EMPLOYEE

Security

CONNECTION

Volume 23 **A quarterly awareness briefing for defense industry and government employees** Number 3

In this issue. . .

Page

China Ramps up Cyber Espionage, U.S. Report Says

Whether it's using human spies or launching attacks in cyberspace, China is stepping up its intelligence efforts against U.S. government and defense-related computer systems. Experts from the U.S.-China Economic and Security Review Commission recently told Congress that Chinese hackers are going after U.S. military and civilian networks more than ever.

In its wide-ranging annual report, the commission found that China is the most aggressive nation in spying on the U.S., and is continuously seeking to recruit more Americans as spies.

It's not too strong to say that China is actually changing the way espionage is being done. The commission found a steep rise in the disruption and infiltration of U.S. government websites, as well as those of other nations that China may consider hostile.

Jump in attacks

The Department of Defense detected 54,640 malicious cyber incidents to its systems in 2008, a 20% rise from a year earlier, and that figure is expected to jump another 60% when 2009 figures are tallied. While the attacks came from all over the world, the commission said China was the largest culprit.

Not all Chinese cyber-attackers can be directly tied to that nation's government, but there is a broad category dubbed "patriotic hackers." Chinese citizens in this group may not receive official support, but China likely plans to deploy them in a conflict.

While China has historically tried to recruit Chinese-Americans as spies – believing, often incorrectly, that they were most likely to be receptive – the Chinese government is now using the Soviet model of bribing informants with cash and gifts, according to the report. The Chinese are expanding "false flag" operations, in which

ORED OFFICE OF RESEARCH AND ECONOMIC DEVELOPMENT
MISSISSIPPI STATE UNIVERSITY
Facility Security Office

sources are deceived into thinking that the information they provide is used elsewhere.

By masking the true use of stolen data, experts say, the Chinese limit the risk of alienating potential spies who don't want to harm the U.S.

As an example, the report cites the case of Tai Shen Kuo, a furniture salesman in New Orleans. He was arrested in August 2008 after persuading two retired U.S. military officials to divulge sensitive information by telling them it was headed to Taiwan rather than mainland China.

The commission also found China has launched an effort to influence U.S. think tanks and academia by rewarding scholars with access and depriving visas to more critical voices.

Case study

One incident against an unnamed U.S. technology firm was discussed in the commission report. In that case, a group of hackers used a communication channel between a host with an Internet address in the People's Republic of China and a server on the victim company's internal network.

In the months leading up to the operation, cyber-spies did extensive reconnaissance, identifying which employee computer accounts they wanted to hijack and which files they wanted to steal. They obtained credentials for dozens of employee accounts, which they accessed nearly 150 times.

The hackers then reached into the company's networks using the same type of program help-desk administrators use to remotely access computers. They copied and transferred files to seven servers hosting the company's email system, which were capable of processing large amounts of data quickly.

The attackers used at least eight U.S.-based computers, some at universities, as drop boxes before sending the sensitive data overseas. The company's security team managed to detect the theft while it was in progress, but not before significant amounts of information were compromised.

Attacks on the rise

China alone is estimated to steal $40 billion to $50 billion in intellectual property from the U.S. each year, but while it's the largest perpetrator, it is hardly the only one: DoD officials say more than 100 foreign intelligence services are known to have launched cyber-attacks on U.S. systems. The DoD alone has more than 7 million computing devices, and each one is a target!

Small wonder, then, that the military spent $100 million defending against cyber-attacks in one recent seven-month period.

Ill-prepared?

Federal cyber security is failing to keep pace with the growing array of threats, according to the Government Accountability Office, which has identified weaknesses in security controls in almost all agencies.

One underlying cause of these weaknesses is agencies' failure to effectively implement information security programs, which entail assessing and managing risk; developing and implementing security policies and procedures; promoting security awareness and training; and monitoring the adequacy of security controls.

The challenge is daunting, but the stakes are high: if the U.S. fails to adequately defend itself against cyber threats, sensitive defense and technology information will continue to flow to those who should least have it. ❑

6 Ways to Stay Cyber-Safe

The weakest link in any computer system is the individual sitting right in front of the keyboard. That means you! Here are expert tips on small, easy steps you can take:

Keep your security software and operating system current. Hackers often take advantage of web browsers and software that don't have the latest security updates.

Protect your sensitive information online. Never click on links in emails that are unfamiliar, and never give out personal data such as your password.

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information.

Don't cut corners. Sure, maybe you just want to get some work done at home. But if your company forbids you from emailing certain files to yourself, or copying them to a USB drive, obey the rules.

Keep the kids away. You'd be amazed how many security breaches have occurred because employees let their kids play a "harmless" game of Minesweeper on their work-issued laptop.

Clean desk. Before leaving the office, clear all sensitive info from your desk.

White House Security

Long before a pair of gate-crashers penetrated a White House state dinner, the Secret Service had detailed a lengthy list of security breaches dating to the Carter administration – including significant failures in the agency's protection of the president.

A recently revealed report, along with descriptions of incidents by homeland security officials, places Tareq and Michaele Salahi – the pair who talked their way into a state dinner and met President Obama – in a rogues' gallery of autograph hounds, publicity seekers, unstable personalities, and others identified by the Secret Service as defeating its checkpoints at least 91 times since 1980.

The document includes accounts such as officers mistakenly admitting to the White House grounds a family in a minivan; a man believed to be a delivery driver; and a woman previously known to agents after she had falsely claimed a "special relationship" with Bill Clinton.

NASA Scientist Offered U.S. Secrets for $2 Million

A scientist accused of attempted espionage wanted $2 million for his secrets and stashed 55 gold Krugerrand coins worth about $50,000 in a California safe deposit box, according to federal prosecutors.

The disclosure came in court papers filed recently, in which prosecutors urged a federal judge to continue the pretrial detention of Stewart D. Nozette, 52, who was arrested in October on charges of selling classified information to an undercover FBI agent who was posing as an Israeli intelligence operative.

Nozette worked as a contractor for NASA and the Defense Department from 2000 to 2006, and had held other sensitive government jobs over the years. Prosecutors said he "posed a grave risk to the national security" and is a flight risk.

Clandestine meetings

In the weeks leading up to his arrest, Nozette met twice with the FBI agent and exchanged sensitive information for $11,000 that was sent to a post office box.

In a separate case, Nozette last year pleaded guilty to overbilling the U.S. government by about $265,000 and faced at least two years in prison. The case was sealed because Nozette was cooperating with authorities investigating unrelated corruption charges.

He had told a colleague that he planned to flee to India or Israel if the government sought to put him in jail for fraud. He told the coworker he planned to share everything he knew with officials of those governments, authorities have said.

That colleague told federal authorities about Nozette's statements. By September, federal agents had launched their undercover sting.

On the day he was arrested, Nozette met with the undercover agent at a Washington, D.C., hotel.

During that meeting, which took place after the post office box exchanges, Nozette told the agent he had "crossed the Rubicon" in terms of sharing sensitive data and that he wanted $2 million for the secrets.

He told the agent that his wife didn't need an Israeli passport or help relocating to Israel because "she would ask too many questions," according to court papers.

According to prosecutors, Nozette also told the agent he had hidden classified information in safe deposit boxes in addition to the gold coins.

Clearance Reciprocity

A bill recently introduced in Congress directs agencies to make sure approved security clearances for federal employees and contractors apply governmentwide.

The legislation, sponsored by Sens. Daniel Akaka (D-Hawaii) and George Voinovich (R-Ohio), amends the portion of the 2004 Intelligence Reform and Terrorism Prevention Act that deals with the security clearance process. It mandates the creation of a performance accountability council to oversee the reduction of the government's security clearance backlog and extends reporting requirements.

A provision in the bill would direct agencies to adhere to "reciprocal recognition of clearances that allow access to classified information granted by all other agencies and departments." Many federal agencies use their own clearance standards and don't necessarily accept background checks performed by other agencies. The intelligence reform law also includes a provision related to reciprocal recognition of security clearances.

SECURITYbriefs

Top 10 Scams and Ripoffs of 2009

Here, courtesy of the Better Business Bureau, are the best (worst?) cons of 2009:

H1N1 scams. Consumers were flooded with efforts to scare them into purchasing cures for, or info about, the Swine Flu.

Memorabilia. With the election of President Obama and the death of Michael Jackson, 2009 provided great opportunities for scammers to sell collectibles – at inflated prices.

Weight loss pills. Ads offering trial offers for nonsensical weight loss pills were everywhere.

Phishing. The scam in which fraudsters try to lure people to a counterfeit replica of their bank's Web site, for example, and have them part with their user names and passwords.

Mystery shopping. Consumers were especially vulnerable to "secret shopper" job offers. In some scams, victims were asked to send money in order to "evaluate" money-wiring services.

Lottery scams. Victims received letters in the mail informing them they'd won millions of dollars. The only catch was that they needed to wire hundreds of dollars back to cover taxes or other fees.

Friend or family in distress. Victims receive a message allegedly from a loved one claiming they are outside of the country and have gotten into trouble. Recipients are asked to wire thousands to pay for legal and travel fees.

Mortgage foreclosure rescue/debt assistance. With many families struggling to save their homes from foreclosure or escape credit card debt, scammers were quick to offer "help." Victims paid hundreds of dollars for assistance they never received.

Job hunter scams. Con men had a large pool of unemployed victims to prey on. One scam required job seekers to pay a fee in order to be considered for a job.

Robocalls. Thousands of people received automated telephone calls. The robocalls often claimed that the consumer's auto warranty was about to expire.

Facebook Spoofed

Security firms are warning of a new spoofed Facebook page that makes a clever attempt to steal users' passwords and other login details.

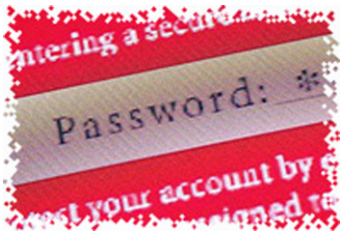
Users of the social networking site are urged to watch out for rogue emails containing links to the bogus page, which can give attackers access to their account if they enter their login details.

Once cyber-crooks have the user's information, they can take any action from the account, including publishing spam comments with malicious links and sending out fraudulent messages.

5 Tips to Create Strong Passwords

1. Use tools that generate random passwords. This way, even if your password becomes compromised, it will only be vulnerable until the randomization expires.

2. A blend of upper- and lowercase letters, numbers, and symbols will make your password tough to crack.



3. Instead of mnemonics, try a "pass-phrase." Researchers have found out that using mnemonics (which require users to generate a password using the first letter of every word in a sentence) is not as secure as initially thought. Far more secure are pass-phrases such as "du-bi-du-bi-dub", which would withstand virtually any brute force attack.

4. Frequent password changes make it more difficult for intruders to access company data using outdated passwords.

5. Avoid personal information. Pet names, birth dates, and favorite sports teams or alma maters are all easily cracked.

Did You Know That. . .

… Los Alamos National Laboratory is failing to adequately protect its classified network, leaving the overseer of the nation's nuclear stockpile vulnerable to attack. That's the gist of a new report from the Government Accountability Office, which found that security controls and policies aren't fully implemented or consistently applied at Los Alamos.

… Secrets leaked by a congressional staffer over a peer-to-peer network name more than 30 lawmakers who are under investigation by the House Ethics Committee. The employee, who was fired in the wake of the gaffe, is said to have inadvertently placed the sensitive information in a file-sharing folder on her home computer.

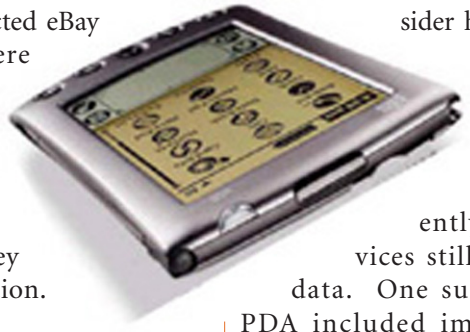
… Office theft is on the rise, in part because security has been beefed up around such traditional theft targets as banks and convenience stores. Law-enforcement officials say more and more robbers are walking into business offices, especially those of small companies with minimal security, and committing holdups or even taking hostages.

Use Caution when Selling that PDA

Looking to make a few bucks selling your outmoded cell phone or PDA? Think again!

In a recent study, nearly 25% of the pre-owned PDAs purchased by researchers on eBay still held highly sensitive corporate data and embarrassing personal information about their previous owners.

Members of a cellular forensics team randomly selected eBay merchants that were selling second-hand Blackberries and Palm PDAs, then purchased a total of 100 such devices. And oh boy, did they find some information.



Recovered data included the following, ranging from the just plain embarrassing to information that could render a company vulnerable to a serious breach:

Website passwords.

Login information for financial and ecommerce sites that regularly save credit card information and other personal identifiers. An insurance company's client lists, including private account numbers and loan applications.

Additionally, email messages were still accessible on several of the PDAs. Moreover, some of these messages included the names, phone numbers, and titles of professional contacts as well as detailed business information that most companies would consider highly confidential.

The forensics research team even noted instances in which apparently inoperable devices still held retrievable data. One such defunct Palm PDA included images containing full frontal nudity taken in a mirror.

Due to studies like this one, experts strongly advise consumers to exercise caution when selling or donating used PDAs. Consumers should assume that their privacy and reputation will not be a priority to the recipient of any of these second-hand devices.

Study: 30% of Teens Report Sexting

A new study from the Associated Press and MTV finds that 50% of 14- to 24-year-olds have experienced some type of digital abuse. The study also says 30% have either sent or received nude photos on their cell phones or online, a practice that's been dubbed "sexting."

Females are slightly more likely to share a naked photo of themselves (13%) than males (9%), while youths who are sexually active are more than twice as likely to send such photos (17% vs. 8%).

Perhaps more disturbing is the finding that 17% passed the image to someone else, and 9% distributed the images to more than one person.

Indeed, 29% of respondents who shared a naked photo of themselves report that they shared the image with someone who they never met in person and only knew online.

The study also says that 61% of those who sent a naked photo or video of themselves have been pressured by someone else to do so at least once.

10 Ways to Work More Securely in 2010

Protecting government and corporate secrets from the prying eyes of hackers, spies, and information thieves is not going to get any easier in 2010.

But forewarned is forearmed, so here we present the 10 most common security land mines that experts say you need to avoid.

Employees taking sensitive information from the office to work at home. Sure, you mean well; you just want to take a folder home to clear your workload. Or maybe you think it'll do no harm to pop some files onto a memory stick so you can address them over the weekend. But this is how data breaches happen! In 2010, obey your employer's guidelines on these practices.

Failure to recognize and report adverse information about a co-worker. Nobody wants to think the worst about a colleague, but the unfortunate fact is that people in trouble – whether it's marriage or money woes, alcohol abuse, etc. – are security risks. Bringing erratic behavior to the attention of Security/HR will do the company and the colleague a favor.

Processing classified data on unapproved computer systems. Using your own laptop or PDA to work on sensitive information is a disaster waiting to happen. Remember, even after you hit the Delete key, data remains on a computer, easily accessible to attackers. Learn and follow your organization's rules regarding computer use.

Employee reluctance to challenge unescorted strangers in restricted areas. Social engineers are adept at "tailgating" their way into restricted areas in order to spy. It is your responsibility to politely confront anybody who lacks the proper access credentials.

Business travelers not reporting suspicious contacts or foreign travel. If you work with sensitive or classified data and neglect to report overseas travel, you may find yourself in hot water. And when attending industry conferences or academic presentations, be aware that spies use these get-togethers for recruitment and to learn secrets. In 2010, keep your guard up.

Employees falling for social engineering ploys for sensitive data. The practice of "tailgating," is just one social-engineering ploy. These human-hackers frequently pose as headhunters or company IT workers, and know a million tricks to persuade workers to part with such information as passwords, product plans, and sales lists. Always report suspicious incidents to your manager and your organization's security personnel.

Employees hosting onsite visits from foreign nationals without security's knowledge. This is an inexcusable practice. Many spies, whether representing an unfriendly nation or a competitor, may request an innocent-seeming site visit, allegedly merely to gather information. While such visits may indeed prove innocent, this year you should be sure to report them to your company in advance for approval.

Cleared workers' failure to recognize potential approaches from foreign spy services. The spy who approaches you won't be a shifty-eyed Boris Badenov; he or she is likely to be personable and sympathetic – perhaps even a trusted colleague. Don't get drawn into seemingly casual conversations in which you divulge sensitive information, and report all such approaches to your Security Dept.

Improper handling and disposal of classified or sensitive data. This year, resolve to be more conscientious about sensitive information in all its forms. Documents should never be left atop an unattended desk, or in a shared printer. Carefully follow all rules regarding what physical documents may be removed from the workplace. And use that shredder!

Workers bringing unauthorized portable devices to work and opening the network to hackers, spies, and data thieves. USB drives, iPods, and personal cell phones may seem innocent, but when connected to the company network they can be used to download sensitive data. Just as importantly, they may introduce malware to the company network when plugged into a business computer. Employers take many steps to keep the network secure, but one screensaver or game uploaded from a memory stick may undo all that work.

2009 Espionage Hall of Shame

The U.S. has become Ground Zero for foreign espionage and theft of trade secrets. That's no secret, but when you rack up an entire year's worth of U.S. data breaches, the scale and intensity of the problem becomes clear.

Many of the spy cases discussed here are the latest evidence of what U.S. officials call an intense effort by the Chinese government to steal government and industrial secrets. With that as a backdrop, here's a roundup of lowlights from the past year.

Gold for secrets

Stewart D. Nozette, a 52-year-old scientist, was charged with attempted espionage after allegedly demanding $2 million for secrets and stashing 55 gold Krugerrand coins in a safe deposit box. Nozette was arrested in October on charges of selling classified information to an undercover FBI agent who was posing as an Israeli intelligence operative. He was a contractor for NASA and the Defense Department from 2000 to 2006, and prosecutors said he "posed a grave risk to the national security."

Delaware to China

The DuPont Co. fired and filed a lawsuit against a Chinese-born employee who was allegedly about to leave the company's Delaware headquarters and return to China with trade secrets. The incident marked the second time in two years that a DuPont researcher with ties to China was accused of stealing trade secrets. The suit accused Hong Meng of breach of contract and misappropriation of trade secrets – specifically, research into a paper-thin computer display technology. Meng allegedly planned to take the proprietary information to his alma mater, Peking University in Beijing.

Boeing, Boeing, gone

A Chinese-born former Boeing engineer who became a U.S. citizen was convicted of spying for China for decades, stealing technology and trade secrets – including data on NASA's space shuttle program. Dongfan Chung, 73, was found guilty of economic espionage and acquiring information on demand using his Secret-level security clearance. The former employee of Rockwell International's space and defense unit (taken over by Boeing in 1996) stole and passed along to China trade secrets related to the space shuttle and the Delta IV rocket programs.

Cuban connection

Thirty years of spying for Cuba sent a retired State Department official to prison for life after he and his wife pleaded guilty to sending secrets to the Communist nation. Walter Kendall Myers, 72, agreed to a life sentence without parole and to cooperate with the federal government in a deal with prosecutors that offered a much lighter sentence for his wife. Gwendolyn Steingraber Myers, 71, had faced up to 20 years in prison. The couple were said to be ideologically motivated, and in fact it was Cuba that urged Myers to seek a State Department job in the first place.

DoD spy

A federal jury convicted a U.S. Department of Defense official of providing classified information to a man working with the People's Republic of China, then lying to the FBI about it. James Wilbur Fondren, Jr., 62, was convicted of unlawfully communicating classified information to an agent of a foreign government and two counts of making false statements to the FBI. Fondren worked at the Pentagon, serving several years as Deputy Director, Washington Liaison Office, U.S. Pacific Command (PACOM). He held a Top Secret security clearance. From 2004 to 2008, he provided DoD documents and other information to Tai Shen Kuo, a naturalized U.S. citizen from Taiwan.

Rocket science gone wrong

A Virginia scientist who sold U.S. rocket technology to China and bribed Chinese officials to obtain a lucrative contract for his company was sentenced to more than four years in federal prison. Quan-Sheng Shu, 68, pleaded guilty to two counts of violating the federal Arms Control Act and one count of bribery and was sentenced to 51 months on each count, to be served concurrently. Prosecutors said the information and equipment Shu sold to China put U.S. national security at risk. That information could have enhanced China's military or intelligence capabilities.

Ex-FBI Linguist

A former FBI contract employee pleaded guilty to giving classified documents to an Internet blogger who then published them, the U.S. Justice Department said. Shamai Kedem Leibowitz, of Silver Spring, Md., pleaded guilty in federal court to a charge of disclosing five FBI documents classified as "Secret" about U.S. communication intelligence activities. Under a plea deal, Leibowitz is expected to serve a prison term of one year and eight months.

Report: Spies Targeting Mobile Technologies

Economic spies are targeting Blackberries and iPhones in a bid to steal trade secrets. Careless downloading by users opens the door to attack.

According to the latest annual report from the Office of the National Counterintelligence Executive, cyber threats are increasingly pervasive and are rapidly becoming a priority means of obtaining economic and technical information. Reports of new cyber attacks against U.S. government and business entities proliferated in 2008.

According to analysts, there are several reasons mobile devices are now prime targets for spies. For starters, the devices are now more powerful than ever, capable of storing enormous quantities of sensitive business data.

The other appeal is that phones and PDAs are notoriously insecure in virtually every way. They rely on easily intercepted wireless transmission, few users password-protect them, and of course they are easily lost or stolen.

Mobile risks

The report, recently made public, says that the targeting of mobile telephones increased last year, specifically where Blackberries and iPhones are concerned. These devices, "essentially general-purpose computers, are susceptible to malicious software," the report states.

In one alarming case, a visiting U.S. security specialist had his handheld penetrated by electronic code as he rode from Beijing's international airport to his hotel.

Chinese economic espionage is mentioned frequently in the report, with one of the most damaging cases involving a researcher at the University of Tennessee who supplied China with Air Force technology on the development of advanced controllers used on munitions-carrying unmanned aerial vehicles. A federal jury in Knoxville convicted professor J. Reece Roth of the crime in September 2008.

Economic spies are seeking both classified and unclassified technology and secrets from the U.S. government and private sector, the report states, including such targets as dual-use, export-controlled and military items.

The most heavily targeted sectors across all agencies include aeronautics, information systems, lasers and optics, sensors, and marine systems, experts say.

According to information compiled during the reporting period, businessmen, scientists, engineers, and academics – as well as state security services from a large number of countries – continue to target U.S. information and technology.

Need to Know

A recent security incident underscores the importance of an often-overlooked aspect of information security: the need-to-know principal.

Brian Keith Montgomery, an analyst assigned to the National Geospatial-Intelligence Agency (NGA), has been charged with unauthorized access to classified computer information.

According to court documents, Montgomery gained access to a classified computer system used for an undisclosed terrorism investigation to which he was not authorized access. He allegedly did this using a password he'd been authorized for another, unrelated system. Montgomery ignored warning messages that his access was not authorized.

Such actions violated the need-to-know principal of classified information protection: even if an individual has the appropriate security clearance, access to information is denied unless the individual has a need to know for her or his official duties.

Initially charged with a felony, Montgomery pleaded guilty to a lesser charge of exceeding his authorized access. The misdemeanor carries up to a year in prison.

The Employee Security Connection (ISSN 0894-2080) is published quarterly by the National Security Institute, 116 Main Street, Suite 200, Medway, MA 02053. Subscriptions are $899 per year, telephone (508) 533-9099 for information concerning company/agency subscriptions.

January – March 2010