-ordinated underworld at work.

By contrast Bryan Sartin, Director of Investigative Response for Verizon Business Security Solutions stressed the "dis-organized" nature. "About five years ago, there were maybe some 200-250 major criminals," he said. " We knew what they did, where they were. Now most of them are behind bars." He suggested that the remaining cybercriminals were a lot less organized, and a lot less sophisticated than perhaps suggested; the report suggests that the only 8% of attacks monitored required advanced computer skills to be carried out and that 83% of victims were targets of opportunity.

While events like Stuxnet and the "advanced persistent threats" continue to dominate the headlines, suggesting as they do international espionage, terrorism and state-level threats, the reality, says Mr. Sartin is that the overwhelming majority of cybercrime is low-level simple attacks. "I am not even sure that in reality there is any such thing as an advanced persistent threat," he said. "Factories" producing attack kits, the software needed to launch a malicious attack

Increasingly cybercrime is becoming an industry. There are "factories" producing attack kits, the software needed to launch a malicious attack, and criminals with little or no computer skills can buy and use them; according to Tony Osborn, UK Public Sector Technology Team at Symantec, they are even sold with support contracts and help lines.

The other interesting trend that both agreed on was the fall off in the value of credit card details, which a few years ago were traded at around $9-14 each can now be bought online for as little as 5-12¢. According to Mr. Sartin, they have been replaced by verified username and password details, especially for systems that do not require two token authentication (typically logins that have a username, password, and a code generated from a standalone device). These can go for as much as $30,000 says Mr. Sartin.

This move up the value chain, says Mr. Sartin, reflects two things; the deluge of credit cards that swamped the market a few years ago and drove prices right

down, and the increasing trend for hackers to look to circumvent security protection. "It is much easier for a hacker to buy a legitimate username and password, log in and plant their malware, than to attempt to get in cleanly and leave no trace," said Mr. Sartin.

This increasing emphasis on personal attacks also extended to so-called "spear-phishing" attacks—attacks that target a specific individual or department within an organization. "There was one woman who works in the computer security industry, so should know better, who was hit," said Mr. Sartin. "She was very keen on knitting. So one day, out of the blue, she gets an email offering her a subscription to her favorite knitting website. It was malware. How did the hackers know? Simple. They read her Facebook profile."

Mr. Sartin said that their report, the 2011 Data Breach Investigations Report was based on the data from some 900 million breaches, and produced in conjunction with the U.S. Security Service and the Dutch Police.

Cyber-Ark Global Survey Shows External Cyber-Security Risks Will Surpass Insider Threats

http://finance.yahoo.com/news/CyberArk-Global-Survey-Shows-bw-2882769903.html?x=0&.v=1&.pf=personal-finance&mod=pf-personal-finance

Press Release Source: Cyber-Ark On Thursday April 14, 2011, 5:00 am EDT

NEWTON, Mass. & LONDON--(BUSINESS WIRE)

Results of Cyber-Ark® Software's fifth annual "Trust, Security and Passwords" survey show that 57 percent of global C-level executives agree that in the next one-to-three years, external threats such as cyber-criminals will become a greater security risk than insider threats. In addition to expanding awareness about the risks associated with cyber espionage or advanced persistent threat (APT)-type attacks, internal threats still represent a security challenge for many organizations today. Consider that nearly one in five of C-level respondents admitted that cases of insider sabotage had occurred at their workplace; and 16 percent believe that competitors may have received highly sensitive information or intellectual property including customer lists, product information and marketing plans from sources within their own organization.

Cyber-Ark's fifth annual "Trust, Security and Passwords" global report is the result of online surveys conducted in the Spring of 2011 with 1422 IT staff and C-level professionals across North America and EMEA. This is the first year

Cyber-Ark extended the survey to the C-suite. The overall expanded sample set impacts benchmarking against previous years' data, but provides a broader view of industry trends to track in future reports.

"Increased awareness that attack vectors can and do originate from both external and internal sources can be attributed in large part to the spectacular external-born breaches that drew headlines in the past year, including the NASDAQ and Gawker breaches. Regardless of the attack vector, the targets inside an enterprise remain the same – highly sensitive intellectual, financial and customer information," said Adam Bosnian, executive vice president Americas and corporate development, Cyber-Ark Software. "Privileged accounts are the key tool that external attackers and insiders leverage to access and exfiltrate an organization's sensitive information. Security teams need to start with improving the protection of these key internal targets – not simply building bigger walls around the enterprise."

The Temptation to Snoop Remains

With recent high-profile attacks that targeted privileged accounts and passwords, like the breach in EMC's RSA Security Division, awareness and a sense of urgency will continue to increase around the need to better monitor and control those powerful accounts. Specific results from global IT staff surveyed found that one quarter (25 percent) said their use of privileged accounts is still not being monitored.

A survey response that has remained fairly constant over the years is identifying the departments most likely to snoop around the network to look at confidential information. With their broad reach and highly privileged, anonymous access to various networks, systems and applications, nearly half (48 percent) of all global respondents chose the IT department as the most likely to snoop. Respondents said that managers were the next most likely (10 percent) followed by human resources (7 percent).

The following results compare "snooping" habits of IT staff around the world: When asked if they had ever accessed information on a system that was not relevant to their role, 28 percent of North American IT staff respondents admitted to snooping, while an even greater number in EMEA, 44 percent, admitted to the same behavior.

Similarly, 20 percent of North American respondents and 31 percent of EMEA respondents said that they or one of their colleagues had used an administrative password to access information that was otherwise confidential or sensitive.
The Impact of Data Breach Laws and Regulations on Privileged Account Perceptions

A new question added to this year's survey focused on measuring how respondents' perception of privileged account security has changed in light of data breach notification laws. According to the results, 77 percent of North American IT staff said their perceptions have changed, while much fewer in EMEA, 24 percent, felt the same way.

"We expected some differences between North American and EMEA respondents, and thought this gap was noteworthy in that it speaks to differences between the regions in terms of how data breach notifications are enforced – either by law in places like the U.S., or as a regulation in the U.K. Regardless, several recent reports have cited escalating fines associated with breaches, so it will be interesting to watch how perceptions change over time," said Bosnian.
Note to editors:

This online survey was conducted with 1422 IT staff and C-level professionals across North America and EMEA. For the most part, the C-level responses were in-line with their colleagues, though it will be interesting to track where differences of opinion grow, especially related to securing new virtualization technologies and liabilities for data breach reporting. To download the complete "Trust, Security and Passwords" report, visit the Surveys & Awards page at www.cyber-ark.com.

About Cyber-Ark

Cyber-Ark® Software is a global information security company that specializes in protecting and managing privileged users, applications and sensitive information to improve compliance, productivity and protect organizations against insider threats and advanced external threats. With its award-winning Privileged Identity Management, Sensitive Information Management and Privileged Session Management Suites, organizations can more effectively manage and govern data center access and activities, whether on-premise, off-premise or in the cloud, while demonstrating returns on security investments. Cyber-Ark works with more than 850 global customers, including more than 35 percent of the Fortune 100. Headquartered in Newton, Mass., Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific. For more information, visit www.cyber-ark.com.

France investigates cyber espionage at defence helicopter firm

http://www.theinquirer.net/inquirer/news/2042435/france-investigates-cyber-espionage-defence-helicopter-firm

Chinese linked again

By Asavin Wattanajantra

Mon Apr 11 2011, 12:13

FRENCH AUTHORITIES are investigating a suspected case of cyber hacking and espionage at a helicopter engine company.

Turbomeca, a subsidiary of the defence firm Safran, had its computer networks hacked and data about propeller systems stolen, according to a report in Le Monde.

Reportedly about 10 people are being held in custody and the attack took place during the first eight months of 2010. There is some suspicion that the attack had help from company insiders.

The report linked the Chinese because Turbomeca is the country's leading helicopter engine supplier working with both private and state companies. Safran is also owned 30 per cent by the French state, which means there could have been a political motivation for the attacks.

Also, last year hackers targeted the French Finance ministry, looking for files related to the G20 summit in Cannes. The Chinese state was also suspected to have been involved in that attack, but there was no firm evidence to support that conclusion.

It seems too easy to point the finger at China, because organised crime also has the resources and motivation to pull off these types of attacks. It's just that China has previously been suspected of state sponsored hacking and espionage, with Google having directly accused the Chinese government of interfering with its technology.

Read more: http://www.theinquirer.net/inquirer/news/2042435/france-investigates-cyber-espionage-defence-helicopter-firm#ixzz1JFOXnrdQ
The Inquirer - Computer hardware news and downloads. Visit the download store today.

MAY IN COUNTERINTELLIGENCE HISTORY

- May 9, 1934: On this date, President Roosevelt tasked the FBI with investigating the Nazi movement within the United States.
- May 17, 1999: On this date, Australian citizen Jean-Phillipe Wispelaere was arrested on charges of attempted espionage against the United States.
- May 19, 1976: On this date the Senate assigned oversight responsibility of foreign intelligence operations to the Select Committee on Intelligence.
- May 20, 1942: On this date, the FBI began its investigation of Velvalee Dickinson. During the course of the investigation, it was determined that Mrs. Dickinson was spying on behalf of Japan, providing information regarding the repair and movement of Naval vessels, communicating this information via coded messages.
- May 20, 1954: Attorney general Brownwell authorized the FBI to conduct microphone surveillance, even if the planting of the microphones required trespass, during national security investigations.
- May 20, 1978: On this date, Russian citizens Rudolph Chernyayev and Valdik Enger, employees at the United Nations were arrested on espionage charges. They attempted to bribe a U.S. naval officer to obtain Navy secrets. Unbeknownst to them, the naval officer was working on behalf of the FBI to catch the Russians in the act.
- May 25, 1945: Former French Air Force officer Paul Jean Marie Cavaillez was arrested by the FBI on charges of being an agent of the German government.

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