FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

September 1, 2011
Volume 3 Issue 9

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

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

A REVIEW OF THE FBI CI TRAINING TOOL "BETRAYED"

From the DVD back cover:

"Doug Collins has been a highly respected analyst at the FBI for twenty five years. He is liked and admired by all the members of his team, but they've seen changes in Doug recently: an attractive young girlfriend, working odd hours, increased frustration at work. And then there was the time he was seen texting on his Blackberry from inside the SCIF. It's all probably nothing. They know his recent divorce has been tough on him. It's not like he's a spy. But what if he is? What is the price of silence?

BETRAYED is more than a compelling, thought provoking drama. It is a uniquely crafted Counterintelligence training tool created through the Counterespionage Section of the FBI."

AN UNSOLICITED REVIEW FROM THE FSO OF A CLEARED DEFENSE CONTRACTOR

…thank you for taking the time in providing our personnel the Counter Intelligence Threat Briefing, yesterday. I've received excellent feedback about your presentation on Collection Trends, Cyber and Insider Threats and strategies to mitigate them. The short movie Betrayed grabbed everyone's attention and drove home important topics to be aware of … It's still the talk of the site. Our director, site manager, and personnel have told me that this was one of the more informative and interesting briefings they've received.

I know we're the first site you've presented this to, and one thing I can say is that stick with it. The movie is very powerful and makes everyone think.

Newsletter editorial comment: "BETRAYED" is an effective Counterintelligence training tool. Its use is clearly enhanced when shown as the centerpiece of a presentation given by FBI Special Agents, Subject Matter Experts, and other Counterintelligence professionals. When presented jointly with representatives from the Defense Security Service, the audience benefits immensely.

An interesting aspect of the movie is that about 6-8 minutes of interviews are conducted with co-workers and associates of actual insiders convicted of espionage, or convicted of theft of trade secrets. Associates of Robert Hanssen, Aldrich Ames, Meng Hong, and others reveal their sense of shock, amazement

and betrayal that someone they worked with, someone who might have been a close friend or work associate, could do such a thing.

Audiences gain most from the interaction after the movie, through the question and answer session offered at the conclusion of the presentation.

The information contained within the movie, the methodology of a spy, and the reticence of co-workers to report suspicious activity all provide viewers with the kind of information that will certainly enhance awareness of the threat and how it may manifest itself. The materials presented through the scenarios demonstrated within the movie are relevant to individuals with access to or charged with the protection of trade secrets, intellectual property, or classified information.

If you are interested in scheduling a presentation including the movie "BETRAYED" followed by Q&A, please contact Patrick Laflin, Tampa FBI CI Strategic Partnership Coordinator, 813-253-1029.

Remarks at the 2011 DISA Customer and Industry Forum

http://www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/speeches/speech.aspx?speechid=1601

As Delivered by Deputy Secretary of Defense William J. Lynn, III, Baltimore, Maryland, Tuesday, August 16, 2011

Thank you General Pollett.

I am glad to join a diverse cross-section of our IT community at this conference. From civilians within the department and members of the military to all those in industry, the work you do to ensure the integrity of our information systems is crucial to every mission we undertake.

Now, General Pollett has been very kind in his introduction. But the truth is he really does not understand my job. General Pollett is not a deputy. He is someone who has a deputy.

What happens when you are deputy is that you are not in charge of anything. Issues come up to you. But if there are any easy issues, somebody below you makes the decision, takes credit, puts out a press release. None of the easy issues make it through. I only get the most difficult ones, where the choices range from truly bad to really awful. As a result, I get to choose which of several constituencies to upset. If a really attractive issue or easy decision somehow slips through, the Secretary reaches down, grabs it, takes credit.

In all seriousness, General Pollett has an impressive record of service at DISA. On the job since December 2008, he has deftly guided DISA through a time of immense change.

He has helped establish a technical roadmap towards an enterprise services "platform." He has worked closely with the Pentagon to adapt to changes affecting the entire Department. And he has displayed strong leadership in the BRAC move to Ft. Meade.

Moves like this are never easy for individuals or families, let alone an entire agency. Especially when it stretches out commutes in Washington traffic. The Baltimore Parkway is not for the faint of heart.

The fact that DISA's move went so smoothly is a testament to the resiliency of DISA staff. On behalf of the Department, I would like to express my appreciation for how well each of you have handled the transition.

Across the department, we face another kind of transition, one on which the future of our forces and security depend. And in this transition, DISA is on the frontlines.

Changes in information technologies have revolutionized how our militaries organize, train, and fight. The information backbone DISA provides enables our most important military capabilities. From ISR and global strike to navigation and command and control, our defense community relies on the networks you are responsible for to keep America safe. You provide the information technology foundation for the most effective fighting force in the world. And you do so at a time where technology is not stagnant, but rather in a constant and rapid state of evolution.

The same adaptability you demonstrated in your move to Ft. Meade also manifests itself in the way you are able to react to technological change. One of the areas we are seeing the most amount of change is in the unprecedented and increasing series of cyber threats. It is clear that as this threat grows and transforms, so must our efforts to defense against it.

I have spent a great deal of my tenure as Deputy working on cyber security. My staff has been so deeply immersed in all the intricacies of the issue that each one of them deserves an honorary degree in computer science. Our work culminated last month with the release of the first ever Defense Strategy for Operating in Cyber Space. The strategy illustrates how cyber security is an issue that demands the full attention of the entire department.

The reality is that our reliance on IT presents a significant vulnerability. It is a reliance that you know very well. You are the professionals that help protect us from dangerous threats to our networks.

To date, the most prevalent cyber threat has been exploitation of our networks. By that, I mean the theft of information and data from both government and commercial networks. On the government side, foreign intelligence services have ex-filtrated military plans and weapons systems designs. Commercially, valuable source code and intellectual property has likewise been stolen from business and universities. The recent intrusions in the oil and gas sector and at NASDAQ join those that occurred at Google as further, troubling instances of a widespread and serious phenomenon.

This kind of cyber exploitation does not have the dramatic impact of a conventional military attack. But over the long term it has a deeply corrosive effect. It blunts our edge in military technology and saps our competitiveness in the global economy.

More recently, a second threat has emerged—and that is disruption of our networks. This is where an adversary seeks to deny or degrade the use of an important government or commercial network. And it happened in the denial of service attacks against Estonia in 2007 and Georgia in 2008. The effect is usually reversible. But the resulting economic damage and loss of confidence may not be.

To this point, the disruptive attacks we have seen are relatively unsophisticated in nature, short in duration, and narrow in scope. In the future, more capable adversaries could potentially immobilize networks on an even wider scale, for longer periods of time.

The third and most dangerous cyber threat is destruction, where cyber tools are used to cause physical damage. This development—which marks a strategic shift in the cyber threat—is only just emerging. But when you look at what tools are available, it is clear that this capability exists. It is possible to imagine attacks on military networks or critical infrastructure—like our transportation system and energy sector—that cause severe economic damage, physical destruction, or even loss of life.

Of course, it is possible that destructive cyber attacks will never be launched. Regrettably, however, few weapons in the history of warfare, once created, have gone unused. For this reason, we must have the capability to defend against the full range of cyber threats. This is indeed the goal of the Department's cyber strategy, and it is why we are pursuing that strategy with such urgency.

We stand at an important juncture in the development of cyber threats. More destructive tools are being developed, but have not yet been used. And the most malicious actors have not yet laid their hands on the most harmful capabilities. But this situation will not hold forever. Terrorist organizations or rogue states could obtain and use destructive cyber capabilities. We need to develop stronger defenses before this occurs. We have a window of opportunity—of uncertain length—in which to gird our networks against more perilous threats. All of you will play a key role in helping us seize this opportunity.

The Department's first-ever cyber strategy will guide how each military service and agency trains, equips commands our forces. It is a strategy based on five pillars. Let me describe them briefly.

First, the Defense Department has formally recognized cyberspace as a new operational domain—like land, air, sea and space. Treating cyberspace as a domain means that the military needs to operate and defend its networks, which is why we established U.S. Cyber Command—which is also housed at Ft. Meade. Second, we have equipped our networks with active defenses. It is not adequate to rely on passive defenses that employ only after-the-fact detection and notification. We have developed and now employ a more dynamic approach to cyber defense. Active defenses operate at network speed, using sensors, software, and signatures derived from intelligence to detect and stop malicious code before it succeeds.

Third, we must ensure that the critical infrastructure on which our military relies is also protected. The threats we face in cyberspace target much more than military systems. Cyber intruders have already probed many government networks, our electrical grid, and our financial system. Secure military networks will matter little if the power grid goes down or the rest of government stops functioning—which is why the Department of Homeland Security's cyber mission is so crucial.

Fourth, we are building collective defenses with our allies. Just as our air defenses are linked to those of our allies to provide warning of aerial attack, so too can we cooperatively monitor our computer networks for cyber intrusions. The fifth pillar of our strategy is to marshal our country's vast technological and human resources to ensure the United States retains its preeminent capabilities in cyberspace, as it does in other domains.

DISA plays a crucial role in our effort to address the cyber threat, and a key role in each part of the strategy. And nowhere is this role more important that DISA's support of Cybercom. Together with Cybercom, DISA has operational control over our defense networks. I know the move to Ft. Meade has been

difficult. But being co-located alongside Cybercom will strengthen each organization and reinforce our cybersecurity efforts.

DISA's industry partners are also key to our cyber strategy. Our networks are mostly operated by the private sector. We rely on private sector networks and services to operate nearly every facet of the Department. And the fact is that the private firms we depend on are susceptible to the same cyber threats we seek to protect .mil networks from.

It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies. In a single intrusion this March, 24,000 files were taken.

When looking across the intrusions of the last few years, some of the stolen data is mundane, like the specifications for small parts of tanks, airplanes, and submarines. But a great deal of it concerns our most sensitive systems, including aircraft avionics, surveillance technologies, satellite communications systems, and network security protocols.

We realize that we must help our partners protect their networks. Toward that end, the Department of Defense, in partnership with DHS, has established a pilot program with a handful of defense companies. In this Defense Industrial Base—or DIB—Cyber Pilot, classified threat intelligence is shared with defense contractors or their commercial internet service providers along with the know-how to employ it in network defense. By furnishing this threat intelligence, we are able to help strengthen these companies' existing cyber defenses.

The government has deep awareness of certain cyber threats. We have what some have termed a "special sauce" of malicious code signatures gathered from various intelligence efforts. Loading these signatures onto existing systems dramatically increases the effectiveness of cyber security. In this way, the DIB Cyber Pilot builds off existing capabilities that are widely deployed through the commercial sector.

Right now about 20 companies are involved in the 90-day pilot program. It is important to note that the pilot is voluntary for all participants, that the U.S. government is not monitoring, intercepting, or storing any private sector communications, and that the pilot has already stopped hundreds of attempted intrusions. The pilot also appears to be cost effective.

In the coming months, we will expand the pilot to the rest of the industrial base, as well as other key areas of critical infrastructure. DISA and industry partners will be crucial to making this initiative work.

We are developing this new cyber strategy at the same time we are entering a period of significant resource constraints.

For the past decade, we have lived in a world where we could meet new security challenges with increased resources. Going forward, we will not have that luxury. We are going to have to make hard choices. Our challenge is to accommodate changing fiscal circumstances without undercutting our military effectiveness.

IT has unique role in contributing to the budget drawdown. It is one of the few areas in which we can likely achieve pure efficiencies. By a pure efficiency, I mean being able to achieve the same results for less money.

Deploying new IT approaches has the potential to be a big money saver. For instance, cloud computing holds potential to reduce IT costs across the enterprise. And consolidating data centers will yield significant savings for each service. We have closed eight data centers since the IT Reform plan was published, and we intend to close another 44 by the end of FY2011. These efforts are very important to the Department. The centrality of IT in our efficiencies initiative means you are "tip of the spear" in our effort to seek savings.

To help guide us through these significant challenges, we are lucky to have an extremely qualified leader at the helm. Many of you know our new CIO, Terri Takai. She is working directly with me and the Secretary to lead our efforts to streamline IT operations and improve IT investment. Beth McGrath, our Deputy Chief Management Officer, is also play crucial role making sure our management systems and IT systems are fully aligned. The Department's success at financial management and achieving audit readiness in particular hinge on IT modernization.

DISA is not only central to the warfighter. It is central to the running of the whole department.

The message I would like to leave you with is that you are central to the effective operation of the Department in an era of downsizing. We will need your experience, judgment, and initiative to help modernize the department while saving money. Your efforts will save taxpayer dollars. But more important, they will benefit the warfighters, yielding huge dividends on the battlefield.

So as you can see, we are at two inflection points: the role of IT and cyber security in our military power is more important than ever before. And given the

potential savings generated by IT efficiencies, information technology is also helping us manage our fiscal situation.

As IT professionals, you are on the frontlines of these efforts. You can identify areas where we can save money. And your work to give our warfighters the best technology can save lives.

So I would like to thank DISA and its partners for all of the vital work you do. As the theme of this conference notes, we are all a part of harnessing "The Power to Connect."

Thank you.

ARRESTS, TRIALS AND CONVICTIONS

Iranian National Sentenced to 51 Months in Prison for Plot to Illegally Export Missile Components and Radio Tests Sets to Iran

http://www.justice.gov/usao/iln/pr/chicago/2011/pr0815_01.pdf

U. S. Department of Justice

United States Attorney Northern District of Illinois

Patrick J. Fitzgerald United States Attorney

Federal Building, 219 South Dearborn Street, Fifth Floor Chicago, Illinois 60604 (312) 353-5300

PRESS CONTACTS: AUSA Patrick Pope 312-353-1980 / Randall Samborn 312-353-5318

MONDAY AUGUST 15, 2011

www.justce.gov/usao/iln

CHICAGO — An Iranian national who maintained a residence and business in California was sentenced to 51 months in federal prison after pleading guilty in May 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., was sentenced Friday afternoon by U.S. District Judge Samuel Der-Yeghiayan in Federal Court in Chicago. Baniameri pleaded guilty on May 31 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).

"This defendant chose to be in the business of illegally exporting items to a state sponsor of terrorism. In doing so, he endangered the national security of the United States," said Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois.

Mr. Fitzgerald announced the sentence today with 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 was represented by Assistant U.S. Attorney Patrick C. Pope.

Former Shionogi Employee Admits to Hack Attack on Company Servers

http://www.justice.gov/usao/nj/Press/files/Cornish,%20Jason%20Plea%20News%20Release.html

FOR IMMEDIATE RELEASE

August 16, 2011

www.justice.gov/usao/nj CONTACT: Rebekah Carmichael

Office of Public Affairs

(973) 645-2888

NEWARK, N.J. – A Georgia man who froze the operations of a New Jersey pharmaceutical company where he had worked by deleting portions of its computer network pleaded guilty this morning, admitting he executed the attack, U.S. Attorney Paul J. Fishman announced.

Jason Cornish, 37, of Smyrna, Ga., pleaded guilty to an Information charging him with knowingly transmitting computer code with the intent to damage computers in interstate commerce. Cornish entered his guilty plea before U.S. District Judge Stanley R. Chesler in Newark federal court.

According to documents filed in this case and statements made in court:

Cornish was an information technology employee at Shionogi, Inc., a United States subsidiary of a Japanese pharmaceutical company with operations in New Jersey and Georgia.

In late September 2010, shortly after Cornish had resigned from Shionogi, the company announced layoffs that would affect an individual identified in court documents as B.N., Cornish's close friend and former supervisor.
In the early morning hours of February 3, 2011, Cornish gained unauthorized access to Shionogi's computer network. Cornish used a Shionogi user account to access a Shionogi server, then took control of a piece of software that he had secretly installed on the server several weeks earlier.

Cornish then used the secretly installed software program to delete the contents of each of 15 "virtual hosts" on Shionogi's computer network. These 15 virtual hosts (subdivisions on a computer designed to make it function like several computers) housed the equivalent of 88 different computer servers. Cornish used his familiarity with Shionogi's network to identify each of these virtual hosts by name or by its corresponding Internet Protocol address.

The deleted servers housed most of Shionogi's American computer infrastructure, including the company's e-mail and Blackberry servers, its order tracking system, and its financial management software. The attack effectively froze Shionogi's operations for a number of days, leaving company employees unable to ship product, cut checks, or communicate by email. Shionogi sustained approximately $800,000 in losses responding to the attack, conducting damage assessments, and restoring the company's network to its prior condition.

The investigation by the FBI's Cyber Crimes Task Force revealed that the attack originated from a computer connected to the wireless network of a Smyrna McDonald's where Cornish had used his credit card to make a purchase minutes before the attack. Cornish also gained unauthorized access to Shionogi's network from his home Internet connection using administrative passwords to which he had access as an employee.

The charge to which Cornish pleaded guilty carries a maximum potential penalty of 10 years in prison and a $250,000 fine. Sentencing is currently scheduled for November 10, 2011.

U.S. Attorney Fishman thanked special agents of the FBI's Cyber Crimes Task Force, under the direction of Special Agent in Charge Michael B. Ward in Newark; and in Atlanta, under the direction of Special Agent in Charge Brian D. Lamkin, with the investigation leading to the guilty plea.

The government is represented by Assistant U.S. Attorney Seth B. Kosto of the U.S. Attorney's Office Computer Hacking and Intellectual Property Section in the Office's Economic Crimes Unit in Newark.

Philippine National Pleads Guilty to Illegal Import of Unmanned Aerial Vehicle

http://www.justice.gov/usao/flm/pr/2011/july/20110728_Chua_Tpa_UAVPlea.pdf

FOR IMMEDIATE RELEASE

CONTACT: WILLIAM DANIELS

THURSDAY, JULY 28, 2011

PHONE: (813) 274-6388

http://www.usdoj.gov/usao/flm/p

FAX: (813) 274-6300

Tampa, Florida - United States Attorney Robert E. O'Neill and Special Agent in Charge Susan McCormick, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) announces that Henson Chua (47, Manilla, Philippines) today pleaded guilty to a violation of the Arms Export Control Act. Chua faces a maximum penalty of 20 years in federal prison. A sentencing date has not yet been set.

According to the plea agreement, Chua knowingly and willfully caused the temporary import into the United States of an item on the U.S. Munitions List, namely an unmanned aerial vehicle. Chua initially listed the item for sale on E-bay and then engaged in communications with undercover agents from ICE HSI, which culminated in the recovery of the item by U.S. officials.

"The unlawful import of military technology poses a serious threat to our national security," said Susan McCormick, special agent in charge of ICE HSI in Tampa. "ICE is committed to working with the U.S. Attorney's Office and military investigators to protect the American public and our military troops overseas from this kind of technology falling into the wrong hands."

This case was investigated by ICE-HSI in Tampa and Los Angeles, California, as well as the U.S. Air Force Office of Special Investigations. It is being prosecuted by Assistant United States Attorney Sara C. Sweeney.

Former U.S. Military Translator Found Guilty of Making False Statements Sentenced to 18 Months in Prison

http://www.justice.gov/usao/mie/news/2011/2011_1_14_lhamama.html

Updated August 18, 2011

January 14, 2011

Issam Hamama age 60, was found guilty by a federal jury in Detroit, Michigan on three counts of making false statements on applications for security clearances and in interviews with agents of the Federal Bureau of Investigation, announced United States Attorney Barbara L. McQuade. Among the jury's findings were that the defendant lied to FBI agents when he said he was not a source for the Iraqi Intelligence Service and that he did not receive payments from the Iraqi government - all of which occurred at a time when Iraq was ruled by Saddam Hussein. Hamama was acquitted of one count of conspiracy to act as agent of the Iraq government, and one count of making a false statement about his foreign business activities.

The jury deliberated for approximately a day and a half before returning the verdict, concluding a trial that began on January 4, 2011 before United States District Judge Nancy G. Edmunds.

U.S. Attorney McQuade was joined in the announcement by Andrew G. Arena, Special Agent in Charge of the Detroit Field Office of the Federal Bureau of Investigation.

The evidence at trial showed that Hamama, an Iraqi native and naturalized U.S. citizen, lived in El Cajon, Calif. He previously lived in Sterling Heights, Michigan. Beginning in 1992, Hamama – known as agent 6129 -- worked in the U.S. as a source for Sadaam Hussein's government, traveling to Washington to take orders and money from the Iraqi Intelligence Service. Hamama would collect information regarding individuals and organizations located in the United States. Hamama also traveled to Iraq as part of his work.

Hamama applied to become a translator for the U.S. military in Iraq in 2003 and 2005 but failed to disclose his secret assignments for Hussein and the Ba'ath Party when he signed security-clearance applications.

The defendant faces a maximum term of imprisonment of 5 years on each of the 3 counts of conviction. Sentencing is scheduled for May 19, 2011. United States Attorney McQuade thanked the Detroit office of the Federal Bureau of Investigation for their efforts that lead to this successful prosecution.

The case was prosecuted by Assistant U.S. Attorneys Cathleen Corken and Michael Martin.

(**Editorial Comment Note: In its sentencing memorandum, the government stated his** "perjury was so frequent and covered so many different subjects that his conduct was a willful attempt to obstruct the truth finding function of the jury." "His presence created extraordinary danger," Assistant U.S. Attorney Michael Martin said during the hearing. "(The government) has a right to know the background of someone who is out there with its troops."

Dutch Citizen Arrested, Charged With Conspiracy to Export Goods to Iran

http://www.justice.gov/usao/nj/Press/files/Davis,%20Ulrich%20News%20Release.html

FOR IMMEDIATE RELEASE

August 8, 2011

www.justice.gov/usao/nj

CONTACT: Rebekah Carmichael

Office of Public Affairs

(973) 645-2888

NEWARK, N.J. – Federal agents arrested a former manager of a Netherlands-based freight forwarding company Saturday evening, August 6, 2011, for allegedly conspiring with others to export goods – including aircraft parts, peroxide, and other materials – to Iran, New Jersey U.S. Attorney Paul J. Fishman announced.

Ulrich Davis, 50, of The Netherlands, is charged in a criminal Complaint with one count of conspiracy to violate the International Emergency Economic Powers Act and the Iranian Transactions Regulations. Davis was arrested at Newark Liberty International Airport as he was attempting to depart for The Netherlands by special agents of the U.S. Department of Commerce Bureau of Industry and Security and the U.S. Department of Homeland Security's Immigration and Customs Enforcement, Homeland Security Investigations.

The defendant appeared this morning before U.S. Magistrate Judge Patty Shwartz in Newark federal court and was detained.

"According to the Complaint, Ulrich Davis sent prohibited shipments to Iran, intentionally hiding the nature of sensitive materials to be provided to the Iranian military," said U.S. Attorney Fishman. "The violation of export laws designed to keep American munitions out of the wrong hands is more than shady business practice; it is a threat to national security."

"This investigation demonstrates our ongoing commitment to pursue individuals, including those in the freight forwarder community, who knowingly violate U.S. export control laws no matter where in the world they set up their illicit operations," said Eric Hirschhorn, Under Secretary for Industry and Security.

According to the criminal Complaint unsealed today:

Davis was the Sales and Business Development Manager for a company described in the Complaint as "the Netherlands freight-forwarding company" in 2007 and 2008. The Netherlands freight-forwarding company was affiliated with a New York-based freight-forwarding company.

Davis and the Netherlands company caused several shipments to be made to Iran without the necessary authorization from the United States government and in violation of the law.

In May 2007, the Netherlands freight-forwarding company caused attitude direction indicators for aircraft to be sent from the United States to Iran. Davis directed the transport company to disguise the nature of the shipment by removing the invoices and list of items from the box.

Also in May 2007, Davis' company forwarded a fuel control unit for use on a Boeing 747 aircraft to Iran. In September 2007, the Netherlands freight forwarder shipped C-130 aircraft parts to Iran; Davis was listed as the employee responsible for the shipment.

In 2007 and 2008, Davis also procured various materials from a New Jersey company – including adhesive primer, peroxide, and aerosols – that were sent to Iran in multiple shipments between August 2007 and January 2008. The shipments were made by the New York-based freight forwarding company, via another country. At least one of the shipper's export declarations filed by the New York freight forwarder falsely identified The Netherlands as the ultimate destination. Davis had instructed an employee of the New York freight forwarder to falsely list The Netherlands as the country of ultimate destination for the exports. The address in The Netherlands was a post office box.

In a January 2008 email regarding the shipments, Davis noted that, "99% of these goods were destined to be send to Teheran [sic]/Iran, which was and still is a very difficult destination due to political reasons."

If convicted of the charge, Davis faces a maximum potential penalty of 20 years in prison and a $1 million fine.

U.S. Attorney Fishman credited special agents of the Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, Boston Field Office, under the direction of Special Agent in Charge John McKenna, and New York Field Office, under the direction of Special Agent in Charge Sidney Simon, for the investigation leading to the arrest and charge. He also thanked HSI, Boston Field Office, under the direction of Special Agent in Charge Bruce Foucart, and Newark Field Office, under the direction of Acting Special Agent in Charge Andrew M. McLees; and Defense Criminal Investigative Service, New Haven Resident Office, under the direction of Resident Agent in Charge Kathryn Feeney, for their assistance.

The government is represented by Assistant U.S. Attorney Joyce Malliet of the U.S. Attorney's Office National Security Unit in Newark and Trial Attorneys Jonathan Poling and Elizabeth Cannon of the Counterespionage Section of the Justice Department's National Security Division.

The charge and allegations contained in the Complaint are merely accusations, and the defendant is presumed innocent unless and until proven guilty.

11-309 ###

Millersville Man Sentenced for Posing as a Retired Army Special Forces Colonel

http://www.fbi.gov/baltimore/press-releases/2011/millersville-man-sentenced-for-posing-as-a-retired-army-special-forces-colonel

Lied for 12 Years about Special Forces and Terrorism Experience to Gain Teaching Employment; Also Fabricated a Story of His Daughter's Kidnapping and Murder by Sex Traffickers

U.S. Attorney's Office

August 30, 2011

District of Maryland
(410) 209-4800

— filed under: Breaking News, Press Release

Baltimore, Maryland - U.S. District Judge William D. Quarles, Jr. sentenced William G. Hillar, age 66, of Millersville, Maryland, today to 21 months in prison followed by three years of supervised release for wire fraud in connection with a scheme to lie about his military experience and academic credentials in order to gain employment for teaching and training. Judge Quarles also ordered Hillar to pay restitution of $171,415 and perform 500 community hours at the Maryland State Veterans Cemeteries.

The sentence was announced by United States Attorney for the District of Maryland Rod J. Rosenstein; Special Agent in Charge Richard A. McFeely of the Federal Bureau of Investigation; and Special Agent in Charge Robert Craig of the Defense Criminal Investigative Service - Mid-Atlantic Field Office.

"William G. Hillar claimed that he had earned praise as a hero, but the truth is that he deserves condemnation as a liar," said U.S. Attorney Rod J. Rosenstein. "He did not serve in the U.S. Army, did not receive military training in counter-terrorism and psychological warfare, and did not lose his daughter to sex traffickers."

"Mr. Hillar's fraudulent representations came to the FBI's attention from concerned citizens, including former members of the Special Forces community. This investigation is an example of the difficulty the public faces trying to verify the accuracy of information on the Internet," said FBI Special Agent in Charge Richard A. McFeely.

"The Defense Criminal Investigative Service is committed to supporting America's warfighters and protecting the interest of the American taxpayers," said Robert Craig, Special Agent in Charge for the DCIS Mid-Atlantic Field Office. "The service members that comprise the Department of Defense's elite special warfare units have undergone years of specialized training and sacrifice to be called Special Forces. To misuse their titles for personal gain is unconscionable and discredits those that served and continue to serve the United States of America."

According to Hillar's plea agreement, from around 1998 to 2010, private and public sector organizations paid Hillar at least $171,415 for teaching, leading workshops, giving speeches and conducting training on counter terrorism, drugs trafficking, human trafficking and related topics. Hillar conducted these activities through a business named "Bill Hillar Training." According to the government's sentencing memorandum, most of Hillar's victims were military, law enforcement or first responder organizations.

In order to secure employment with these organizations, Hillar falsely represented in resumes, biographical statements and on the Internet that:

"William G. Hillar is a retired Colonel of the U.S. Army Special Forces. He has served in Asia, the Middle East, and Central and South America, where his diverse training and experiences included tactical counter-terrorism, explosive ordnance, emergency medicine and psychological warfare." Hillar also represented that he received a Ph.D. from the University of Oregon.

Hillar never served in the U.S. Army or the Special Forces and never attained the rank of Colonel. Hillar never served in Asia, the Middle East and Central and South America, and did not acquire in those locales training and experiences in counter-terrorism, explosive ordnance, emergency medicine and psychological warfare. Hillar did serve in the U.S. Coast Guard Reserve as an enlisted sailor from 1962 to 1970, achieving the rate of Radarman, Petty Officer Third Class.

According to the government's sentencing memorandum, the organizations that Hillar purported to train exercise critical public safety and national security functions, and require ongoing training and education in order to respond to new and changing threats. Hillar, who was not qualified, displaced qualified teachers and trainers, thereby putting members of our military, law enforcement and first responders at risk.

Moreover, the government's sentencing memorandum states that Hillar fabricated a gruesome tale that his own daughter had been kidnapped, forced into sex slavery, sodomized and tortured before being hacked to death with machetes and thrown into the sea. He further claimed that this experience and his life story was the basis for the 2008 film "Taken". The significant press attention that film generated, in turn, generated free press for Hillar. Hillar admits that he fabricated the story about his daughter, who was alive and well.

United States Attorney Rod J. Rosenstein praised the FBI and the Defense Criminal Investigative Service for their work in the investigation, and thanked Assistant United States Attorney Leo Wise, who prosecuted the case.

NEWSLETTER EDITOR COMMENT: Though not a counterintelligence or even a national security case, this still shows the importance of properly and thoroughly vetting the individuals you allow into your workplaces. If you truly don't know someone's true background, even if they are wearing a uniform, validate (JPAS, Credentials, Badges, etc. If in doubt, call the organization they claim to represent to validate.)

Brookline Man Pleads Guilty to Foreign Economic Espionage

http://www.fbi.gov/boston/press-releases/2011/brookline-man-pleads-guilty-to-foreign-economic-espionage

U.S. Attorney's Office

August 30, 2011 District of Massachusetts

(617) 748-3100

— filed under: Press Release
BOSTON—A Brookline man pleaded guilty today to foreign economic espionage. This is the first prosecution in Massachusetts for foreign economic espionage and only the eighth in the nation.

ELLIOT DOXER, 43, pleaded guilty before U.S. District Judge Denise J. Casper to one count of foreign economic espionage for providing trade secrets over an 18-month period to an undercover federal agent posing as an Israeli intelligence officer.

The parties stipulated in an agreed statement of facts that on June 22, 2006, DOXER sent an e-mail to the Israeli consulate in Boston stating that he worked in the finance department of Akamai Technologies, Inc., and was willing to provide any information that might help Israel. In later communications, DOXER said that his chief desire "was to help our homeland and our war against our enemies." He also asked for payment in light of the risks he was taking.

In September 2007, a federal agent posing as an undercover Israeli intelligence officer spoke to DOXER and established a "dead drop" where the agent and DOXER could exchange written communications. From October 2007 through March 2009, DOXER visited the dead drop at least 62 times to leave information, retrieve communications, and check for new communications.

Included in the trade secret information that DOXER provided the undercover agent were an extensive list of Akamai's customers; contracts between the company and various customers revealing contact, services, pricing, and termination date information; and a comprehensive list of the company's employees that revealed their positions and full contact information. DOXER also broadly described the company's physical and computer security systems and stated that he could travel to the foreign country and could support special and sensitive operations in his local area if needed. Because Akamai's information was disclosed only to an undercover agent from the beginning, the information was never in danger of actual exposure outside the company.

We acknowledge the government of Israel for their cooperation in this investigation, and underscore that the information does not allege that the government of Israel or anyone acting on its behalf committed any offense under U.S. laws in this case. We would also like to acknowledge and thank Akamai Technologies, Inc., for its assistance throughout all stages of the investigation and prosecution.

DOXER was arrested on October 6, 2010, on a complaint charging him with wire fraud.

That charge will be dismissed at the end of this case as part of the plea agreement. The charge of foreign economic espionage carries a maximum penalty of 15 years in prison, a three-year term of supervised release and a $500,000 fine. Judge Casper scheduled sentencing for November 30, 2011.

United States Attorney Carmen M. Ortiz and Richard DesLauriers, Special Agent in Charge of the Federal Bureau of Investigation - Boston Field Office made the announcement today. The case is being prosecuted by Assistant U.S. Attorneys William D. Weinreb and Scott L. Garland, respectively in Ortiz's Antiterrorism and National Security Unit and Cybercrimes Unit, and by Trial Attorneys Kathleen Kedian and David Recker of the Department of Justice's Counterespionage Section.

TECHNIQUES, METHODS, TARGETS

A Byte Out of History: Going SOLO: Communist Agent Tells All

http://www.fbi.gov/news/stories/2011/august/communist_080211/communist_080211

08/02/11

Morris Childs' intelligence work was handled by the FBI under the code name SOLO.

In April 1958, a representative of the Communist Party of the United States (CPUSA) named Morris Childs made important trips to the Soviet Union and China. His purpose: to re-establish formal contact between the CPUSA and these countries.

First, Morris visited with key Communist Party and Soviet leaders in Moscow. He learned of their wider political goals, their concerns and fears, and their deep

interest in restoring connections with the CPUSA. Then he went to Beijing, where he made similar inroads and met with Premier Mao Tse Tung.

After three months, Morris returned home and reported all he'd learned to CPUSA leaders. But as a new Freedom of Information Act release in the FBI Vault makes clear, he was also secretly talking to President Dwight Eisenhower, the vice president, the secretary of state, and a select group of other U.S. officials. Morris, you see, was actually one of the FBI's greatest Cold War agents.

Born Moishe Chilovsky in the Ukraine, Morris Childs and his family immigrated to the U.S. in 1912. He joined the emerging communist movement in Chicago as a teenager and devoted his life to the cause. In 1947, his work ended after an internal power struggle removed him as editor of the CPUSA's flagship newspaper and his continuing struggle with heart disease left him sickly and incapacitated. Unable to pursue other work for the movement, Childs was soon forgotten.

Meanwhile, America's growing realization of the penetration of the U.S. government by the Soviets and the subsequent political debate over the role of communism in society became the focus of the day. By the early 1950s, the FBI began taking a more proactive approach to dealing with Soviet intelligence. That included zeroing in on the CPUSA—in part, by approaching Communist officials who had left the party. One of the first on the list was Morris Childs' brother Jack.

Jack willingly cooperated and strongly advocated that the Bureau contact his brother, paving the way for a 1952 meeting between Morris and Special Agent Carl Freyman. The two got along quite well, sharing a knowledge of communist philosophy and an interest in wider intellectual and cultural issues.

After several meetings, Childs agreed to return to the CPUSA as an informant for the FBI. With the assistance of Jack, the Bureau helped Morris rehabilitate both his health and his role in the Party. Morris began feeling better after a Bureau-arranged stay at the Mayo Clinic, and within a year he started reaching out to his old comrades. He and Jack were accepted back into the CPUSA and eventually were tasked with deepening contacts with the Canadian Communist Party and through it, the Soviet Union.

Over four decades, Morris made more than 50 visits overseas for the CPUSA, each time reporting with great detail and insight about the issues and concerns of the leadership of the Soviet Union and China. Considering that these two nations were such closed societies, Morris's intelligence was invaluable—a fact recognized by President Ronald Reagan when he awarded Morris (and posthumously, Jack) with the Presidential Medal of Freedom.

The intelligence work of the brothers—and later their wives—was handled by the FBI under the code name SOLO. In the coming months, stay tuned as we reveal more details of this long-running operation as additional sections of the SOLO file are released in our Vault.

Espionage in the Defense Industry

http://www.fbi.gov/about-us/history/famous-cases/espionage

During a social gathering held in 1970 at a commercial establishment in the New York City vicinity, one Sergey Viktorovich Petrov (fictitious name), a Russian citizen, happened to strike up a casual conversation with an individual employed as an engineer with the Grumman Aerospace Corporation.

In the course of the ensuing verbal exchange, Petrov explained that he was Russian and was employed at the United Nations (UN) where he translated papers relating to various scientific affairs. He added that he lived in New York City with his wife and daughter, and that he was trained in aeronautical engineering. He also related that he had a five-year contract.

The engineer revealed his employment and noted that he was engaged in design planning relating to the F-14 fighter aircraft that was being developed by Grumman for the United States Navy. He explained that his company had been dismissing a large number of engineers, and therefore, his future employment prospects at Grumman were rather bleak. The American illustrated his points by commenting on certain economy measures he had undertaken in his personal spending habits due to his uncertain future.

Before the chance meeting was over, Petrov bought his new-found friend a drink. He told the engineer he would enjoy seeing him again in the near future at which time he could perhaps treat the American to a steak dinner. The engineer accepted Petrov's invitation at 7 p.m., one week later.

Petrov and the engineer met as planned the following week. At Petrov's suggestion, the engineer followed the Russian's car to a restaurant in Amityville, Long Island. During the two-hour-long dinner, they discussed a number of general topics. At one point, Petrov said he was seriously considering starting a business in the New York City area. He added that he would enjoy having the engineer as an employee should the latter lose his job at Grumman. Petrov went on, explaining that in the meantime he was preparing his doctoral thesis. In this regard he wished to obtain some engineering data about the F-14 aircraft. Petrov said he would pay the engineer for any information he could provide, but quickly added that he did not need any classified data. Petrov said he especially desired

some information about the F-14's wing sweep mechanism since this concept greatly intrigued him. He remarked that in case the engineer was unable to provide him with details of the wing sweep mechanism, he would, nevertheless, appreciate any information whatsoever concerning the work performed at the Grumman plant.

Petrov then told the engineer that if he could provide anything of value, he would be paid approximately $300 per month. The engineer promised Petrov he would consider his request and would inform the Russian of his decision at an engineering conference which was to be held soon. The engineer added that Petrov would, no doubt, wish to attend this meeting since the subject matter would be of interest to him. To the engineer's surprise, however, the Russian replied that he did not think it would be wise for him to attend his forthcoming conference. He also cautioned the engineer to give no sign of recognition should their paths cross at any future scientific meeting.

Before concluding their meeting, Petrov obtained the engineer's home telephone number but declined to provide his own in return. They then agreed to meet again in front of their present location at 7 p.m. on a date about three weeks later. Petrov told the engineer that if for some reason he could not make it on that day, then they would meet on the following Monday at the same time and place.

At the conclusion of this second meeting, the engineer, suspicious of Petrov's intentions, reported his suspicions to the Grumman security office which immediately notified the New York Field Office of the FBI. Special agents of the FBI interviewed the engineer who agreed to cooperate by meeting again with Petrov in order to ascertain the Russian's intentions. The engineer explained that his remarks concerning his somewhat precarious financial situation seemed to impress Petrov. The agents then instructed the engineer to continue to express a need for money at future meetings.

At their next meeting, Petrov asked the engineer to be alert for any reports or publications relating to the F-14. He added that he was also interested in any other material to which the engineer had daily access. In reply, the American inquired as to what he could expect in the way of monetary compensation. The Russian promised to pay him from $100 to $300, the exact amount depending solely on the material's value.

Petrov asked the engineer if he would have any problems in removing material from the plant. Petrov then commented that if the engineer could borrow the requested data overnight, he would return it the next day. Although Petrov previously had said he did not require any confidential material, at this point he

mentioned that any confidential information the engineer could provide would be "worth more."

Future meetings between Petrov and the engineer continued on a almost monthly basis. They were invariably held at different restaurants on Long Island on Monday evenings at 7 p.m. FBI agents, conducting a surveillance of the meetings, observed that most of them were held within close proximity of Long Island railroad stations. Future meetings between the American and the Russian were always arranged at the conclusion of each previous meeting. The date, time, and place of the next meeting were agreed upon together with an alternate meeting date in case either party was unable to attend on the original date.
As their relationship progressed, Petrov provided the engineer with small sums of money—usually about $250—for each report the American gave the Russian. Petrov never ceased to pressure the engineer for F-14 technical reports, especially confidential ones. The engineer, however, continued to bring routine reports to the meetings, explaining that confidential reports were very difficult to obtain. Petrov then suggested that the engineer should request a transfer to another area of the Grumman plant where he would be in a position to have access to a much larger variety of engineering data. He promised to compensate the engineer for any decrease in salary that might occur as a result of any such transfer.

Several months later, in response to Petrov's urgings, the engineer offered him some drawings relating to the F-14's wing design. He warned the Russian that he had to have the drawings back before he returned to work the next day. At this point, Petrov told the engineer he would furnish him with a copying machine, thereby eliminating the necessity of bringing the actual reports and drawings to future meetings.

At a subsequent meeting on March 1, 1971, Petrov gave the engineer an inexpensive, portable copying machine. He then suggested that the American use the machine in a motel room and promised to reimburse the engineer for all expenses incurred in this regard. Such an arrangement would enable the engineer to return the original reports to his office the next day while having a copy available for Petrov at their next meeting.

During their March meeting, Petrov remarked that he would probably be returning to the Soviet Union in May for a vacation. He made it clear, however, that in the meantime he expected the engineer to "keep busy" obtaining and copying F-14 reports.

Shortly before returning to Russia on May 19, 1971, Petrov set up a schedule of future meetings. On odd months the meetings would be held on the first Monday of the month, while the even month meeting dates would be on the second

Monday. Alternate meeting dates, in case one of them missed the regular day, would be on the following Monday of each month. Petrov then told the engineer he would return to the United States in August. They agreed to meet again on August 9th at a restaurant in the vicinity of Islip, Long Island.

Following Petrov's return from the Soviet Union, their dinner meetings continued on a regular basis. They met at previously designated restaurants and, during dinner, discussed the engineer's employment prospects at Grumman and what material the engineer had managed to bring with him. After dinner they normally left the restaurant and entered the engineer's car where the F-14 reports and money were exchanged. Petrov would then get out of the car and depart the area on foot. During their earlier meetings, Petrov drove his own automobile to the meeting location. Later, however, the Russian started driving to a railroad station located several stops short of the meeting site and then rode a train to his final destination. Petrov explained to the engineer that no one would recognize him so far from New York City, but he was afraid the police might begin to notice his car after a while.

During their November 1, 1971 meeting, Petrov furnished the engineer with a specially altered 35-mm camera. This camera was capable of taking 72 photographs from each 36-exposure roll of film. Included with the camera were a couple of rolls of film and a high-intensity lamp. Petrov instructed the engineer in the camera's operation and told him to use both the camera and the copying machine until he was certain he could operate the camera correctly. The Russian explained that it would be much easier to pass the engineering reports if they were on film. The engineer could place the film in a cigarette package and give it to Petrov who would in return hand the American a similar package containing cigarettes.

During their January 3, 1972 meeting, Petrov told the engineer that his contract at the UN would probably terminate in October or November of that year. He stated that, should he have to return to Russia, he would introduce the engineer to a colleague with whom the American could continue to do business. Petrov added that if he failed to appear at their designated meeting site on both of the first two Mondays of that month, then the engineer was to go to a movie theater in Freeport, Long Island the following Monday. The engineer was to walk up the right side of the theater entrance at precise intervals of 7:00 to 7:07 p.m. and 7:30 to 7:35 p.m. A man, standing in this area, would say to the engineer: "Hello. Are you interested in buying an antique Ford of 1930?" The engineer was to reply: "Yes. I am. After all, I was born in 1930." As an extra precautionary measure, the new man would have one half of a dollar bill. The engineer would have the other half of the dollar bill.

Their fifteenth and final meeting took place at a restaurant near Patchogue, Long Island on February 14, 1972. Petrov seemed pleased when the engineer told him he had brought along some confidential pages from a report on the F-14 project. Petrov then said that since their business arrangement was working out so well, he wanted to minimize the possibility of anyone recognizing them together. He mentioned a plan to use walkie-talkies to eliminate all unnecessary personal contact. Petrov, unaware of his impeding arrest that evening, promised to give the engineer his walkie-talkie unit at their next meeting. He instructed the engineer to place the rolls of film, containing the Grumman reports, in small, metal containers which would then be cast in plaster of Paris bricks. The engineer was to place the bricks in predesignated locations and then transmit a radio signal to Petrov who would be stationed about one-half mile away. Upon receipt of this signal, Petrov would wait approximately one-half hour before retrieving the brick.

Petrov told the engineer that during the first three months of this new system, the drop-off points for the plaster bricks would be somewhere on Long Island. Subsequent drop-off points would be on the west side of the Tappan Zee Bridge in Rockland County, north of New York City.

When asked about payment for the confidential report that the engineer had brought along that evening, Petrov replied that he would have to look at it to determine its value. Upon finishing dinner, they left the restaurant and entered the engineer's car. At this point, Petrov asked if the engineer had the confidential material ready. In response, the engineer removed a large grey envelope stashed in the back of the car which contained a copy of an F-14 engineering report, a roll of film containing a copy of the same report, and several pages that were classified "confidential" from another report. The engineer then handed the envelope to Petrov who placed it into his attaché case. Petrov, after giving the engineer a small, white envelope in return, got out of the car and started to walk toward the parking lot's exit. At this moment, based upon a prearranged signal, FBI agents immediately intercepted and arrested Petrov before he could escape. The Russian, seeing that capture was imminent, attempted to dispose of the evidence by throwing his attaché case high into the air. However, it was immediately retrieved by one of the FBI agents.

Petrov was taken to the Federal Detention Center in New York City. The following morning, he was brought before the U.S. magistrate for the Eastern District of New York in Brooklyn. The U.S. magistrate set bail at $500,000 and remanded Petrov into the U.S. marshal's custody until a Russian translator could be obtained the next day.

Ironically, Petrov, who worked as a Russian-English translator at the UN, remained silent during his court appearance, indicating that he did not understand the English language!

A search of Petrov's person turned up three index cards. Each contained hand-drawn diagrams of various locations within the New York area. These were obviously the drop-off sites that Petrov had had in mind when he discussed the use of plaster bricks with the engineer.

Petrov was arraigned and released after his $500,000 bail was reduced to $100,000. A federal grand jury returned an indictment on February 17, 1972, charging Petrov with espionage and violation of the Foreign Agents Registration Act. On August 14, 1972, the indictment was dismissed following instructions from the White House to the U.S. Department of Justice and after Petrov returned to the Soviet Union with prior court approval. It was decided by top U.S. officials that this dismissal would best serve the national and foreign policy interests of the United States.

Malicious Users Seeking to Exploit Interest Related to the 10 Year a Anniversary of the 11 September 2001 Terrorist Attacks

Malicious users seeking to exploit interest related to the 10 year anniversary of the 11 September 2001 terrorist attacks will likely use subject lines related to the incident in phishing1 e-mails on or around 11 September 2011. Network administrators and general users should be aware of these attempts and avoid opening messages with attachments and/or subject lines related to 9/11.

BACKGROUND

This NCCIC Bulletin is being provided for your situational awareness because of the malicious cyber activity that is commonly associated and that precedes high profile events or the anniversaries of significant events. Both government agencies and private organizations could possibly become recipients of malicious activity, most commonly in the form of socially engineered spear-phishing emails.

These emails will appear to originate from a reputable source, with the email subject closely aligned to the event and usually of interest to the recipient. The email in most cases will contain a malicious attachment with a subject name relevant to the event alluring the recipient to open. The attachment when opened will launch malware into the users system in most cases in the form of a key logger or remote access Trojans.

DHS/NCCIC ACTIONS

The NCCIC will continue to monitor reporting from multiple public and private sources, and generate additional products if new information becomes available.

DHS/US-CERT is collecting phishing email messages and web site locations so that we can help people avoid becoming victims of phishing scams. You can report phishing to US-CERT by sending email to phishing-report@us-cert.gov.

Computer lab's Chinese-made parts raise spy concerns

NEWSLETTER EDITORIAL COMMENT: The article located at the below link, with a brief extract from the article, details concerns of several U.S. Senators or members of the House of Representatives concerning the use of foreign made components within sensitive U.S. government systems. This topical area is indicative of another potential methodology used to compromise vital systems. Please go to the link below to read this article in its entirety.

http://www.washingtontimes.com/news/2011/aug/16/computer-labs-parts-raise-spy-concerns/print/ -

The Washington Times

Tuesday, August 16, 2011

A U.S. supercomputer laboratory engaged in classified military research concluded a recent deal involving Chinese-made components that is raising concerns in Congress about potential electronic espionage.

The concerns are based on a contract reached this summer between a computer-technology firm and the National Center for Computational Engineering at the University of Tennessee, whose supercomputers simulate flight tests for next-generation U.S. military aircraft and spacecraft, and simulate submarine warfare for the Navy.

The five lawmakers, in their letter, raised concerns that (**UNAMED COMPANY**) is seeking to place its gear inside sensitive installations by partnering with U.S. vendors. In the case of the University of Tennessee National Center for Computational Engineering, a company called (**UNAMED COMPANY**) won the bid. That company specializes in data-storage architecture, and it has sensitive contracts with the FBI and other U.S. government agencies.

In an interview, (**UNAMED COMPANY**) stated their storage architecture was not at risk of being compromised by an intelligence service. Data for the system would be encrypted, and the storage system will not be connected to the

Internet. He also said the (**UNAMED COMPANY**) hardware was not installed on the disc drives, where the data would be stored.

"If you were to do the kinds of activities the senators are talking about, you would put that technology in the disk drives because the data lives on the disk drives," "(**UNAMED COMPANY**) does not manufacture the disk drives."

Jeffrey Carr, the CEO and founder of Taia Global, a cybersecurity firm said, however, that encryption is not enough.

"There are so many alternative ways of compromising a network. It can be done through a thumb drive, a printer server," he said. "It could be done through a vendor that seeks to install or to service the equipment, it could be done through an insider, an alternative communication channel like Bluetooth or another peer-to-peer network. It could done through an internal email."

http://www.washingtontimes.com/news/2011/aug/16/computer-labs-parts-raise-spy-concerns/print/

END OF EXTRACT: Please read the original article in its entirety at the link above.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

NEWSLETTER EDITORIAL COMMENT: This article demonstrates known methodology utilized by cyber scammers. The reader should note that variants of this scam could be utilized in virtually all internet transactions, not only for

automobiles. This method also could be used to obtain identity and financial information.

Buying A Car Online? Read This First

http://www.fbi.gov/news/stories/2011/august/car_081511/car_081511

8/15/11

You can buy almost anything over the Internet—including clothes, a pizza, music, a hotel room, even a car. And while most transactions are conducted lawfully and securely, there are instances when criminals insert themselves into the marketplace, hoping to trick potential victims into falling for one of their scams.

Today, the FBI's Internet Crime Complaint Center (IC3) issued an alert about a specific type of cyber scam that targets consumers looking to buy vehicles online.

How the scam works. While there are variations, here's a basic description: consumers find a vehicle they like—often at a below-market price—on a legitimate website. The buyer contacts the seller, usually through an e-mail address in the ad, to indicate their interest. The seller responds via e-mail, often with a hard-luck story about why they want to sell the vehicle and at such a good price.

In the e-mail, the seller asks the buyer to move the transaction to the website of another online company….for security reasons….and then offers a buyer protection plan in the name of a major Internet company (e.g., eBay). Through the new website, the buyer receives an invoice and is instructed to wire the funds for the vehicle to an account somewhere. In a new twist, sometimes the criminals pose as company representatives in a live chat to answer questions from buyers.

Once the funds are wired, the buyer may be asked by the seller to fax a receipt to show that the transaction has taken place. And then the seller and buyer agree upon a time for the delivery of the vehicle.

What actually happens: The ad the consumer sees is either completely phony or was hijacked from another website. The buyer is asked to move from a legitimate website to a spoofed website, where it's easier for the criminal to conduct business. The buyer protection plan offered as part of the deal is bogus.

And the buyer is asked to fax the seller proof of the transaction so the crooks know when the funds are available for stealing.

And by the time buyers realize they've been scammed, the criminals—and the money—are long gone.

Red flags for consumers:

- Cars are advertised at too-good-to-be true prices;
- Sellers want to move transactions from the original website to another site;
- Sellers claim that a buyer protection program offered by a major Internet company covers an auto transaction conducted outside that company's website;
- Sellers refuse to meet in person or allow potential buyers to inspect the car ahead of time;
- Sellers who say they want to sell the car because they're in the U.S. military about to be deployed, are moving, the car belonged to someone who recently died, or a similar story;
- Sellers who ask for funds to be wired ahead of time.

Number of complaints. From 2008 through 2010, IC3 has received nearly 14,000 complaints from consumers who have been victimized, or at least targeted, by these scams. Of the victims who actually lost money, the total dollar amount is staggering: nearly $44.5 million.

If you think you've been victimized by an online auto scam, file a complaint with IC3. Once complaints are received and analyzed, IC3 forwards them as appropriate to a local, state, or federal law enforcement agency.

Fake 'wrong transaction' hotel spam hits email

Scammers want you to click on attachment, which has malware

http://www.msnbc.msn.com/id/43948767/ns/technology_and_science-security/
Despite the subject matter in a newest wave of spam emails, online scammers never take a vacation.

Hundreds of emails have been making the rounds in the past few days informing people that a hotel made a "wrong transaction" while processing their credit card. In turn, the emails offer recipients a refund.

PLEASE VISIT THE WEBSITE AT THE LINK ABOVE TO READ THIS ARTICLE IN ITS ENTIRETY

Coding error reveals RSA attackers operated from China

(Editors Comments: The article, located in its entirety at the below hyperlink, discusses how coding errors by the by the malware's author reveal his "nom de guerre" to be "Lion". System logs can be searched for the error message. If found, it is likely the network has been targeted by Advanced Persistent Threats. The article is partially extracted below.)

http://www.net-security.org/secworld.php?id=11393

Posted on 04 August 2011.

A simple error message returned by a server to which a malware sample was trying to connect revealed to Dell SecureWorks researchers the origin of the RSA attack, says Joe Stewart, the company's Director of Malware Research.

Even though the message was seemingly truncated, the pattern could be tied to "HTran", a very old piece of software that is used to obfuscate the real source or target of the attack by redirecting TCP traffic to alternate hosts.

The error message in question happens due to a coding mistake by the author of the software, a Chinese hacker that goes by the handle of "Lion". The great news is that this knowledge can be used by organizations to detect Advanced Persistent Threats targeting their networks…

Please read the article in its entirety, located at the hyperlink above.

Chinese State TV Reveals Inconsistencies?

A spate of news articles all relating to the same point were recently published.

All referred to a July broadcast of a CCTV news story. For approximately no longer than 10 seconds, a report concerning cyber security displayed footage of a computer display. The footage showed a U.S. based IP address, apparently located at the University of Alabama, Birmingham. The IP address was somehow connected to a Falun Gong supporter or site.

On display on a monitor display playing behind the newscaster were Chinese characters reflective of a distributed denial of service attack type of software, and of a PLA attack system. Next, characters to the effect of "choose attack target" were displayed, then the U.S. based IP address.

Andrew Erickson, associate professor at the U.S. Naval War College's China Maritime Studies Institute, and Gabriel Collins, a commodities and security specialist focusing on Russia and China wrote in a report the whole of the above tended to validate the PLA had orchestrated cyber attacks outside of the PRC.

If this were to be true, it would tend to contradict Chinese protestations to the contrary.

See the article detailing this information in its entirety at http://online.wsj.com/article/SB10001424053111904009304576528363095538754.html?mod=googlenews_wsj .

SEPTEMBER IN COUNTERINTELLIGENCE HISTORY

- September 1, 1919: The Communist Party of America was formed.
- September 6, 1939: In response to the Nazi and Soviet invasions of Poland on September 1, 1939, Executive Order 8247 was signed by President Roosevelt, designating the FBI as the responsible entity for the coordination and dissemination of intelligence and security information to other Federal Agencies. President Roosevelt publicly announced that the FBI was to take charge of investigative work in matters relating to espionage, sabotage, and neutrality act violations.
- September 18th, 1950: Alfred Dean Slack of Syracuse, New York was indicted on espionage charges in connection with passing secrets about high explosives to Harry Gold, a pivotal member of the Atom Bomb Spies that included the Rosenbergs. Slack was a chemist by profession. He was sentenced on 9/22/1950 to 15 years in prison.
- September 23rd, 1950: The McCarran Act (The Internal Security Act) was passed. The act created a Subversive Activities Control Board. Communists, communist front, and communist action organizations were required to register with this board. Espionage and Sabotage laws were strengthened, and subversive citizens were allowed to be detained. Subversive aliens could be deported.
- September 24th, 1996: Robert C. Kim, a Navy computer specialist, was arrested by the FBI and the Naval Criminal Investigative Service for conspiracy to commit espionage. He was convicted on 5/12/1997.
- September 28th, 1962: Yeoman First Class Cornelius Drummond of the U.S. Navy was arrested by the FBI in New York City on espionage charges

in connection with his having passed classified information to Soviet intelligence officers. He was convicted on August 15th, 1963 and sentenced to life imprisonment.

- In the month of September, 1939, the FBI was authorized to hire 150 additional agents. $1.5 million dollars were allocated for this hiring burst, and an additional $2.7 million dollars allocated for an anticipated additional 100 agents. The beginning of World War II greatly increased the caseload related to 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