FBI Tampa CI Strategic Partnership Newsletter

December 19, 2011
Volume 1, Issue 5

Federal Bureau of Investigation | Tampa Division
5525 West Gray Street
Tampa, FL 33609, 813-253-1000

INSIDE THE ISSUE

COUNTERINTELLIGENCE TRENDS

Guess who: The 25 worst passwords of 2011

GOVERNMENT COMPUTER NEWS
November 18, 2011

It probably won't surprise you that the most common password used online is "password," followed by the ever-popular "123456." It wouldn't surprise a hacker trying to steal your personal information, either.

Security company **SplashData** has published its list of the worst passwords of 2011, compiled from millions of stolen passwords that hackers had posted online, according to **Daily Finance**.

Use of bad, easily guessed passwords has been a complaint of security experts since the dawn of the Web, but little seems to have changed. "Password" and the numbers 1 through 8 — in varying lengths but always in order — litter the list, along with gems such as "qwerty," "abc123" and even "111111."

This year, for some reason, words such as "monkey," "dragon" and "sunshine" also appear, along with common first names "ashley" and "michael."

Weak passwords can make life easy for hackers looking to get into your bank records and other sensitive information.

The company recommends that users use passwords of eight characters or more, mixing in letters, numbers and special characters when allowed, separate short words with spaces or underscored and don't use the same user name and password for multiple websites. But then everybody knows that. Doing it is another story.

Below are SplashData's 25 worst password of the year.
1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon
11. baseball
12. 111111
13. iloveyou
14. master
15. sunshine
16. ashley
17. bailey
18. passwOrd
19. shadow
20. 123123
21. 654321
22. superman
23. qazwsx
24. michael
25. football

China and the Economic Espionage Act of 1996

STRATEGY PAGE
November 2, 2011

On October 18th, Chinese-born Kexue Huang pled guilty in an American court to stealing trade secrets from his employers (Dow Chemical Company and Cargill) and sending them to China and Germany. This was the eighth time someone was charged under the Economic Espionage Act of 1996, a law which made it a federal criminal offense to steal trade secrets. Most of these prosecutions have involved China.

Sometimes the Chinese connection is cleverly concealed. Four years ago, a Chinese engineer (Yuefei Ge) and a Chinese-American one (Lan Lee) were prosecuted for stealing military laser and communications technology, and then seeking backing from a company owned by the Chinese military, to finance the development of military equipment, based on the stolen technology. The two were tried for economic espionage, based on the 1996 Economic Espionage Act.

What was clever about Ge and Lee was that they were not stealing technology for a foreign power, but for the purpose of developing militarily useful applications of the technology. These items would then be sold to China, particularly if the Chinese came through with the research and development money. China has thus mobilized the power of venture capital to encourage their spies. Up until that point, only three people had been convicted of economic espionage, as defined by this Act, but the FBI was finding there was a lot more of it out there. The first conviction in a trial only occurred last year. Most of those caught tend to plead guilty in order to avoid a harsher sentence.

Some of these investigations are uncovering espionage efforts that have gone on for decades. Two years ago, a U.S. court convicted a Chinese born American citizen of spying for China for over 30 years. Born in China in 1936, Dongfan Chung arrived in Taiwan in 1948, and came to the United States in 1962. He then spent four decades working for aerospace firms, mainly Boeing, before he was arrested in 2006. Documents found in his home detailed his long relationship with Chinese intelligence, and his passing on technical details of the Space Shuttle (which Chung spent most of his career working on), in addition to the Delta IV satellite launcher, the F-15 fighter, B-52 bomber, CH-46/47 helicopters, and several other military systems. Chung was still working as a consultant for Boeing when he was arrested. He was sentenced to 16 years in prison, a sentence that was upheld on appeal this year.

Chung was the second person, and first American, convicted under the 1996 Economic Espionage Act. His lawyers admitted that Chung possessed thousands of classified documents in his home, but tried to make the case that he never actually transferred any of this material to Chinese intelligence. The jurors did not believe this defense.

GPS Intelligence Announces Availability of MicroTracker II Tracking Device

AZOSENSORS
October 31, 2011

GPS Intelligence has released the MicroTracker II, a GPS tracker capable of monitoring multiple objects of value including people, assets and vehicles. The portable MicroTracker II allows owners to monitor high value assets such as shipments and inventory as well, while the tracker securely tracks its safe dispatch and delivery.

The MicroTracker II adds extra security with its high sensitivity and is ideal for high profile events, meetings and international travel.

The national sales manager of GPS Intelligence, Brian Arrowood stated that the MicroTracker II is not only the smallest tracker but is also capable of tracking for extended periods of time where there may be weak or obstructed GPS signals.

Available in black and white designs, the small device can be carried in a briefcase, backpack, computer bag and purse and can also be attached to a belt. It is a lightweight tracking device weighing only 2.12 ounces. Its sensitivity and accuracy can pinpoint a location in rural, urban and mountainous regions.

The MicroTracker II is small enough to drop in a purse, attach to a belt, or slip into any backpack, briefcase or computer bag. This is ideal for parents who can monitor the safety of their children during transit, in sporting events and after-school programs. Moreover, the parents can also track the movements of their children when they go cross-town, hiking, camping or on out-of-town holidays.

For asset and vehicle safety, the device can be placed in the glove compartment or a briefcase, providing excellent anti-theft security. The users are provided with notifications when the vehicle is moving, wanders awake from the track or stops. The MicroTracker II includes Geo-Fence boundary alerts, motion alerts, Locate Now, Address & Stop reports, aerial, birds-eye, 3D and 2D views and Panic Button features. Tracking assistance and support is available with the Coverttrack online tracking center.

DOD Reports 'Stunning' Spike In Espionage Targeting U.S. Military Technology, Trade Secrets

INSIDEDEFENSE.COM
October 25, 2011

A new Pentagon report finds "a stunning increase" in espionage targeting sensitive U.S. military technology and defense industry trade secrets over the last year, including newly concerted efforts -- particularly from East Asia and the Pacific -- to acquire autonomous underwater vehicle technology.

In fiscal year 2010, private firms that build the Pentagon's arsenal reported to the Defense Security Service a 140-percent increase over FY-09 in "suspicious contact reports determined to be of intelligence value" from "both friends and foes," according to the new DOD accounting.

“The technology base of the United States is under constant attack,” states the previously unreported 78-page assessment, "Targeting U.S. Technologies: A Trend Analysis Of Reporting From Defense Industry." The report was published by the Defense Security Service, an arm of the Pentagon acquisition executive's directorate, on Oct. 19.

"The number of suspicious contact reports resulting from foreign attempts to obtain illegal or unauthorized access to sensitive or classified information and technology resident in the U.S. cleared industrial base more than doubled from FY-09 to FY-10," states the report. "The large scope and diversity of collection efforts targeting U.S. technologies meant that foreign entities simultaneously directed considerable efforts at many technologies using variations of methods and collectors."

The majority of collection attempts over the last year originated from East Asia and the Pacific region, according to the report, and commercial firms “were the most active collector” for a second consecutive year.

The DSS report highlights "the increasing foreign threat" to autonomous underwater vehicle technology. More than 70 percent of the efforts to gain information about this area have come from the Pacific Rim, according to the report.

"The U.S. Navy’s ability to establish and maintain underwater battlespace dominance is of special importance in this region," the report states. "Successful development of AUVs for East Asian and Pacific military purposes would likely pose a threat to that dominance by increasing foreign understanding [of] U.S. AUV technologies, potentially enabling them to develop effective countermeasures."

DOD suppliers reported to the Pentagon efforts by foreigners to obtain information and access to technologies across all of the Military Critical Technology List's 20 categories, according to the report. Two technology areas of greatest interest, according to the DSS, were information systems and lasers, optics and sensors. Aeronautics and electronics technologies ranked third and fourth, according to the report.

"FY-10 witnessed a persistent stream of collection attempts targeting U.S. technologies," the report states. "Entities from all regions of the globe sought U.S. technologies to obtain an advantage against regional adversaries, replicate U.S. capabilities, develop countermeasures to U.S. systems, or simply profit commercially. Both friends and foes targeted U.S. technologies."

The DSS report, prepared annually based on information provided by cleared contractors, is the unclassified version of an assessment that details suspicious contacts. The goal is to identify attempts to obtain illegal access to sensitive or classified information or technologies.

"The stakes are high in the battle against foreign collection and espionage targeting U.S. technology, trade secrets, and proprietary information," Stanley Sims, the Defense Security Service director, states in the report's preface. "Not only is our national security at risk but also our technological edge, which is closely tied to the health of our economy and the economic success of the cleared contractor community. Most importantly, every time our adversaries gain access to restricted information it jeopardizes the lives of our warfighters, since those adversaries can use the information to develop more lethal weapons or countermeasures to our systems."

Foreign commercial companies whose business includes supplying militaries account for 35 percent of the "suspicious" contacts, according to DSS, a decrease from nearly 50 percent in FY-09. Suspicious contacts reported from "government" collectors, ministries of defense, branches of the military, foreign military attaches and foreign liaison officers fell to 11 percent. Three other categories saw corresponding increases in FY-10: "government affiliated" individuals representing research institutes, laboratories and universities; "individuals" seeking financial gain or ostensibly conducting academic or otherwise "research" work; and individuals whose affiliation is "unknown."

FBI Official Calls for Alternate Internet to Secure Critical Systems

GOVERNMENT COMPUTER NEWS
October 24, 2011

The United States needs an alternate, transparent, restricted Internet if it is to secure the critical systems that handle such things as utilities and financial transactions, an FBI official says.

Shawn Henry, the bureau's executive assistant director, speaking at the International Systems Security Association conference recently, said the increasing numbers of cyber threats continue to outpace efforts to defend critical computer systems. These efforts are further hampered by the anonymity of the Internet.

"We can't tech our way out of the cyber threat," Henry said, according to the **Associated Press**. "The challenge with the Internet is you don't know who's launching the attack."

Earlier this month, the Government Accountability Office released a **report** stating that information security incidents at 24 federal agencies have increased 650 percent during the past five years due to a combination of more numerous threats and persistent shortcomings in security controls, **GCN reported**.

Having an alternate Internet accessible only by known, trusted parties, with no anonymity, would greatly improve defense efforts, said Henry, who called cyber threats one of the "most serious threats" facing the nation, reported **eWeek**.

Henry called the Internet "arguably the greatest invention" but at the same time an "incredibly dangerous place," eWeek reported. He also advocated taking highly sensitive information completely offline.

Henry is not the only FBI official calling for a separate, more secure network, nor is the FBI the first to mention such an option. At the May Federal Computer Week Federal Executive Briefing on risk mitigation, Steven Chabinsky, deputy assistant director of the FBI's Cyber Division, also called for an alternate network with greater visibility and less privacy, **GCN reported**.

"There is no such thing as safe and secure cloud computing because there is no such thing as safe and secure computing," he said. Chabinsky stopped short of suggesting a separate Internet or proposing a specific architecture.

And people file-sharing information pirates, upset that a group such as WikiLeaks can lose its Web hosting company after running afoul of authorities, have talked about building their own alternate Internet registry, **New Scientist** reported.

Why Smart Phones are Targets: Popularity is Up, Security is Down

GOVERNMENT COMPUTER NEWS
October 20, 2011

Smart phones and tablets will increasingly become targets for malware attacks not only because of their growing popularity but because security steps for the devices are often difficult or ignored, according to a newly released security advisory report out of Georgia Tech.

"Mobile applications are increasingly reliant on the browser," said Patrick Traynor, GTISC researcher and assistant professor at the Georgia Tech School of Computer Science. "As a result, we expect more Web-based attacks against mobile devices to be launched in the coming year."

The Emerging Cyber Threats Report 2012, presented at last week's Georgia Tech Cyber Security Summit 2011, focused specifically on the rise of vulnerabilities from mobile browsers and applications that are reliant on an Internet connection. In one example, researchers discussed that smart phone users aren't as aware as desktop and laptop users when a malicious link is clicked due to the smaller screen size and disappearing address bar.

Another reason the fact that Internet security protocol information is either lacking or hard to access on mobile devices. "If you're a security expert and you want to see the [Secure Sockets Layer] certificates for a site from your mobile phone browser, it is extremely difficult to find that information -- if it's there at all," said Traynor. "And if a security expert can't verify a connection and a certificate, how do we expect the average user to avoid compromise?"

The report points to not only the lack of verification by security experts, but also the lack of overall problem solving when vulnerabilities do arise. The report cited that device constraints and "tension between usability and security" make it difficult for security experts to devote time to debug issues.

This is evident in that, unlike traditional Web browsers, mobile browsers rarely get fixes for issues that arise over time. "One of the biggest problems with mobile browsers is that they never get updated," said Dan Kuykendall, co-CEO and chief technology officer for NT OBJECTives. "For most users, their operating system and mobile browser is the same as it was on the phone's manufacture date. That gives the attackers a big advantage."

Another disadvantage to mobile security is in the case of how quickly a patch or fix can be applied on the rare instances of updates. While fixes can be turned around in a matter of days for a specific vulnerability, it can take months to roll out, due to OS limitations and carrier testing and regulations, giving would-be attackers plenty of time to exploit the hole before going unpatched.

Georgia Tech's security report forecasts that attacks will become more sophisticated and numerous in the next few months, especially for those targeting the Android and iOS platforms. During the study, researchers have noticed an evolution of attacks on these two mobile OSes that rival computer viruses.

"The Zeus-in-the-Mobile (ZitMo) and several other examples of Android malware are acting more like traditional bots by communicating with a command-and-control (C2) architecture," said Gunter Ollmann, vice president of research for Damballa, in the report. "This marks an evolution beyond premium rate fraud and other tactics that do not rely on C2, and makes mobile devices as susceptible to criminal breach activity as desktops."

While criminal breeches of tablets and smartphones and the spreading of malware are growing risks in the mobile security landscape, researchers at Gergia Tech also point to these same devices being used to spread harmful programs to desktops.

Researchers noticed an uptick of security incidents involving the upload of harmful software through a mobile device connected to a traditional PC. This attack, while not new, had previously been associated with the transfer of malware through USB devices.

The threats report advises that with the growing increase of smartphone and tablet attacks, security protocols need to evolve with the attacks, especially in the enterprise setting.

"As mobile devices become an increasingly attractive target in the integrated economy, it is critical for organizations to adopt a multi-faceted strategy that leverages the right combination of security best practices with business technology requirements," said Tony Spinelli, senior vice president and chief security officer of Equifax.

ARRESTS, TRIALS AND CONVICTIONS

U.S. Court Awards DuPont $920.3 Million in Damages

REUTERS
November 23, 2011

SEOUL (Reuters) - A U.S. court awarded DuPont $920.3 million in damages on Tuesday, ruling that South Korea's Kolon Industries Inc <120110.KS> violated trade secrets for a fiber used to make Kevlar bulletproof vests, Kolon said on Wednesday.

The South Korean firm said in a regulatory filing that it would appeal the decision and take all legal measures in response to the court ruling.

A U.S. federal jury in September ordered Kolon Industries Inc to pay $919.9 million in damages after finding the textile company willfully and maliciously stole trade secrets and confidential information regarding its Kevlar para-aramid fiber.

Devens Company Seeks $1.2b from Chinese Firm

BOSTON GLOBE
November 10, 2011

American Superconductor Corp. is seeking more than $1.2 billion in damages and payments for contracted shipments from its once-largest customer, a Chinese wind turbine maker accused of stealing the Devens firm’s technology.

During a call with investors yesterday, American Superconductor chief executive Daniel P. McGahn said the company has filed several lawsuits in China against Sinovel Wind Group Co. of Beijing, alleging copyright infringement and theft of trade secrets.

Court and arbitration proceedings are expected to begin in the next few months, as the company tries to collect damages as well as nearly $70 million owed for past shipments ordered by Sinovel and $700 million in undelivered parts.

“We believe the strength of our cases is undeniable,’’ McGahn said.

American Superconductor, which makes control systems for wind turbines and other advanced technologies for utilities, began to suspect Sinovel of theft in June, following the Devens company’s discovery of an imperfect

replica of its software in a Sinovel wind turbine in China. Months before, the Chinese company had stopped accepting shipments of parts from American Superconductor, causing its revenues to plunge.

An investigation eventually led the company to an engineer at an American Superconductor subsidiary in Austria, who was later found guilty of stealing proprietary software and sentenced by Austrian authorities to a year in jail. Sinovel could not be reached for comment yesterday. The Chinese company has explicitly denied stealing American Superconductor's technology, and says American Superconductor's products had become subpar and failed to meet requirements for China's power grid. It has filed a counterclaim with the Beijing Arbitration Commission against American Superconductor, alleging breach of contract.

But yesterday, McGahn told investors he believes his company has strong evidence against Sinovel, including "hundreds of e-mails between senior Sinovel staff members and our now incarcerated former employee,'' and Chinese officials will rule in favor of American Superconductor.

"These messages give a detailed account and timetable of the crime,'' McGahn said. "They show that certain senior level Sinovel employees knew that this [intellectual property] was obtained illegally.''

Those details helped boost the company's stock, which rose about 11 percent to close at $4.53 per share.

Chun Sentenced for Illegally Exporting Defense Articles without a License

U.S. DEPARTMENT OF JUSTICE
November 10, 2011

Kue Sang Chun, age 67, of Avon Lake, Ohio, was sentenced to 14 months in prison for illegally shipping components used in infrared rifle scopes to South Korea, federal law enforcement officials announced today.

Chun previously pleaded guilty to one count of exporting defense articles on the U.S. Munitions List without first obtaining an export license or written authorization from the U.S. Department of State, and one count of knowingly making and subscribing a false U.S. Individual Income Tax return.

"This defendant violated important regulations designed to protect national security," said Steven M. Dettelbach, United States Attorney for the Northern District of Ohio. "He did it for money and intentionally failed to pay taxes on the money he made from his crimes.

Steven Anthony, Special Agent in Charge of the Federal Bureau of Investigation's Cleveland Field Office, said: "Investigations surrounding the foreign acquisition of U.S. defense articles outside of legitimate channels are among the most serious matters the FBI handles. Helping to maintain the technological advantage of the U.S. defense industry and our military demands our very best effort in these regards.

"Whether an individual infrared detector or 100 of them, the American public can be assured that the FBI will exhaust every available avenue to recover any item exported illegally and to hold all involved accountable," Anthony said.

Chun is a former employee at the NASA Glenn Research Center, though he is not accused of taking technology or related materials from there.

Chun, between 2000 and 2005, knowingly exported and caused the export from the United States to the Republic of Korea (South Korea) of Infra Red Focal Plane Array detectors and Infra Red camera engines which were designated as defense articles on the United States Munitions List, according to court documents. Chun did so without first obtaining an export license or written authorization for such export from the U.S. Department of State.

Count two charges Chun with knowingly making and subscribing a false U.S. Individual Income Tax return for the year 2005, which failed to report approximately $83,399.08 of taxable income he earned during said tax year.

This case is being prosecuted by Assistant U.S. Attorneys Robert W. Kern and Justin E. Herdman of the Cleveland U.S. Attorney's Office, following an investigation by the Cleveland Offices of the Federal Bureau of Investigation and the Internal Revenue Service, Criminal Investigations.

The investigation is ongoing.

Chinese-born Motorola engineer charged with stealing trade secrets

WANT CHINA TIMES
November 8, 2011

Jin Hanjuan, a Chinese-born US citizen, has been charged by US prosecutors of stealing trade secrets for a Chinese company linked to the People's Liberation Army. This has been the seventh economic espionage case in the US this year, among which only one has not involved China, Bloomberg reports.

Jin was caught attempting to bring over 1,000 documents downloaded from a Motorola computer as well as US$31,000 in cash to China when she was stopped by a random check at Chicago's O'Hare International Airport in February 2007.

US prosecutor Christopher Stetler said Jin, who bought a one-way ticket to China, was set to accept a job offer at SunKaisens, a Beijing-based company providing communication systems for the Chinese military. "This is a woman who led a double life," Stetler was quoted as saying by the Associated Press.

During her time at Motorola Solutions as a software engineer, Jin also worked for mobile communication system developer Lemko, founded by former Motorola employee Shaowei Pan, who has been accused of stealing trade secrets. Jin faces up to 15 years in prison for economic espionage and is also charged with three other offences, Bloomberg reported.

Westman Gaus, Jin's lawyer, said the documents Jin carried did not contain any information that could be classified as trade secrets. He said Jin tried to refresh her technology knowledge after taking a one-year medical leave. The technology the documents contained concerned "walkie-talkie type features on Motorola cellphones," according to AP. It was an obsolete technology, Gaus said.

In addition, the defense lawyer questioned Motorola's motive. If the documents contained sensitive information, they should not be able to be downloaded and accessed easily. Lemko's spokesman Raymond Minkus said Motorola has overvalued the reported trade secrets and tried to cover up mismanagement. Lemko also accused Motorola Solutions of using business relations to interfere with the legal process.

In October, Chinese-born Canadian scientist Kexue Huang admitted he passed trade secrets belonging to AgroSciences LLC and Cargill where he worked to Hunan Normal University, causing losses worth US$7 billion to the US companies.

Five Individuals Indicted in a Fraud Conspiracy Involving Exports to Iran of U.S. Components Later Found in Bombs in Iraq: Indictment Also Alleges Fraud Conspiracy Involving Illegal Exports of Military Antennas to Singapore and Hong Kong

U.S. DEPARTMENT OF JUSTICE
October 25, 2011

WASHINGTON – Five individuals and four of their companies have been indicted as part of a conspiracy to defraud the United States that allegedly caused thousands of radio frequency modules to be illegally exported from the United States to Iran, at least 16 of which were later found in unexploded improvised explosive devices (IEDs) in Iraq. Some of the defendants are also charged in a fraud conspiracy involving exports of military antennas to Singapore and Hong Kong.

Yesterday, authorities in Singapore arrested Wong Yuh Lan (Wong), Lim Yong Nam (Nam), Lim Kow Seng (Seng), and Hia Soo Gan Benson (Hia), all citizens of Singapore, in connection with a U.S. request for extradition. The United States is seeking their extradition to stand trial in the District of Columbia. The remaining individual defendant, Hossein Larijani, is a citizen and resident of Iran who remains at large.

The arrests and the indictment were announced by Lisa Monaco, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; John Morton, Director of the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE); Mark Giuliano, Executive Assistant Director of the FBI's National Security Branch; Eric L. Hirschhorn, Under Secretary of Commerce; and David Adelman, U.S. Ambassador to Singapore.

"Today's charges allege that the defendants conspired to defraud the United States and defeat our export controls by sending U.S.-origin components to Iran rather than to their stated final destination of Singapore. Ultimately, several of these components were found in unexploded improvised explosive devices in Iraq," said Assistant Attorney General Monaco. "This case underscores the continuing threat posed by Iranian procurement networks seeking to obtain U.S. technology through fraud and the importance of safeguarding that technology. I applaud the many agents, analysts and prosecutors who worked on this extensive investigation."

"These defendants misled U.S. companies in buying parts that they shipped to Iran and that ended up in IEDs on the battlefield in Iraq," said U.S. Attorney Machen. "This prosecution demonstrates why the U.S. Attorney's Office takes cases involving misrepresentations regarding the intended use of sensitive technology so seriously. We hope for a swift response from Singapore to our request for extradition."

"One of Homeland Security Investigations' (HSI) top enforcement priorities is preventing sensitive technology from falling into the hands of those who might seek to harm American personnel or interests — whether at home or abroad," said ICE Director Morton. "This international investigation conducted by ICE's HSI and our law enforcement partners demonstrates the importance of preventing U.S. technology from falling into the wrong hands, where it could potentially be used to kill or injure our military members and our allies. Our agency will continue to work closely through our attachés to identify these criminals, dismantle their networks, and ensure they are fully prosecuted."

"This multi-year investigation highlights that acquiring property by deceit has ramifications that resonate beyond the bottom line and affects our national security and the safety of Americans worldwide," said FBI Executive Assistant Director Giuliano. "We continue to work side-by-side with our many partners in a coordinated effort to bring justice to those who have sought to harm Americans. We consider this investigation as the model of how we work cases - jointly with the Department of Homeland Security/Immigration and Customs Enforcement and the Department of Commerce/Office of Export Enforcement and collectively with our foreign partners to address the threats posed by Iranian procurement networks to the national security interests of the United States both here and abroad."

"These cases are the product of vigorous, cooperative law enforcement focused on denying to Iran items that endanger our coalition forces on the battlefield in Iraq," said Under Secretary of Commerce Hirschhorn. "We will continue aggressively to go after such perpetrators -- no matter where they operate -- to guard against these types of threats."

U.S. Ambassador to Singapore, David Adelman, praised the cooperation within the U.S. executive branch agencies and with the Singaporean authorities. "Twenty-first century law enforcement is most effective when countries work collaboratively as evidenced by this strong, cooperative effort between the U.S. and Singapore. Congratulations to all the officials in both our countries who made this happen," he said.

The Charges

The indictment, which was returned in the District of Columbia on Sept. 15, 2010, and unsealed today, includes charges of conspiracy to defraud the United States, smuggling, illegal export of goods from the United States to Iran, illegal export of defense articles from the United States, false statements and obstruction of justice.

The charged defendants are Iranian national Larijani, 47, and his companies Paya Electronics Complex, based in Iran, and Opto Electronics Pte, Ltd., based in Singapore. Also charged is Wong, 39, an agent of Opto Electronics who was allegedly supervised by Larijani from Iran. The indictment also charges NEL Electronics Pte. Ltd., a company in Singapore, along with NEL's owner and director, Nam, 37. Finally, the indictment charges Corezing International Pte. Ltd., a company in Singapore that maintained offices in China, as well as Seng, 42, an agent of Corezing, and Hia, 44, a manager, director and agent of Corezing.

Wong, Nam, Seng and Hia allegedly conspired to defraud the United States by impeding U.S. export controls relating to the shipment of 6,000 radio frequency modules from a Minnesota company through Singapore to Iran, some of which were later found in unexploded IEDs in Iraq. Seng and Hia are also accused of conspiring to defraud the United States relating to the shipment of military antennas from a Massachusetts company to Singapore and Hong Kong. Singapore has agreed to seek extradition for Wong and Nam on the charge of conspiracy to defraud the United States relating to the components shipped to Iran, and to seek extradition for Seng and Hia on the charge of conspiracy to defraud the United States relating to the military antenna exports.

In coordination with the criminal actions announced today, the Commerce Department announced the addition of 15 persons located in China, Hong Kong, Iran and Singapore to the Commerce Department's Entity List. In addition to the five individual defendants in this case, the Commerce Department named additional companies and individuals associated with this conspiracy. In placing these parties on the Entity List, the Commerce Department is imposing a licensing requirement for any item subject to Commerce regulation with a presumption that such a license would be denied.

Exports of U.S. Components Later Found in IEDs

According to the indictment, IEDs caused roughly 60 percent of all American combat casualties in Iraq between 2001 and 2007. The first conspiracy alleged in the indictment involved radio frequency modules that have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs.

The indictment alleges that, between June 2007 and February 2008, the defendants fraudulently purchased and caused 6,000 modules to be illegally exported from the Minnesota company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, the defendants allegedly told the Minnesota firm that Singapore was the final destination of the goods. The defendants also caused false documents to be filed with the U.S. government, in which they claimed that a telecommunications project in Singapore was the final end-use for the modules. In reality, each of the five shipments was routed from Singapore to Iran via air cargo. The alleged recipient of all 6,000 modules in Iran was Larijani, who had directed Wong, his employee in Singapore, to order them.

According to the indictment, the defendants profited considerably from their illegal trade. The defendants allegedly made tens of thousands of dollars for arranging these illegal exports from the United States through Singapore to Iran.

The indictment alleges that several of the 6,000 modules the defendants routed from Minnesota to Iran were later discovered by coalition forces in Iraq, where they were being used as part of the remote detonation systems of IEDs. In May 2008, December 2008, April 2009, and July 2010, coalition forces found no less than 16 of these modules in unexploded IEDs recovered in Iraq, the indictment alleges.

During this period, some of the defendants were allegedly communicating with one another about U.S. laws prohibiting the export of U.S.-origin goods to Iran. For example, between October 2007 and June 2009, Nam contacted Larijani in Iran at least six times and discussed the Iran prohibitions and U.S. prosecutions for violation of these laws. Nam later told U.S. authorities that he had never participated in illicit exports to Iran, even though he had participated in five such shipments, according to the indictment.

Exports of Military Antennas

The indictment further charges Seng, Hia, and Corezing with a separate fraud conspiracy involving the illegal export of two types of military antenna from the United States. The indictment alleges that these defendants conspired to defraud the United States by causing a total of 55 cavity-backed spiral antennas and biconical antennas to be illegally exported from a Massachusetts company to Singapore and Hong Kong without the required State Department license.

These military antennas are controlled for export as U.S. munitions and are used in airborne and shipboard environments. The indictment states that the biconical antenna, for example, is used in military aircraft such as the F-4 Phantom, the F-15, the F-111, the A-10 Thunderbolt II and the F-16 combat jets.

Seng, Hia and Corezing are alleged to have, among other things, conspired to undervalue the antennas to circumvent U.S. regulations on the filing of shipper's export declarations to the U.S. government. They also allegedly used false names and front companies to obtain the antennas illegally from the United States.

Additional Misrepresentations

The indictment further alleges that Larijani, based in Iran, made false statements about doing business with an accused Iranian procurement agent and that he attempted to obstruct an official proceeding by the U.S. Department of Commerce.

In January 2010, the Department of Commerce placed Larijani's company, Opto Electronics, on the Entity List, which is a list of companies to which U.S. businesses cannot export controlled dual-use items without obtaining U.S. government licenses. In response, Larijani repeatedly contacted Commerce Department officials in Washington, D.C., from Iran, requesting that his company be removed from the Entity List, according to the indictment. Commerce officials advised Larijani that, in considering whether his firm should be removed from the list, he needed to disclose whether he or his firm had any involvement with Majid Kakavand or Evertop Services Sdn Bhd.

Kakavand is an accused Iranian procurement agent who has been indicted in the United States, along with his Malaysian company Evertop Services, for illegally exporting U.S. goods to Iran, including to military entities in Iran involved in that nation's nuclear and ballistic missile programs. Kakavand remains a fugitive and is believed to be in Iran.

According to the indictment, Larijani denied to Commerce officials on three occasions that he or his company, Opto Electronics, had done any business with Kakavand or Evertop Services. In fact, the indictment alleges that Larijani had been in communication with others about his business dealings with Kakavand on at least five occasions from 2006 through 2009.

This investigation was jointly conducted by ICE agents in Boston and Los Angeles; FBI agents in Minneapolis; and Department of Commerce, Bureau of Industry and Security agents in Chicago and Boston. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control, and the Office of International Affairs in the Justice Department's Criminal Division, particularly the Justice Department Attaché in the Philippines, as well as the FBI and ICE Attachés in Singapore.

U.S. law enforcement authorities thanked the government of Singapore for the substantial assistance that was provided in the investigation of this matter.

The prosecution is being handled by Assistant U.S. Attorneys Anthony Asuncion and John W. Borchert of the U.S. Attorney's Office for the District of Columbia; and Trial Attorneys Jonathan C. Poling and Richard S. Scott of the Counterespionage Section of the Justice Department's National Security Division.

The public is reminded that an indictment contains mere allegations. Defendants are presumed innocent unless and until proven guilty in a court of law.

Woman Sentenced in Effort to Smuggle Scopes to Russia

NY TIMES
October 24, 2011

She would always be "the other Anna," her alleged criminal misdeeds and her personal life not quite the measure of the Anna who came before her.

But Anna Fermanova would nonetheless be linked to Anna Chapman, for reasons beyond given names. Ms. Chapman was one of 10 members of a Russian spy ring brought down by the Federal Bureau of Investigation last year. Her nights on the town and alluring photographs on Facebook enthralled the media and evoked a character out of a James Bond movie.

Ms. Fermanova was arrested in July 2010, shortly after Ms. Chapman was, for trying to smuggle night-vision weapon scopes to Russia. Ms. Fermanova, who had a similar predilection for posting stunning pictures on Facebook, became a news media darling herself, inspiring headlines like, "Anna Fermanova Is America's New Sexy Russian Outlaw."

But that is where the two cases diverge. Ms. Chapman and her comrades pleaded guilty to conspiracy to act as unregistered agents and were returned to Russia less than two weeks after their arrest as part of a prisoner swap, the likes of which have not been seen since the cold war. They were hailed as heroes in Russia, where Ms. Chapman began hosting a weekly television program.

Ms. Fermanova, 25, also pleaded guilty, but the prosecution and her lawyers agreed that she was not a spy. Her defense lawyer, Scott H. Palmer, said that being foolish was more like it.

Ms. Fermanova was before a Federal District Court judge in Brooklyn on Monday, begging for leniency in a sentencing hearing.

Mr. Palmer said his client, with the help of her soon-to-be ex-husband, bought the scopes legally in the United States and tried to sell them illegally to men in Russia who, she believed, were hunters. Ms. Fermanova has pleaded guilty to the unlicensed export of an item on the United States Munitions List, military defense items subject to government control.

"I just wanted to say that I was truly sorry for what I did," Ms. Fermanova said, wiping away tears. "I completely realize it was a really foolish act. It was a means to make a little extra cash."

Mr. Palmer argued for a sentence of probation because, he said, Ms. Fermanova, who was born in Latvia but is a United States citizen living in Texas, did not know that the items could have slipped into the wrong hands. The recommended sentence in such a case is 46 months in prison.

"As far as she is concerned, the hunters that were buying them were rich," Mr. Palmer said.

The judge, Carol Bagley Amon, seemed less than sympathetic to the argument. "The court recognizes that these items are not as dangerous as other items on the list," she said. But, she said, "they could have easily gotten out of the hands of hunters into another stream of commerce."

"It is the court's view," the judge added, "that deporting munitions, particularly something such as night vision goggles — this is a very serious offense. The sentence imposed has to promote a respect for the law."

The prosecutor, Seth DuCharme, also recommended a shorter sentence, though not because the government believed the crime was not serious. Ms. Fermanova had cooperated with the government, Judge Amon said.

Judge Amon ordered a sentence of four months in federal prison followed by three years of probation, including four months of being subject to home arrest. She also ordered a $1,000 fine.

Ms. Fermanova must surrender by Dec. 5.

Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets: First Prosecution in Indiana for Foreign Economic Espionage

U.S. DEPARTMENT OF JUSTICE
October 18, 2011

http://www.justice.gov/criminal/cybercrime/huangPlea.pdf

WASHINGTON – Kexue Huang, a Chinese national and a former resident of Carmel, Ind., pleaded guilty today to one count of economic espionage to benefit a component of the Chinese government and one count of theft of trade secrets.

The guilty plea was announced by Assistant Attorney General Lanny A. Breuer of the Criminal Division, Assistant Attorney General for National Security Lisa O. Monaco, U.S. Attorney Joseph H. Hogsett of the Southern District of Indiana, U.S. Attorney B. Todd Jones of the District of Minnesota, and Robert J. Holley, Special Agent in Charge of the Indianapolis Field Office of the FBI.

This is the first trade secret prosecution in Indiana under a provision of the Economic Espionage Act that prohibits trade secret theft intended to benefit a component of a foreign government. Since its enactment in 1996, there have been a total of eight such cases charged nationwide under the Economic Espionage Act.

Huang, 48, pleaded guilty to the charges before U.S. District Judge William T. Lawrence in the Southern District of Indiana. In July 2010, Huang was charged in an indictment filed in the Southern District of Indiana for misappropriating and transporting trade secrets to the People's Republic of China (PRC) while working as a research scientist at Dow AgroSciences LLC. Today, a separate indictment filed in the District of Minnesota was unsealed, charging Huang with stealing a trade secret from a second company, Cargill Inc.

According to court documents, from January 2003 until February 2008, Huang was employed as a research scientist at Dow, a leading international agricultural company based in Indianapolis that provides agrochemical and biotechnology products. In 2005, Huang became a research leader for Dow in strain development related to unique, proprietary organic insecticides marketed worldwide.

As a Dow employee, Huang signed an agreement that outlined his obligations in handling confidential information, including trade secrets, and prohibited him from disclosing any confidential information without Dow's consent. Dow employed several layers of security to preserve and maintain confidentiality and to prevent unauthorized use or disclosure of its trade secrets.

Huang admitted that during his employment at Dow, he misappropriated several Dow trade secrets. According to plea documents, from 2007 to 2010, Huang transferred and delivered the stolen Dow trade secrets to individuals in Germany and the PRC. With the assistance of these individuals, Huang used the stolen materials to conduct unauthorized research with the intent to benefit foreign universities that were instrumentalities of the PRC government. Huang also admitted that he pursued steps to develop and produce the misappropriated Dow trade secrets in the PRC, including identifying manufacturing facilities in the PRC that would allow him to compete directly with Dow in the established organic pesticide market.

According to court documents, after Huang left Dow, he was hired in March 2008 by Cargill, an international producer and marketer of food, agricultural, financial and industrial products and services. Huang worked as a biotechnologist for Cargill until July 2009 and signed a confidentiality agreement promising never to disclose any trade secrets or other confidential information of Cargill. Huang admitted that during his employment with Cargill, he stole one of the company's trade secrets – a key component in the manufacture of a new food product, which he later disseminated to another person, specifically a student at Hunan Normal University in the PRC.

According to the plea agreement, the aggregated loss from Huang's criminal conduct exceeds $7 million but is less than $20 million.

"Mr. Huang used his insider status at two of America's largest agricultural companies to steal valuable trade secrets for use in his native China," said Assistant Attorney General Breuer. "We cannot allow U.S. citizens or foreign nationals to hand sensitive business information over
to competitors in other countries, and we will continue our vigorous criminal enforcement of economic espionage and trade secret laws. These crimes present a danger to the U.S. economy and jeopardize our nation's leadership in innovation."

"Today's plea underscores the continuing threat posed by the theft of business secrets for the benefit of China and other nations," said Assistant Attorney General Monaco.

U.S. Attorney Hogsett noted that it is the first time economic espionage has been charged in the Southern District of Indiana. Hogsett remarked that "as U.S. Attorney, I am committed to working with Hoosier businesses who have been victimized and doing everything within our influence to protect Hoosier companies." Hogsett praised Dow for its cooperation with the investigation and prosecution, noting that "companies must first report and then work with federal investigators and prosecutors if we are to stem the illicit export of trade secrets vital to the economy not only of Indiana but the United States." Hogsett also stated, "the dual prosecutions from Indiana and Minnesota should serve as a warning to anyone who is considering robbing American companies of their information and weaken the American economy by selling that information to foreign governments or others that he will face severe consequences. The federal agents and prosecutors who worked tirelessly in these two cases are to be commended for their hard work and dedication."

FBI Special Agent in Charge Holley stated: "Among the various economic espionage and theft of trade secret cases that the FBI has investigated in Indiana, the vast majority involve an inside employee with legitimate access who is stealing in order to benefit another organization or country. This type of threat, which the FBI refers to as the Insider Threat, often causes the most damage. In order to maintain our competitive advantage in these sectors, industry must identify their most important equities, realize that they are a target, implement internal protection mechanisms to protect their intellectual property, and communicate issues of concern immediately to the FBI."

At sentencing, Huang faces a maximum prison sentence of 15 years on the economic espionage charge and 10 years on the theft of trade secrets charge.

The case is being prosecuted by Assistant U.S. Attorney Cynthia J. Ridgeway of the Southern District of Indiana, Trial Attorneys Mark L. Krotoski and Evan C. Williams of the Criminal Division's Computer Crime and Intellectual Property Section, and Assistant U.S. Attorney Jeffrey Paulsen of the District of Minnesota, with assistance from the National Security Division's Counterespionage Section.

Ex-U.S. government scientist admits attempted Israel spying

REUTERS
September 7, 2011

A former U.S. government scientist pleaded guilty on Wednesday to attempted espionage for passing top-secret national defense information to an undercover FBI agent posing as an Israeli intelligence officer.

The plea deal calls for Stewart Nozette, 54, of Chevy Chase, Maryland, to receive a sentence of 13 years in prison. The judge said at the hearing that he would accept the guilty plea and would impose the agreed-upon
prison term. Nozette admitted that in 2009 he provided classified information about U.S. satellites, early warning systems, defense or retaliation against large-scale attack, communications intelligence and key defense strategy elements. According to the charge, he did it with the intent to hurt the United States and to help Israel. As part of the deal, he pleaded guilty to one count and U.S. government prosecutors agreed to dismiss the remaining three counts against him. "Stewart Nozette betrayed America's trust by attempting to sell some of the nation's most closely guarded secrets for profit," said Lisa Monaco, assistant attorney general in charge of the Justice Department's

national security division. Nozette, who had top-secret security clearances, worked for various government agencies, including the Department of Energy and the U.S. space agency, NASA.

TECHNIQUES, METHODS, TARGETS

Attackers Get Sneakier with Encrypted Malware

PCWORLD
November 14, 2011

Malware just got sneaky! Well, *sneakier*, that is. Attackers in Brazil have found a way to sneak around antivirus programs by using cryptography.

Recently Dmitry Bestuzhev, Kaspersky Lab's Head of Global Research and Analysis Team for Latin America, was looking over some potentially malicious links from Brazil when he discovered some files with .jpeg filename extensions. At first glance, Bestuzhev thought that they were some form of steganography--the art and science of hiding messages. But upon further inspection, the reseacher discovered that they were actually more like .bmp (bitmap) files, than JPEGs.

The data contained within the files themselves was obviously encrypted and contained some kind of malware; Bestuzhev later discovered that the data was in the form of block ciphers--a cryptographic method that encrypts 128-bit blocks of plain text in to 128-bit blocks of cipher text. Since block ciphers can only be composed of 128-bit blocks, they must break up the message into several blocks and encrypt each one individually. A process called modes of operation allows a cryptographer to repeatedly use block ciphers to encrypt an entire program--or piece of malware, in this case.

Modes of operation can use randomization based on an additional input value making it very difficult for any one program or decryter to be able to decrypt the code. When the file is opened, unencryped code--a decryption script in this case--would then run and execute the decrypted malicious code.

Unfortunately for the Web and its users, most antivirus software relies largely on searching for patterns of data that are alike or similar to its virus definitions. Some more advanced programs use heuristics to identify not necessarily problem code but virus structures based on miscellaneous wildcard characters (*not* A-Z and 0-9) and extra pointless "padding" code. However, even when a program is using heuristics, your virus scanner may only notify you that it's an untrusted or unknown file.

Even more unfortunate, the wildcard characters could be hidden in another type of seemingly useful file (e.g. .jpeg files) that actually displays an image, and therefore, might not trigger the virus scanner at all. Could it get even worse? Yes, but to my knowledge, most, if not all, virus scanners also are incapable of determining what will happen when the decryption script is run--that is, they don't actually execute the code to find out what will happen.

According to Bestuzhev the virus writers behind this particular attack publishes new mirrors and new variants of the malware about every 2 days, though the encryption code has remained the same so far. This is certainly scary for anyone out there that values their private information, and I just hope that the antivirus software companies can keep up.

'Socialbot' fools Facebook, and users give up their info

GOVERNMENT COMPUTER NEWS
November 3, 2011

Researchers at the University of British Columbia were able to infiltrate Facebook with a herd of automated “socialbots” that went largely undetected by the network’s defenses for eight weeks, friending and harvesting personal information from thousands of users.

"We believe that large-scale infiltration in [online social networks] is only one of many future cyber threats, and defending against such threats is the first step towards maintaining a safer social Web for millions of active Web users," they wrote in a **paper** describing their experiment.

The socialbots were programmed to regularly post updates to their pages and to seek out mutual connections with existing friends who would be more likely to accept new friending requests, mimicking human behavior well enough that only 20 of 102 socialbots were detected and blocked by the Facebook Immune System.

Facebook was chosen for the experiment because it was believed to have a more robust defensive system for detecting automated activity, the researchers wrote.

The Facebook Immune System performs real-time checks on all read and write actions in the Facebook database. "In fact, we did not observe any evidence that the FIS detected what was really going on," they wrote.

The socialbot herd and its controller were all maintained on a single machine for simplicity's sake, but a more extensive network could be created using traditional botnet methods with distributed, compromised computers hosting the socialbots.

They created 49 male and 53 female accounts, each one initially friending other socialbot accounts to create the illusion of a real person with real Facebook friends. In a two-week "bootstrap" phase, each bot sent out 25 friendship requests per day to random account IDs. Of 5,053 requests, 976 — or a little more than 19 percent — were accepted.

It was found that sex matters. Female socialbots had an acceptance rate of 22.3 percent, compared with 15.9 percent for the males. Interestingly, all of the 20 socialbots that were identified and blocked were female. All were discovered because a Facebook user had flagged them for spamming.

After the bootstrapping phase, the socialbots dissolved their connections with each other and spent six weeks in propagation, sending requests to their friends' friends. Of 3,517 such requests, 2,079 or 59 percent were accepted.

The bots were programmed with HTTP-request templates that allowed each to send friendship requests as if they were sent from a browser. They also used an API provided by iheartquotes.com to pull random quotes and blurbs that were used as messages for their status updates.

The command server had interfaces with three useful websites: a CAPTCHA-breaking business to defeat CAPTCHA codes used to identify spamming bots; hotornot.com, a photo-sharing website that was used to grab photos for socialbot account profiles; and mail.ru, an e-mail provider.

"As the socialbots infiltrated Facebook, they harvested a large set of users' data," the researchers wrote. "We were able to collect news feeds, users' profile information, and 'wall' messages. We decided, however, to only focus on users' data that have monetary value such as Personally Identifiable Information."

Information gathered included birthdates, addresses, names of spouses, places of work, school attended, hometown, e-mail addresses and phone numbers.

Operating a socialbot network from your own computer apparently does not break any laws as long as there is no identity theft or fraud involved, but the researchers addressed the ethical question raised by their experiment.

"We believe that minimal-risk realistic experiments are the only way to reliably estimate the feasibility of an attack in real-world," they concluded. "These experiments allow us, and the wider research community, to get a genuine insight into the ecosystem of online attacks, which are useful in understanding how similar attacks may behave and how to defend against them."

Bad vibrations: How smart phones could steal PC passwords

GOVERNMENT COMPUTER NEWS
October 18, 2011

Smart phones are becoming sensitive enough that they could be used to steal passwords from people typing on a close-by keyboard by detecting the vibrations from the keystrokes, a Georgia Tech University research team says.

The research team found that the accelerometer on a smart phone sitting next to a keyboard could be used to interpret keyboard strokes with 80 percent accuracy, according to an **announcement from Georgia Tech**. Such an attack wouldn't be easy, but it is possible, as smart phones become increasingly sensitive, Patrick Traynor, a Georgia Tech assistant professor of computer science who led the research team, said in the release. Traynor said the research team first tested its idea with an iPhone 3GS but didn't get good results. "But then we tried an iPhone 4, which has an added gyroscope to clean up the accelerometer noise, and the results were much better," he said. "We believe that most smart phones made in the past two years are sophisticated enough to launch this attack.

The technique also exploits a component of smart phones that has been overlooked as a potential weakness. "There is information that is being leaked, and of the hardware on your phone, the accelerometer is the one thing that no one ever worried about," Traynor told **Technology Review**. "No one thought that you could turn on the accelerometer and get any meaningful data."

Accelerometers are devices inside phones that detect their position and motion. Depending on the device, they can be used to determine whether a phone's screen should be in portrait or landscape mode or when it is in motion. Accelerometers are used in gaming devices such as the Nintendo Wii for motion input and in automotive systems for automatic collision detection.

An attack would likely start with a smart-phone user being induced to download a seemingly innocuous application that contains keyboard-detection malware, the researchers said. When within range of a keyboard, the software listens for pairs of keystrokes, models the patterns of those keystrokes and compares them to a preloaded dictionary, looking for the statistically probable word being typed.

Traynor said the attack is difficult and isn't something people should worry much about. It's also easily avoided. The researchers found it had an effective range of 3 inches, so users just need to keep their phones on the other side of the desks or in their pockets. (Also, strong passwords wouldn't be found in a preloaded dictionary, although if the accuracy of such an attack improves, it conceivably could be used to steal other data, such as personal information being entered.)

Phone manufacturers also could set accelerometers with a low sample rate and have phones show a permission request if a user downloads an app that asks for a higher rate.

The Georgia Tech researchers said the accelerometers on new phones sample for vibrations at about 100 times per second — a higher rate would produce more accurate results, a lower rate less accurate ones.

By contrast, a smart phone's microphone samples for vibrations at about 44,000 per second. Although researchers have performed successful keystroke detection with microphones, manufacturers have programmed phones to ask permission for apps that request access to the device's microphone and other sensors. To date, those protected sensors haven't included accelerometers.

The researchers will present their results Oct. 20 at the 18th ACM Conference on Computer and Communications Security in Chicago.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

Zero-Day Adobe Vulnerability Targeted Defense Contractor

GOVERNMENT COMPUTER NEWS
December 8, 2011

Adobe is warning of a zero-day vulnerability in Adobe Reader on Windows that could lead to attackers hijacking a system, and that apparently has been used against defense contractor Lockheed Martin and others.

The "critical" issue, called "U3D memory corruption vulnerability" by Adobe, could cause a system to crash and also allow unrestricted access by hackers. The exploit is carried out via a hole in the compression file format called universal 3-D. While other companies, including Hewlett-Packard and Intel, use the universal 3-D file format, there has been no word of this particular vulnerability popping up in non-Adobe software.

Adobe warned that the "vulnerability is being actively exploited in the wild in limited, targeted attacks against Adobe Reader 9.x on Windows." The targets have included Lockheed Martin and Mitre, which manages many U.S. research centers, and other organizations.

Adobe credited Lockheed and the Defense Security Information Exchange (DSIE) with reporting the vulnerability. The apparent choice of targets has given rise to speculation that the exploit it being used to target defense contractors, ThreatPost **reported**.

Lockheed was the target of a failed attack earlier this year that was carried out using security token information stolen from RSA Security. RSA in March reported the breach, which gathered information on its SecurID authentication tokens, and later said it **came from a nation-state**. An additional report said the attack originated in China.

A patch is currently being worked on to fix the vulnerability found in Adobe Reader 9.x versions, and it should be released no later than Dec. 12, according to a **security advisory** issued Dec. 6. Fixing both Adobe Reader X and Acrobat X is considered to be a lower priority task for Adobe compared with fixing earlier versions of Reader.

"Because Adobe Reader X Protected Mode and Adobe Acrobat X Protected View would prevent an exploit of this kind from executing, we are currently planning to address this issue in Adobe Reader X and Acrobat X for Windows with the next quarterly security update for Adobe Reader and Acrobat, currently scheduled for Jan. 10, 2012," wrote Wendy Poland, member of the Adobe Product Security Incident Response Team, in a **blog post**.

There is also less of a risk factor for Macintosh and Unix systems to be exploited with this vulnerability, so a fix will also wait until the next quarterly update.

In the meantime, Brad Arkin, senior director of product security and privacy for Adobe, says that to be 100 percent sure your system is safe, update your older versions of Reader and Acrobat to X.

"We put a tremendous amount of work into securing Adobe Reader and Acrobat X, and, to date, there has not been a single piece of malware identified that is effective against a version X install," Arkin wrote in a **blog post**. "Help us help you by running the latest version of the software!"

Could Hackers Steal Info, Start a Fire Using Your Printer?

GOVERNMENT COMPUTER NEWS
November 30, 2011

Networked printers have long been seen by security experts as a potential — although to date unexploited — entry point into networks.

But now a team of researchers at Columbia University's School of Engineering and Applied Science say they have discovered a flaw in certain Hewlett-Packard LaserJet printers that would make it easier for hackers to gain control of the devices, potentially stealing personal information, executing attacks on networks and even giving it instructions that might make it overheat enough to catch fire, researchers said.

Exploiting the flaw, the researchers were able to give the printer so many rapid instructions that the fuser (the device that heats up to dry the ink on the paper) got hot enough to make paper smoke, **MSNBC reported**.

HP at first denied any possibility of this flaw existing, citing zero customer complaints of printers being hacked by outside users. Then the company issued a statement admitting there was a security flaw and said it was working on firmware updates but that it was impossible for their printers to cause a fire. Again, HP emphasized that there have been no complaints from customers about their printers being hacked.

HP may have a point about the fire part. Even in the researchers' private demonstration before several federal agencies earlier this month, a thermal switch shut the printer down before anything actually caught fire. HP says this switch is in all of the company's LaserJet models, so none of them could start a fire that way.

However, shutting down the printer this way effectively disables it, at least until certain parts are replaced.

HP said the vulnerability applies to some LaserJets that are connected to the Internet without a firewall. "In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network," the company said. "In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade."

The company said it is working on a firmware upgrade and will notify customers who could be affected. Meanwhile, HP recommends putting printers behind a firewall and disabling remote firmware upload on exposed printers when possible.

Although few, if any, network attacks have ever occurred via printers, this security flaw sheds light on their vulnerability to intrusion, which could open the doorway to viruses and the like. Right now, no antivirus solution on the market could detect, let alone fix, a virus that might reside on a printer's firmware. Something to think about.

But the real question is: If a printer were hacked like this, could it finish **printing its explosive detector** before catching fire? And is that dramatic irony? I always get confused about literary devices.

Lab's Behavioral System can Catch Insider Threats

GOVERNMENT COMPUTER NEWS
November 17, 2011

Researchers at the Energy Department's Oak Ridge National Laboratory are developing a tool to identify malicious insiders and stop them from sending sensitive information outside the enterprise.

The system, which is being tested in a lab environment, uses a host-based agent to "learn" a user's behavior and to look for anomalous behavior or other signatures, said computer scientist and project leader Justin Beaver.

"It turns out there is a lot of data on each host you can leverage if you know what to look for," Beaver said.

He said his team's work has demonstrated that profiles of normal behavior can be built from low-level system data on a user's computer over a relatively short time and that signatures for exfiltrating data can be recognized. The system responds to these events by seamlessly switching the malicious user to a honeypot environment where he is isolated from data but his actions can be studied.

Although the system works in the lab it is not yet ready for an operational environment, in part because of false positives, erroneous results that can trigger a response against the user.

"In this particular operation, false positives can be dangerous," Beaver said. The system will have to be tweaked to reduce false positives and to include a human in the loop to ensure that the work of legitimate users is not interrupted by mistakenly shunting them off the system.

The research is an internally funded project to address the problem of insider threats. The work does not defend against intrusions, but responds to a threat that already is inside the enterprise perimeter.

"A lot of defense is set up to operate at the perimeter," Beaver said. "The unspoken assumption is that the inside is safe. That is rarely true."

Research so far has focused on user behavior, to identify malicious humans rather than malicious code that might have been installed on a compromised machine. The logical next step would be to extend the work to malware, Beaver said. But, "right now we have a lot of user data" that can be used to define and identify suspicious behavior. Similar data on malware has not yet been collected.

Oak Ridge was the victim in April of a successful phishing attack that infected its network with what a spokesperson called a "very sophisticated" piece of malware, apparently designed to steal information from the lab's network. E-mail and Internet access at the lab were shut down until the infection could be identified and removed.

Among the characteristic information leveraged by the system are system call sequences. Each function on a computer initiates a series of calls for services. This occurs at a low level in the operating system, out of the user's view, and creates a characteristic pattern for each user over time. Researchers found that normal patterns remain surprisingly consistent for individuals as they switch between computers and jobs.

"It doesn't seem to matter at the low system call level," Beaver said. He said that the number of unique system calls forming a user's "signature" usually levels off at around 200, so that a useful baseline usually can be created in a matter of hours or days. The system also looks for other patterns of activity associated with the exfiltration of data.

This analysis and detection is done by an agent on the host computer. Response is handled on a central controller, which can move the suspect user to a dynamic honeypot that duplicates the system in which he is working.

"It looks like the same data from a navigation standpoint," Beaver said, but the actual content is false. At this time, the switch to the dynamic honeypot only works in a virtual environment, such as a cloud.

FBI busts clickjacking ring, but could the crime have been prevented?

GOVERNMENT COMPUTER NEWS
November 10, 2011

The massive clickjacking ring the Justice Department busted this week was the kind of criminal operation that Internet overseers and the government have been aiming to prevent by increasing security in the Internet's Domain Name System.
But although the protocol that would authenticate DNS queries has made its way to significant parts of the Internet, the full deployment that would make it truly effective is still a ways off.

Justice on Nov. 9 arrested six people in Estonia and issued an indictment for a seventh in Russia on charges of running a clickjacking ring that infected 4 million computers in 100 countries and netted the defendants $14 million since it started operating in 2007, the **FBI said**.

About 500,000 computers in the United States were infected, including some at government agencies such as NASA.

The alleged crime ring, operating under the company name Rove Digital and based in Estonia, made its money by using malware called DNSChanger to redirect searches for such sites as Netflix, Apple iTunes, the IRS or the Wall Street Journal to sites that paid the defendants for the traffic.

For example, the FBI said, someone clicking on a link to the iTunes store would be redirected to a sham site that purported to sell Apple software.

The DNSChanger malware changed DNS settings, routing traffic to rogue DNS servers the thieves had set up in Chicago and New York, which redirected users to malicious or unintended websites, the FBI said.

The ring was broken up after a two-year investigation, dubbed Operation Ghost Click, by the FBI along with NASA's Office of Inspector General, the Estonian Police and Border Guard Board, the National High Tech Crime Unit of the Dutch National Police Agency, and a number of academic and private-sector contributors, the FBI said.

If you think your computer may have been compromised, the FBI offers detailed instructions on how you can check **here**, or you can ask the FBI to check it **here**.

The Domain Name System, which underpins Internet activity, translates website names such as gcn.com and e-mail addresses to numerical IP addresses so computers can communicate with one another. Concern about its security arose in 2008 after security researcher Dan Kaminsky discovered a vulnerability that would allow for cache poisoning and for Web requests to be misdirected.

Kaminsky helped engineer a patch, but it was only a temporary fix, and the drumbeat began for widespread deployment of **DNS Security Extensions**, a protocol that allows DNS queries and answers to be digitally signed and authenticated, guaranteeing the origin of DNS data, data integrity, and authenticated denial of existence for an address that cannot be found.

When fully deployed, DNSSEC would help prevent such malicious tactics as such as pharming, cache poisoning and DNS redirection.

DNSSEC has made steady, if slow, progress, being deployed on the root zones of top-level domains such as .com, .gov and .net as well as on the Internet's authoritative **root zone**. But for it to work properly, it has to be deployed throughout the Internet's domains, and that's where it has run into hurdles.

The federal government, for instance, has pushed for DNSSEC deployment, with the Office of Management and Budget setting a deadline of December 2009 for deployment on all federal systems. But in July 2011, the General Services Administration said agencies had been stuck as 50 percent deployment for a year.

Among the problems agencies face are "orphan websites" that are outdated or have been abandoned, GSA's .gov program manager said then, adding that a White House plan to consolidate websites and eliminate duplicative sites could help.

New cyber attack targets chemical firms: Symantec

REUTERS
October 31, 2011

At least 48 chemical and defense companies were victims of a coordinated cyber attack traced to a man in China, according to a report from security firm Symantec Corp. Computers belonging to these companies were infected with malicious software known as "PoisonIvy," which was used to steal information such as design documents, formulas, and details on manufacturing processes, Symantec said October 31. It said the firms included multiple Fortune 100 corporations that develop compounds and advanced materials, along with businesses that help manufacture infrastructure for these industries. The bulk of the infected machines were based in the United States and United Kingdom, Symantec said, adding the victims include 29 chemicals companies, some of which developed advanced materials used in military vehicles. "The purpose appears to be industrial espionage, collecting intellectual

property for competitive advantage," Symantec said in a white paper on the campaign that it dubbed the "Nitro" attacks. The cyber campaign ran from late July through mid- September and was traced to a computer system in the United States owned by a man in his 20s in Hebei province in China, according to Symantec. Researchers said they were not able to determine if the hacker, who they dubbed "Covert Grove", acted alone or conducted the attacks on behalf of another party or parties. Symantec said the Nitro attackers sent e-mails with tainted attachments to between 100 and 500 employees at a company, claiming to be from established business partners or to contain bogus security updates. When a recipient opens the attachment, it installs "PoisonIvy," a Remote Access Trojan that can take control of a machine and that is easily available over the Internet. While the hackers' behavior differed slightly in each case, they typically identified desired intellectual property, copied it, and uploaded it to a remote server, Symantec said in its report. Dow Chemical Co said it detected "unusual e-mails being delivered to the company" last summer, and worked with law enforcers to address this situation.

'Son of Stuxnet' virus could be used to attack critical computers worldwide

MSNBC.COM
October 18

A powerful new computer virus that some are calling the "Son of Stuxnet" has infected critical infrastructure computers around the world, msnbc.com reported October 17. The new worm, dubbed Duqu, does not have the narrow focus of Stuxnet. But it shares so much code with the original virus that researchers at Symantec Corp. said it must either have been created by the same group that authored Stuxnet, or by a group that somehow managed to obtain Stuxnet's source code. "There is a common trait among the (computers) being attacked," a Symantec researcher said. "They involve industrial command and control systems." Symantec speculates that Duqu is gathering intelligence as a precursor to a future attacks. At the moment, Duqu only creates a back door into infected systems, connecting them to a command computer somewhere in India. No marching orders have yet been given, the researcher said. Duqu is so similar to Stuxnet that F-Secure's antivirus program initially identified it as Stuxnet, according to F-Secure's chief research officer. The virus is designed to leave the back door open for precisely 36 days, and then self-destruct. Symantec was first alerted to the existence of Duqu October 14, when an unnamed security firm that had already worked with a Europe-based victim shared its research with the firm. Symantec researchers worked through the weekend of October 15 and 16 trying to understand the virus. Their analysis shows Duqu may have been used to surveil computers around the world as far back as December 2010. McAfee researchers said in a blog post that both Stuxnet and Duqu utilize fraudulent "stolen" digital certificates that had been issued to companies in Taiwan. The use of what appear to be real digital certificate keys make both programs particularly deceptive.

UAV computer virus might be from gaming malware: Ground control systems for Air Force UAVs likely infected by malware used to steal log-ins and passwords

DEFENSE SYSTEMS
October 14, 2011

The computer virus that worked its way into the systems used to remotely pilot the Air Force's armed unmanned aerial vehicles in September was not an intentional attack on the systems but likely a result of malware used to steal log-ins and passwords used in online gaming, the Associated Press reports.

Air Force Space Command officials responsible for the service's cybersecurity efforts said Oct. 12 the virus did not invade the flight controls for the drones, but instead infiltrated the ground control systems for the drones flown remotely from Creech Air Force Base, Nev., according to the news network.

The virus came from malware that routinely tries to steal information from people who gamble or play games like Mafia Wars online, a defense official told the Associated Press on condition of anonymity.

The infection was discovered on a portable hard drive used to transfer information among systems at Creech, said AFSC spokeswoman Col. Kathleen Cook.

The defense official might have been speaking generally or referring to something targeting Facebook logins if Mafia Wars is indeed involved, because computer users play the game via their Facebook account, gaming security expert Chris Boyd of GFI Software told The Register.

If that's the case, the malware might have been a phishing toolbar, according to The Register.
Still, it's difficult to pin down all of the details of what occurred unless more information is released, the Register noted.

Mafia Wars maker Zynga quickly weighed in on the matter, dismissing that its product was connected with the malware that infected the Air Force's UAV systems, reports The Atlantic Wire.

"We actively take steps to maintain and protect the trust of our customers, including educating players about the risks associated with visiting untrusted sites and downloading untrusted applications," Zynga said in a statement.

RSA chief says two groups for SecurID breach

IDG NEWS SERVICE
October 11

October 11, at RSA's security conference in London, England, the RSA president revealed more details about the March 2011 attack that compromised SecurID, an authentication system used by 40 million people in at least 30,000 organizations worldwide to securely access IT systems. RSA insists the attack did not undermine the integrity of the entire system. RSA, which has worked with the FBI, DHS, British law enforcement and other agencies, believes that two groups were responsible for the attack. The EMC executive chairman declined to identify the groups, but said that due to the sophistication of the intrusion "we can only conclude it was a nation-state sponsored attack." The RSA president said both groups had been known to authorities before, although they were not known to work together. RSA spotted the attack as it was using technology from NetWitness, a company it acquired in April, the president said. It is now believed hackers gained access to RSA's systems by sending certain employees in EMC's human resources department an Excel spreadsheet rigged to exploit an Adobe Flash vulnerability, although RSA has not confirmed this. Additionally, the hackers had knowledge about RSA's internal naming conventions used for hosts on its network as well as Active Directory — a Microsoft product used for managing authentication of users on corporate networks — which made their movements inside the system appear to be more legitimate. The president said the attacks were sophisticated: they used advanced techniques to connect to RSA's systems and used different malware, some of which was compiled just hours before an attack. The data stolen was compressed and encrypted before it was exfiltrated, making it more difficult to identify.

The FBI Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

SME Patrick Laflin james.laflin@ic.fbi.gov **813-253-1029**

Individuals interested in subscribing to this publication or interested in further information should send an email or call.