Tampa CI Strategic Partnership Newsletter

January 1, 2011
Volume 3 Issue 1

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

INSIDE THIS ISSUE:

COUNTERINTELLIGENCE (CI) TRENDS

TEN TIPS FOR 2011

Welcome to 2011. To help you, your staff and your employees face the challenges of a new year we submit ten tips designed to enhance your overall security posture.

1. **Security Awareness Training**. Keep your staff and employees informed. Remind them of what must be protected. Don't forget to remind them that not only classified information merits protection. Define what you consider to be proprietary information, and trade secrets, and remind ALL employees why that information must be protected.

   Folks love to hear what we call "war stories", in other words, actual examples of how and why security lapses have occurred at other companies or government locations. This newsletter contains many examples. Disseminate some of these examples as learning points.

   The Defense Security Service and the FBI are available to visit your companies and provide presentations to your employees to help enhance your security education. Don't hesitate to ask. Information regarding FBI presentations is contained at the end of this newsletter.

2. **Computer – SPAM.** Many companies have SPAM filters built into their corporate networks. These filters, when successful, prevent the vast majority of SPAM emails from getting through the corporate firewall.

   However, there are times when SPAM can be a tripwire, an indicator of a probe of your corporate network for potential vulnerabilities for exploitation by intruders.

   One possible indicator, especially for newer companies or small companies, is a surge of SPAM emails, far exceeding the daily norm. These surges most likely would come when a small company, a new company, has a great success or a new product, or signs a major contract. We are talking about an event that is newsworthy, that has generated a press release from the company, something that has put it on the radar scope that could cause an intelligence service to take notice.

From a security perspective, it would be useful for the Information Technology (IT) personnel of your company to be aware when there is publicity regarding the company, and to simultaneously monitor the volume of SPAM being sent to the company. If a significant surge is noted, it would be prudent to check your system for potential vulnerabilities or exploits. If a surge is noted, a Suspicious Contact Report (SCR) submission to DSS would be appropriate. Also, if you have suspicions or concerns, don't hesitate to contact the FBI.

3. **Computer – Access and use of External Devices.** Many of the recent convictions for Economic Espionage or Theft of Trade Secrets cases involved individuals who had downloaded excessive amounts of information from their companies. One individual downloaded over 44 gigabytes of information onto an external storage device. Another individual had downloaded ten times as much data as the next nearest employee. The use of thumb drives to steal trade secrets was a frequent common denominator in many of these cases.

   Many IT departments log downloads, or monitor the connection of external devices to their systems. In many or even most of these cases, this information is only logged, and is never reviewed. If the possibility exists, an IT Department could consider setting tripwires, based on the amount of data being downloaded, or the connection of external devices (especially if against corporate policy, or perhaps based on the time of day, or day of the week connected if after hours or on a non work day) or perhaps based on some other anomaly. When the tripwire is set off, a silent warning could be sent to the IT and Security Departments for examination in greater detail.

   Closer scrutiny in the examples above could have prevented two now convicted felons from stealing hundreds of millions of dollars worth of proprietary information from their employers.

4. **Foreign Travel.** One of the more frequent tripwires for Espionage, Economic Espionage and Theft of Trade Secret cases is foreign travel. Many companies no longer keep records or are aware of the foreign travel of their employees. In many cases there is no requirement by DSS to report foreign travel or keep records of this information.

   If not prohibited by policy, FSO's could consider requiring employees traveling overseas to report this information to security prior to travel. Pre-travel security briefings can be given followed up with post travel security debriefings. Depending on the purpose of the travel, and the

destinations to be visited, more tailored or specific travel briefings and debriefings could be given.

Information about suspicious contacts derived from these debriefings should be submitted to DSS as SCR's.

Companies in need of information to provide to business travelers can obtain handouts from the FBI.

5. **SCR's and Suspicious Activity – Report it!**

Paragraph 1-301 of the NISPOM requires contractors(1)to promptly report to the Federal Bureau of Investigation (FBI) (with a copy to DSS(2)) information coming to the contractor's attention concerning "actual, probable or possible espionage, sabotage, terrorism, or subversive activities" at any of the contractor's locations.

The affirmative requirement for contractors to report these activities has been stated in the NISPOM since the first NISPOM was issued in 1995. The NISPOM imposes this reporting obligation because the hostile acts listed in NISPOM 1-301 are, by their nature, so serious that when they are directed against any of a contractor's locations, they can pose a threat to classified information and to the security of the entire contractor. The specific form of the activity has no bearing on the basic requirement to report.

Certain cyber intrusions (3) will fall under the reporting requirement of NISPOM 301, regardless of the classification level of information contained on the affected system. Specifically, cyber intrusions that indicate actual, probable or possible espionage, sabotage, terrorism, or subversive activities against information systems (IS) maintained by contractors must be reported to the FBI, with a copy to DSS, regardless of whether the IS processes classified or unclassified information.

Cyber intrusions are often targeted against specific information or technologies; however, the target cannot always be easily identified at the time the intrusions take place. It may be unclear that the intrusions are intended to lead to espionage, sabotage, terrorism, or subversive activities when the initial intrusions concern systems processing only unclassified information. Data gleaned from intrusions of systems containing unclassified information can include the identity of systems administrators, personal identifying information of employees that may provide indicators of exploitable issues (e.g., financial problems, drug use, etc.), or system vulnerabilities. This data can then be used

advantageously for nefarious reasons and to focus more specific technical and non-technical exploitation techniques. These intrusions may signal an increased level of security risk to the contractor, the classified Government programs it supports, the information it holds, and the contractor's employees.

A cyber intrusion reportable under NISPOM 1-301 may involve one or more of a combination of active efforts, such as: port and services scanning from consistent or constant addresses, hacking into the system, placing malware hacking tools into the system, or passive efforts (e.g., unsolicited emails containing malware or internet sites that entice users to download files that contain embedded malware). Reportable cyber intrusions may include exploitation of knowledgeable persons through "phishing" and "social engineering" that occur in or out of phase with the application of the malware.

Contractors should consider the following guidelines when making a determination to report a cyber intrusion to the FBI and to DSS under NISPOM paragraph 1-301:

• Evidence of an advanced persistent threat;
• Evidence of unauthorized exfiltration or manipulation of information;
• Evidence of preparation of contractor systems or networks for future unauthorized exploitation;
• Activity that appears to be out of the ordinary, representing more than nuisance incidents; and
• Activities, anomalies, or intrusions that are suspicious and cannot be easily explained as innocent.

Contractors are also reminded they are required by NISPOM paragraph 1-302b, to report to DSS efforts by any individual, regardless of nationality, to "obtain illegal or unauthorized" access to IS processing classified information. Additionally, under NISPOM paragraph 1-302j, contractors must report "significant vulnerabilities" identified in IS "hardware and software used to protect classified material."

1 As defined by the NISPOM, a "contractor" is any industrial, educational, commercial or other entity that has been granted a facility clearance.

2 Some contractors have executed a Framework Agreement under the DIB Cyber Security/Information Assurance Program to submit such reports to the Defense Cyber Crime Center (DC3). These contractors may satisfy the requirement to provide a copy of NISPOM 1-301 reports to DSS by submitting a copy of their report to DC3. DSS

analysts at DC3 will determine if the report meets the threshold for reporting per the terms of this ISL. If a report meets the threshold, the analysts will forward to DSS for appropriate action.

3 An intrusion, as defined in the National Information Assurance Glossary, Committee on National Security Systems Instruction No. 4009, is the unauthorized act of bypassing the security mechanisms of a system.

6. **Don't be Afraid to Contact DSS or the FBI.** For one thing, as discussed in tip number five above, you are required to contact the FBI and DSS, under the NISPOM, when you have suspicious contacts or activities that could represent possible espionage, sabotage, terrorism, or subversive activities" at any of your locations. This also includes possible cyber intrusions.

   This reporting is not only required, but it can help to mitigate or prevent the loss of classified and proprietary information. It shows customers of the company's dedicated efforts to protect the customer, it's willingness to follow the NISPOM.

   When you contact the FBI, don't expect a mass presence of raid jacketed FBI Agents obnoxiously taking over your facilities, rooting around every nook and cranny of your facilities until they uncover a spy or terrorist. It is not in anyone's interest to be indiscrete or highly visible.

   Rather, expect a low key, low visibility approach, with limited individuals being contacted. The FBI does not want to disrupt the operations of your company. Working closely with appropriate individuals at a company, investigators can determine whether the basis for an investigation even exists. Then, if it is determined that more robust investigation is merited, investigative techniques can be quietly put into place to ascertain facts and provide evidence of wrong doing.

   Two examples, the Chi Mak investigation at L-3 Power Paragon and the Greg Chung investigation at Boeing were both worked with discretion, and with the full cooperation of the respective companies. Both cases represented successful investigations and prosecutions resulting in convictions. The respective companies were lauded for their cooperation. The companies' bottom lines were not negatively impacted.

7. **Know what you consider to be proprietary information or trade secrets, and protect them.** As defined by the Economic Espionage Act of 1996, the term 'trade secret' means all forms and types of financial,

business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

What represents "reasonable measures" to protect your trade secrets and proprietary information?

1. Recognize there is an insider and outsider threat to your company.
2. Identify and valuate trade secrets.
3. Implement a proactive plan for safeguarding trade secrets.
4. Secure physical and electronic versions of your trade secrets.
5. Confine intellectual knowledge on a "need-to-know" basis.
6. Provide training to employees about your company's intellectual property plan and security.

Some ways to do this include:

- Marking trade secrets and proprietary information.
- Ensuring employees are admonished as to what you allow in regards to the use, storage, retention and transportation of trade secrets and proprietary information.
- Ensure all employees are required to return all trade secrets and proprietary information they possess, in any form, to the company before leaving employment. Make certain they sign a statement affirming that they retain no proprietary information or trade secrets.
- If possible, run a computer audit for excessive downloads or connections of external storage devices prior to an employee's departure from the company.
- If suspicions exist, report this information to the FBI.

8. **Partnerships with the FBI – InfraGard; Strategic Partnership Program; FBI Business Alliance; FBI Academic Alliance.** Many recipients of this newsletter are members of InfraGard. We encourage you to spread the word to your key IT professionals, especially those charged with network security and protection of the network against intrusions. Their membership in InfraGard can tip them off to potential threats or vulnerabilities before they impact your company. Membership in InfraGard places them in a position to communicate with other IT professionals, discussing issues, concerns, or threats with their peers.

At the executive level, many of the companies receiving this newsletter are represented on the FBI's Business Alliance. Through the Business Alliance, we are building relationships with cleared defense contractors to enhance their understanding of the threat posed to their programs and personnel by foreign intelligence services and foreign competitors. This dialogue results in an increase in the quality and quantity of counterintelligence-related information shared with the FBI by these contractors, resulting in the disruption of foreign intelligence activities targeting their work.

Through the delivery of counterintelligence education and the sharing of actionable intelligence, we enable business partners to identify counterintelligence vulnerabilities within their organizations.

Counterintelligence awareness can result in modifications to their internal behaviors and processes that decrease susceptibility to theft of intellectual property. The protection of our Business Alliance partners' intellectual property results in tangible benefits to our national security.

If your company is a member of our Business Alliance, we suggest you inquire through your internal channels how this membership is being implemented within your company, and how information from this partnership is channeled to you and your employees to better enhance your security posture locally. Please contact us if you don't know if your company is a member of the FBI's Business Alliance.

The Academic Alliance is a national outreach effort charged with sharing information and establishing a dialogue with academic institutions to increase awareness of threat and national security issues in order to foster a spirit of cooperation.

The Academic Alliance has two distinct outreach components:

1) The National Security Higher Education Advisory Board (NSHEAB) includes presidents/chancellors from our nation's top public and private research institutions. The board, which meets regularly, provides a forum for FBI leadership and academia to discuss national security issues of mutual concern. The NSHEAB also facilitates dialogue between government security officials and educational policy makers. The board provides the FBI with perspectives on the culture of higher education-including its traditions of openness, academic freedom, and international collaboration.

2) The College and University Security Effort (CAUSE). Through CAUSE, FBI Special Agents in Charge meet with the heads of local colleges and universities to discuss national security issues and share information and ideas. Topics covered include briefings on national security threats that these research institutions may be facing. We enable counterintelligence protection by explaining how and why some foreign entities may be attempting to steal research and intellectual property.

One thing we would like to encourage, and in fact stress, is that the FBI considers itself in partnership with the Cleared Defense Contractors (CDCs) we work with. Through this newsletter, through our presentations, seminars and briefings, and through our Business Alliance, we are pushing information to the CDC's. In order to protect against the threat of espionage, economic espionage, and the theft of trade secrets, we strongly encourage the CDCs to push information out to the FBI.

Don't wait for a call or a visit, or a chance meeting at a presentation or seminar. If you have information you think might be of use to the FBI, please call your Strategic Partnership Program representatives, listed at the end of this newsletter. If you have agents you work with on a frequent basis, call them. Call the FBI complaint desk if you cannot reach anyone else, but let's make this a two way street. A problem noticed by one CDC can be mirrored throughout the entire CDC community. Early reporting can mitigate or stop problems.

9. **Advanced Persistent Threat.** Though not a definitive source, I think we can all agree that this definition of Advanced Persistent Threat (APT), found at Wikipedia is an accurate definition of the APT threat faced by CDC's on a continual basis:

The "Advanced Persistent Threat" (APT) refers to advanced and normally clandestine means to gain continual, persistent intelligence on an individual, or group of individuals such as a foreign nation state government. While the APT is more commonly thought of as being an

article of the computer era, it has existed since the realization of the benefits of intelligence gathering and long before the invention of the computer or internet.

In the computer security community, it is used to specifically refer to a sub-set of such threats, in a long-term pattern of targeted sophisticated hacking attacks aimed at governments, companies and political activists, and by extension, also to refer to the groups behind these attacks. A common misconception associated with the APT relates to its specificity to the targeting of Western governments. While examples of technological APT's against Western governments may be more publicized, this is incorrect, and the technological ('cyber') APT has been used by actors in many nations as a means to gather intelligence on individuals, and groups of individuals of interest.

Some of the groups involved in the APT have been alleged by numerous sources to be affiliated with, or agents of, nation-states.

Definitions of precisely what an APT is can vary, but can be summarized by their named requirements below:

Advanced – Operators behind the threat utilize the full spectrum of intelligence gathering techniques. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence gathering techniques such as telephone interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available DIY (Do It Yourself) construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

Persistent – Operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful.

Threat – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The

operators have a specific objective and are skilled, motivated, organized and well funded.

The following article, found at http://www.businessweek.com/print/technology/content/jul2009/tc20090 76_873512.htm is illustratrative of the threat faced by CDCs.

Under Cyberthreat: Defense Contractors

Northrop Grumman's info security chief addresses the "well-resourced, highly sophisticated" attacks against makers of high-tech weaponry Tim McKnight is well acquainted with threats to cybersecurity. A former special agent with the FBI, he specialized in corporate espionage and foreign counterintelligence. He's also handled information security for Cisco Systems (CSCO) and BAE Systems and has participated in a group called the Transglobal Secure Collaboration Program, whose mission is protecting intellectual property in the aerospace industry.

Those security chops are tested daily in McKnight's role as chief information security officer at Northrop Grumman (NOC). The defense industry faces "a near-existential threat from state-sponsored foreign intelligence services" that target sensitive IP, according to a report by the Internet Security Alliance, a nonprofit organization on whose board McKnight sits.

Northrop Grumman experienced the implications of that threat firsthand recently. According to a Frontline investigation that aired June 23, reporters were able to purchase an unencrypted hard drive of a Northrop Grumman employee in Ghana for $40. The drive reportedly contained hundreds of documents about government contracts.

"Detailed Asset-Disposal Procedure"

McKnight recently spoke with BusinessWeek.com writer Rachael King. A Northrop Grumman PR representative wouldn't let McKnight address the issues raised by Frontline, instead issuing a statement that said: "We believe this hard drive may have been stolen after one of our asset-disposal vendors took possession of the unit. …We have a detailed asset-disposal procedure in place. Despite sophisticated safeguards, no

company can inoculate itself completely against crime. The fact that this information is outside our control is disconcerting." But McKnight was able to discuss other threats facing his industry. Edited excerpts follow.

Are defense contractors being singled out in highly targeted attacks?

It's gotten to a point where it has a name for itself: the APT or "advanced persistent threat," meaning that they are well resourced, highly sophisticated, clearly targeting companies or information, and they're not giving up in that mission.

Where is this coming from? Is it state-sponsored or organized crime?

Attribution is probably one of the biggest problems for our nation, both from a defensive and an offensive posture as a country. Obviously we know that the likes of China and Russia have the greatest capabilities, like the U.S., from an espionage perspective. But we are starting to see quite a capability in the organized crime, criminal aspect. Clearly you're seeing this with a lot of the credit-card or financially motivated crimes that are occurring.

I've heard that phishing attacks against executives are getting more sophisticated. Do you see evidence of that?

The [phishing e-mails] look more and more authentic in the last couple years. There's definitely targeting of either executives in corporations or in government or specific roles in organizations. We see targeting of our contracts people because they have a lot of knowledge of the marketplace, what's out there, what are our big opportunities and what we're going after, whether that's from a competitive intelligence perspective or a nation-state perspective. We have a special training program just for our executives and their admins.

We had recently done a test within our organization where we did a spear phishing on our management to ascertain how knowledgeable they are. It was pretty common that 65% to 70% didn't click it, reported it, deleted it, handled it in the appropriate way. But we still had that good 30% that clicked on the link and went to the bad Web page where we said, "This was a test and unfortunately you failed." …Social engineering and the use

of e-mail will continue to be a systemic problem for all network defenders and security folk going forward.

What kind of tools do you use to keep your network secure?

We've focused a lot on…capabilities where you're capturing all traffic, not just bits and pieces of it. With the sheer number of viruses and malcode that's out there, most antivirus [software] is probably only hitting about 60% of what's out there at this point. We're moving toward more behavioral-based technology, based on what's the normal behavior of the system. Does it normally run its CPU at 80% on a Sunday evening at 11:55 p.m.? Does it usually have traffic going outbound with large data sets beyond the normal Web traffic?

Most of the attacks in about the last three to four years have [involved] legitimate credentials. The analogy would be that they had a set of keys to your home and they know the codes to your alarm system at home so they can enter and leave as they please, without leaving a track unless you're looking for things like entering during an abnormal hour of the day when you're at work. Obviously, Northrop is a world-class operation when it comes to both offensive attack and exploitation of networks and defense, which is my area of expertise.

What other trends are you seeing now?

As companies and governments have begun to do a better job of the health care of the security of their networks, the sophistication has gone up. So, the attacks are more "stealthy," more sophisticated. They really become a needle in the haystack as you're trying to find them in a large network.

10. **The risks of using social networking sites.** It is incumbent on security professionals to be aware of the risks associated with social networking sites, and to educate employees regarding these risks.

Many companies use Facebook, Linkedin and other social networks to announce job availabilities, company news, and other public purposes. Each company must weigh the risks of using this new media. It's when individuals start using this media that risks start to multiply. The article

below, found at http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html#ixzz19Rdb73Mz is illustrative of these risks:

The new head of MI6 has been left exposed by a major personal security breach after his wife published intimate photographs and family details on the Facebook website.

Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all Britain's spying operations abroad.

But his wife's entries on the social networking site have exposed potentially compromising details about where they live and work, who their friends are and where they spend their holidays.

Amazingly, she had put virtually no privacy protection on her account, making it visible to any of the site's 200million users who chose to be in the open-access 'London' network - regardless of where in the world they actually were.

There are fears that the hugely embarrassing blunder may have compromised the safety of Sir John's family and friends.

Lady Shelley Sawers' extraordinary lapse exposed the couple's friendships with senior diplomats and well-known actors, including Moir Leslie, who plays a leading character in The Archers. And it revealed that the intelligence chief's brother-in-law - who holidayed with him last month - is an associate of the controversial Right-wing historian David Irving.

Immediately after The Mail on Sunday alerted the Foreign Office to the astonishing misjudgment, all trace of the material – which could potentially be useful to hostile foreign powers or terrorists - was removed from the internet.

The move suggests that MI6 or the Foreign Office, which is also responsible for the GCHQ electronic eavesdropping centre in Cheltenham, had not vetted what sort of information Sir John and his family were distributing over the internet.

Though extreme as an example, this clearly shows the risks of social networks affect even the most knowledgeable of intelligence officials, let alone an employee working on a special project. In the example

given here, the vulnerabilities were exposed by the spouse. Sir John Sawers did not himself have a Facebook page. What do the Facebook pages of the spouses and children of your employees state? Jobs, projects, sensitive information? Names, addresses, interests, likes, vulnerabilities of cleared employees? Perhaps it wouldn't be a bad idea as part of your security education program to ask your employees to do a self audit of their public internet presence, and ensure they don't have information out there that might be of use to an adversary.

We hope you have found this list useful. Have a happy and prosperous new year.

ARRESTS, TRIALS AND CONVICTIONS

Former Goldman Sachs Computer Programmer Found Guilty in Manhattan Federal Court of Theft of Trade Secrets

Department of Justice Press Release

For Immediate Release

December 10, 2010 United States Attorney's Office

Southern District of New York

Contact: (212) 637-2600

http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo121010.htm

PREET BHARARA, the United States Attorney for the Southern District of New York, announced that SERGEY ALEYNIKOV was found guilty today by a jury in Manhattan federal court of one count of theft of trade secrets and one count of transportation of stolen property in interstate and foreign commerce, in connection with the theft of proprietary computer code concerning a high-frequency trading platform from his former employer, Goldman Sachs. U.S. District Judge DENISE L. COTE presided over the two-week trial.

Manhattan U.S. Attorney PREET BHARARA said: "As today's guilty verdict demonstrates, we will use the full force of the federal law to prosecute those who steal valuable and proprietary information from their employers, whether those firms are on Wall Street or Main Street. The brazen theft of intellectual property by Sergey Aleynikov had the potential to cause serious harm to the company, and now he will pay for his crimes. We will continue working with our

law enforcement partners to investigate and prosecute corrupt professionals who exploit their access to employer's secrets."

According to the documents previously filed in this case and the evidence introduced at trial :

From May 2007 to June 2009, ALEYNIKOV was employed at Goldman Sachs as a computer programmer responsible for developing computer programs supporting the firm's high-frequency trading on various commodities and equities markets. Goldman Sachs had obtained the high-frequency trading system in 1999, when it acquired Hull Trading Company, the previous owners of the system, for approximately $500 million. Since acquiring the system, Goldman Sachs modified and maintained the system, and took significant measures to protect the confidentiality of the system's computer programs, including firewalls to limit access to the firm's computer network, and limiting internal access to the high-frequency trading program. Goldman Sachs' high frequency trading system generates millions of dollars per year in profits for the firm. Goldman Sachs takes several measures to protect the system's source code, including requiring all Goldman employees to agree to a confidentiality agreement.

In April 2009, ALEYNIKOV resigned from Goldman Sachs and accepted a job at Teza Technologies ("Teza"), a newly-formed company in Chicago, Illinois. He was hired to develop Teza's own version of a computer platform that would allow Teza to engage in high-frequency trading. His last day of employment at Goldman Sachs was June 5, 2009.

Beginning at approximately 5:20 p.m. on June 5, 2009—his last day working at Goldman Sachs—ALEYNIKOV, from his desk at Goldman Sachs, transferred substantial portions of Goldman Sachs' proprietary computer code for its trading platform to an outside computer server in Germany. He encrypted the files and transferred them over the Internet without informing Goldman Sachs. After transferring the files, he deleted the program he used to encrypt the files and deleted his computer's "bash history," which records the most recent commands executed on his computer.

In addition, throughout his employment at Goldman Sachs, ALEYNIKOV transferred thousands of computer code files related to the firm's proprietary trading program from the firm's computers to his home computers, without the knowledge or authorization of Goldman Sachs. He did this by e-mailing the code files from his Goldman Sachs e-mail account to his personal e-mail account, and storing versions of the code files on his home computers, laptop computer, a flash drive, and other storage devices.

On July 2, 2009, ALEYNIKOV flew to Chicago, Illinois, to attend meetings at Teza's offices, bringing with him his laptop computer and another storage device, each of which contained Goldman Sachs's proprietary source code. He was arrested on July 3, 2009, as he arrived at Newark Airport following that visit.

ALEYNIKOV, 40, faces a maximum of 15 years in prison. He is scheduled to be sentenced on March 18, 2011.

Mr. BHARARA praised the investigative work of the FBI in this case.

This case is being handled by the Office's Complex Frauds Unit. Assistant U.S. Attorneys JOSEPH FACCIPONTI and REBECCA ROHR are in charge of the prosecution.

Former Paint Manufacturing Chemist Sentenced to 15 Months in Prison for Stealing Trade Secrets Valued up to $20 Million

Department of Justice Press Release

http://chicago.fbi.gov/dojpressrel/pressrel10/cg120810.htm

For Immediate Release

December 8, 2010 United States Attorney's Office

Northern District of Illinois

Contact: (312) 353-5300

CHICAGO—A former chemist for a northwest suburban paint manufacturing company was sentenced today to 15 months in federal prison for stealing trade secrets involving numerous formulas and other proprietary information valued up to $20 million as he prepared to go to work for an overseas competitor. David Yen Lee, formerly a technical director in Valspar Corp.'s architectural coatings group since 2006, pleaded guilty in September to using his access to Valspar's secure internal computer network to download approximately 160 original batch tickets, or secret formulas for paints and coatings. He also obtained raw materials information, chemical formulas and calculations, sales and cost data, and other internal memoranda, product research, marketing data, and other materials from Valspar's offices in Wheeling.

Lee, 54, formerly of Arlington Heights and currently of Jersey City, N.J., was sentenced by U.S. District Judge Robert Gettleman, who also ordered mandatory

restitution of $30,975 to reimburse Valspar for the costs of its internal investigation. Lee was ordered to begin serving the sentence next year.

Lee admitted that between September 2008 and February 2009, he had negotiated employment with Nippon Paint, located in Shanghai, China. On Feb. 27, 2009, Lee accepted employment with Nippon as vice president of technology and administrator of research and development beginning on April 1, 2009, in Shanghai. Lee was scheduled to fly from Chicago to Shanghai on March 27, 2009. He did not inform Valspar that he had accepted a job at Nippon until he resigned on March 16, 2009.

At Valspar, Lee's duties included scouting new paint technologies, coordinating with other paint laboratories, coordinating staffing and projects with Huarun Limited, a Valspar subsidiary located in China, and overseeing Valspar's technical service group, which conducted experiments for paint coloring.

Between November 2008 and March 2009, Lee downloaded technical documents and materials belonging to Valspar, including the paint formula batch tickets. He further copied certain downloaded files to external thumb drives to store the data, knowing that he intended to use the confidential information belong to Valspar for his own benefit. The total value of the trade secret information Lee took was estimated at between $7 million and $20 million. There was no evidence that he actually disclosed any of the stolen trade secrets.

The sentence was announced by Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois, and Robert D. Grant, Special Agent-in-Charge of the Chicago Office of Federal Bureau of Investigation. The government was represented by Assistant U.S. Attorney Jessica Romero.

Russian 'spy' tried to access details of Britain's nuclear arsenal, say MI5

http://www.telegraph.co.uk/news/worldnews/europe/russia/8182577/Russian-spy-tried-to-access-details-of-Britains-nuclear-arsenal-say-MI5.html

MI5 has been investigating a House of Commons researcher at the centre of a Russian spy scandal for more than six months, it is understood.

By Duncan Gardham, Security Correspondent, and Martin Beckford 9:30PM GMT

05 Dec 2010

Katia Zatuliveter, who works for an MP on the sensitive Defence Select Committee, has been arrested and served with a deportation order on the grounds of national security.

She is accused of using her position to try and gain sensitive material from the Government, after questions were tabled from the office of her employer, Mike Hancock MP, requesting an inventory of Britain's nuclear arsenal and the location of its international submarine bases.

MI5 has been concerned for some time that Miss Zatuliveter, 25, whose father is a well-connected Russian businessman, has had access to confidential documents supplied to the committee.

She had already studied for a master degree at the University of Bradford and was initially cleared to work at the House of Commons but suspicions soon grew within the security services that she was attempting to pass on secret information.

The deportation order is thought to be the culmination of a long investigation into her background and connections that has looked into both her family and social contacts.

It is unclear whether suspicions of links to the Russian SVR – the modern equivalent of the KGB – arose during her trips abroad or in Britain but it is understood that MI5 has spent some time trying to identify her handler in order to amass sufficient evidence to bring a case against her.

Sources told The Daily Telegraph that MI5 had already launched the investigation when Miss Zatuliveter was stopped at Gatwick airport in August on the way back from celebrating her birthday in Croatia with friends.

The Security Service has been concerned about Russian intelligence case officers arriving in Britain under "non-official" cover, using business or academic visits as a pretext for spying or recruiting others to spy.

More than 170,000 Russians visit Britain every year and around 2,000 are enrolled in universities.

Levels of activity are now said to be back to Cold War levels with up to 35 diplomats based in Britain who are working for the Russian intelligence agencies the SVR and the GRU, its military equivalent.

Jonathan Evans, the director general of MI5, has said the Russians "continue to devote considerable time and energy trying to steal our sensitive technology on

civilian and military projects and trying to obtain political and economic intelligence at our expense."

Now demands are being made to tighten up the vetting of Parliamentary staff, while Mr. Hancock is facing questions over his decision to employ Miss Zatuliveter.

His constituency town is home to the Royal Navy while she once wrote a think-tank article that criticized Nato and defended Russian military action.

Among the Parliamentary questions recently put down by Mr. Hancock, who also sits on the All-Party Parliamentary Group on Russia, was one asking the Defence Secretary to publish "a full historical inventory of the UK's nuclear arsenal", another asking for "an update on the quantities of (a) plutonium, (b) enriched uranium and (c) other special nuclear materials that are outside international safeguards" and a series about the future of the Trident submarines.

Yvette Cooper, the shadow foreign secretary, said: "Depending on what happens in this individual case, if there do turn out to be problems and breaches of security here, then obviously the wider security in Parliament would need to be looked at, and I am sure the Speaker would take that very seriously."

When the Defence Select Committee meets later this week, Mr Hancock is likely to be asked to withdraw from its activities - which include scrutinizing the Government's military policy - until the case of his aide has been resolved.

Dai Havard, the Labor vice-chairman of the committee, said: "It raises a whole suspicion. He's now got a problem of trying to demonstrate that whole activity isn't going to taint him, and perhaps one of the best ways is for him to step aside for a while until it's resolved.

"I think inevitably we'll have to ask him what's going on there."
The committee occasionally receives classified briefings behind closed doors and is given and secret papers, but these are locked in a safe and only accessible to members.

"The committee is not damaged by it in the sense that we know the most sensitive information we deal with would have been protected her physically, she would not have been able to see it and he would not have been able to take it to her," said Mr. Havard.

Patrick Mercer, the Tory MP for Newark, said: "I know Mike and have been a colleague of his on the Defence Select Committee. I think it might be wise for

him to move a little bit cautiously over the next few months if he doesn't want questions to be raised over what his motives are for these questions.

"I think the chairman of the committee will no doubt give some very trenchant advice to Mike in light of these anomalies."

Yuri Felshtinsky, a Russian espionage expert, said: "I would consider this to be by definition a security risk. Not because there is no trust, but because any agency responsible for security would consider this to be a risk.

"The basic rule is that a Russian citizen probably should not be an assistant to a member of the British Parliament."

However Mr. Hancock, who is presently on bail over an alleged indecent assault against a female constituent, defended his employee, saying: "I have no reason to believe she did anything but act honorably during the time she was working for me.

"She is determined to fight her corner and she genuinely believes, and I back her 100 per cent, that she has nothing to hide and has done nothing wrong. If she has, the (security) services are right. But they need to prove their point now."

Two Engineers Found Guilty of Stealing Goodyear Trade Secrets

Department of Justice Press Release

http://knoxville.fbi.gov/dojpressrel/pressrel10/kx120910.htm

For Immediate Release

December 9, 2010 U.S. Department of Justice

Office of Public Affairs

(202) 514-2007/TDD (202) 514-1888

WASHINGTON—A federal jury convicted Clark Alan Roberts, 47, and Sean Edward Howley, 39, both former engineers with Wyko Tire Technology Incorporated, located in Greenback, Tenn., of stealing trade secrets from the Goodyear Tire and Rubber Company, Assistant Attorney General Lanny A. Breuer of the Criminal Division and U.S. Attorney William C. Killian for the Eastern District of Tennessee announced today.

After a one-week trial, the jury found Roberts and Howley guilty of one count of conspiracy to commit trade secret theft, one count of trade secret theft, one count of unlawful photographing of trade secrets, three counts of transmittal of trade secrets, one count of possession of trade secrets, two counts of wire fraud, and one count of conspiracy to commit wire fraud.

"Unable to create an effective design on their own, these engineers stole trade secrets from a competitor in order to fulfill a contract," said Assistant Attorney General Breuer. "We will not allow the hard work and resources businesses put into product development to be compromised by individuals who unlawfully obtain protected secrets."

"The ruling in this case will send a message that complicated trade secret violations will be aggressively investigated and prosecuted by U.S. Attorney's Offices and the Department," said U.S. Attorney Killian.

According to the evidence presented in court, Wyko secured a $1.2 million contract in early 2007 with the Haohua South China Guilin Rubber Company Limited (HHSC), a Chinese tire manufacturing company located in Guilin, Peoples Republic of China, to supply tire building equipment for use in producing radial "off the road" (OTR) tires, which are used on very large earth moving and mining equipment. Wyko was in the business of making tire building equipment for Goodyear and other tire manufacturers. One of the pieces of equipment that Wyko agreed to sell to HHSC was called a swab down device, which is used during the manufacture of a giant OTR tire. However, Wyko had never built a swab down device before and was having difficulty in the spring of 2007 completing their design of the swab down device.

On May 30 and 31, 2007, Roberts and Howley, traveled to a Goodyear tire manufacturing facility located in Topeka, Kan., to service Wyko equipment located in the Goodyear plant with the intention of taking photographs of Goodyear's swab down device to assist them with completing their design even though they knew Goodyear protected the swab down device as a trade secret. On May 31, 2007, the defendants used a cell phone camera to surreptitiously take seven unauthorized photographs of a Goodyear swab down device, without the knowledge or permission of Goodyear. The defendants then e-mailed the unauthorized photographs to employees at a Wyko subsidiary located in Dudley, England, who used the trade secret information contained in the photographs to complete a similar piece of tire building equipment for the HHSC contract.
The defendants are scheduled to be sentenced on the 10 felony counts by U.S. District Court Judge Thomas Phillips on April 14, 2011. The defendants face a maximum of 10 years in prison for each trade secret count, 20 years in prison for each wire fraud count, and $2.5 million in fines.

The case was prosecuted by Trial Attorney Thomas S. Dougherty of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney D. Gregory Weddle of the U.S. Attorney's Office for the Eastern District of Tennessee. The case was investigated by the FBI's Knoxville Division.

Ga. Man Sentenced for Stealing Trade Secrets

http://www.myfoxatlanta.com/dpp/news/local_news/Ga.-Man-Sentenced-for-Stealing-Trade-Secrets-20101215-ap-sd

MACON, Ga. (AP) - A Georgia man was sentenced to three years in federal prison after pleading guilty to stealing trade secrets that prosecutors say cost his former company $14 million.

Kevin Crow, 57, was also sentenced this week to three years of supervised release and a $10,000 fine.

Prosecutors say Crow, an engineer for Turbine Engines Components Technologies Corp., took about 100 computer discs containing trade secrets from the firm after he was laid off in June 2007.

They say he contacted the company's employees requesting price sheets and contract reviews after he was hired at a competitor, Precision Components International. They say he also admitted in a conversation that he took the discs, blueprints and other information from his former firm.

Prosecutors say the corporation suffered at least $14 million in losses.

Man charged with stealing secrets from wireless company Sirf

Robert McMillan

November 16, 2010 (IDG News Service)
http://www.computerworld.com/s/article/print/9196878/Man_charged_with_stealing_secrets_from_wireless_company_Sirf?taxonomyName=DRM+and+Legal+Issues&taxonomyId=144

A San Ramon, California, man is facing charges he stole valuable technology from his former employer in hopes of building competitive location-aware products.

Zhiqiang "Michael" Zhang was arrested Tuesday, on charges that he stole trade secrets from Sirf Technology, a San Jose, California, maker of Global Positioning System chipsets, used by wireless location-aware programs in devices such as mobile phones and automobile navigation systems. A noted expert on location aware technology, Zhang had been a director of software development before resigning from Sirf in May 2009. He had been with the company for seven years.

According to prosecutors, Zhang then set up a company called Anywhere Logic "in order to develop and sell location-based services utilizing trade secrets stolen from Sirf."

Zhang allegedly hired two Sirf engineers, Xiaodong Liang and Yanmin Li away from Sirf to work at Anywhere Logic. They have also been charged in the case, but are now living in China.

Zhang was indicted by a grand jury on Nov. 10, but the indictment was sealed until he was arrested. He could face a 10 year sentence if convicted of the charges.

He was released on a US$500,000 bond after making his first court appearance at the U.S. District Court for the Northern District of California in San Jose, Tuesday.

Sirf was acquired by the U.K.'s Cambridge Silicon Radio, a maker of Bluetooth and wireless chipsets, in 2009.

Robert McMillan covers computer security and general technology breaking news for The IDG News Service. Follow Robert on Twitter at @bobmcmillan. Robert's e-mail address is robert_mcmillan@idg.com

Washington Man Charged in Connection with Attempts to Ship Sensitive Military Technology to China

Department of Justice Press Release

http://seattle.fbi.gov/dojpressrel/pressrel10/se120610.htm

For Immediate Release

December 6, 2010 United States Attorney's Office

Western District of Washington
Contact: (206) 553-7970

Man Arrested in FBI Sting Operation After Attempting to Smuggle Parts Out of United States

SEATTLE—A Woodinville, Washington man made an initial appearance in U.S. District Court in Seattle today following his arrest in connection with an attempt to smuggle sensitive military technology to the People's Republic of China.

Lian Yang, 46, came to the attention of the FBI early last year when agents were tipped that Yang was looking for a way to purchase and smuggle certain restricted parts from the United States. Law enforcement agents and a person working with law enforcement posed as possible sources to monitor Yang's efforts. Yang was arrested on Dec. 3, 2010, when he was scheduled to meet with undercover agents to exchange cash for five of the parts he had ordered. Yang is charged by complaint with conspiracy to violate the Arms Export Control Act.

"The Arms Export Control Act is a critical safeguard for our nation. Our national security and economic competitiveness rely on vigorous protection of our sensitive technologies," said U.S. Attorney for the Western District of Washington Jenny A. Durkan. "I commend the FBI and Homeland Security Investigations (HSI) for their work on this case."

According to the complaint unsealed today, Yang attempted to purchase and export 300 radiation-hardened, programmable semiconductor devices that are used in satellites. The parts are export restricted and require export license or approval from the U.S. State Department authorizing the export of these items.

Yang contemplated creating a shell company in the United States that would appear to be purchasing the parts, concealing the fact the parts were to be shipped to China. Yang planned that false purchase orders would be created indicating that parts that could legally be exported were being purchased, not restricted parts. Yang agreed to pay $620,000 to obtain the 300 parts through subterfuge.

According to the complaint, in the early spring and summer of 2010, Yang met with a person working with law enforcement to discuss his desire to purchase the parts and ways to get them. In September and October 2010, there was a series of meetings with undercover agents posing as contacts who could obtain the restricted parts. On multiple occasions Yang and the participants in the meetings discussed legal restrictions on exporting these types of parts. In late July 2010, Yang was detained when he returned from a trip to China and was questioned about some equipment in his luggage. Customs and Border Protection personnel as well as HSI agents reviewed with Yang the laws regarding technology going to China. Yang continued to try to purchase the parts

for export, arranging to wire transfer funds to an account controlled by those he thought would assist him. In fact, the account was set up by the FBI.

The charges contained in the complaint are only allegations. A person is presumed innocent unless and until he or she is proven guilty beyond a reasonable doubt in a court of law.

Conspiracy to violate the Arms Export Control Act is punishable by up to five years in prison.

The case is being investigated by the FBI with assistance from HSI. The case is being prosecuted by Assistant U.S. Attorneys Todd Greenberg and Tom Woods.

California man charged with attempting to export military items to Iran

http://www.ice.gov/news/releases/1012/101216wilmington.htm

WILMINGTON, Del. - David C. Weiss, U.S. attorney for the District of Delaware, John P. Kelleghan, special agent in charge of U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) in Philadelphia, and Edward T. Bradley, special agent in charge, Defense Criminal Investigative Service, Northeast Field Office, announced that Marc Knapp, 35, of Simi Valley, Calif., has been charged in a two-count felony Information with attempting to export controlled technology to Iran and other countries.
The information charges that Knapp engaged in a seven-month course of criminal conduct involving illegal exports to Hungary and attempted exports to the Islamic Republic of Iran and Russia.

The Information charges Knapp with one count of violating the International Emergency Economic Powers Act, Title 50, United States Code, Sections 1702 and 1705(c), and Executive Order 13222, and Title 31, Code of Federal Regulations, Sections 560.204-560.205, and one count of violating the Arms Export Control Act, Title 22, United States Code, Sections 2778(b)(2) and 2778(c), and Title 22, Code of Federal Regulations, Sections 121.1, 123.1, and 127.1.

Knapp faces a maximum statutory sentence of 40 years incarceration, followed by three years supervised release, a $2 million fine, forfeiture, and a $200 mandatory special assessment.

"This case demonstrates the threat to our national security posed by those, like Knapp, who are willing to trade with Iran and attempt to provide that nation with American goods and technology, particularly military components," said U.S. Attorney Weiss. "I applaud our law enforcement partners for their exceptional dedication in pursuing this major investigation. I would like to thank the government of Hungary and particularly the National Customs and Tax Bureau for their invaluable assistance."

"Homeland Security Investigations will continue to pursue those who are willing to put America's national security at risk," said Special Agent in Charge Kelleghan. "The export of technology to Iran is prohibited so that our innovations cannot be used to harm Americans or our allies. Enforcing export laws is one of HSI's top priorities and we will continue to work with our partners to ensure that sensitive military technology does not end up in the wrong hands. As shown here today, those who choose to violate these laws will be held accountable."

"The Defense Criminal Investigative Service remains vigilant for offenders both within and outside our borders who intend to harm our nation's security," said Special Agent in Charge Bradley. "The unlawful sale of sensitive Defense technology increases hostile nations' ability to injure U.S. military forces. Our mission of protecting America's warfighters remains paramount and is substantially furthered by these cooperative, priority investigations."

As set forth in the Information, as well as affidavits accompanying a Criminal Complaint and various search warrants, Knapp's conduct involved the illegal export and attempted export of the following U.S. defense articles:

an F-5B Tiger II fighter jet;

five (5) CSU-13 anti-gravity (Anti-G) flight suits, which are worn by pilots to counteract the forces of gravity and acceleration;

one F-14 NATOPS emergency procedures manual, which is designed for use by pilots during in-flight emergencies in F-14A and B (Tomcat), F-5 (Tiger II) and F-4B (Phantom) fighter jets;

three (3) electronic versions of the NATOPS emergency procedures manual;

four (4) AN/PRC-149 survival radios, which are hand-held search and rescue radios used primarily by U.S. Navy pilots as an emergency locator beacon; and

two (2) F-14 (GRU-7A) ejection seats.

According to court documents that have been unsealed, a cooperating defendant introduced Knapp to an undercover ICE HSI special agent (UC). The UC met with Knapp on several occasions, at locations in California, Pennsylvania, Delaware, and Budapest, Hungary. During the meetings, Knapp informed the UC that he had various defense items for sale. He also admitted to procuring an F-14 (GRU-7A ejection seat), which was sold to the UC by another source. Over the course of their interaction, Knapp provided the UC with various lists containing items for sale, and he sent photographs and descriptions to the UC via email.

On two occasions, Knapp exported items outside the United States. On Feb. 22, 2010, Knapp exported two (2) CSU-13Anti-Gravity flight suits and a NATOPS emergency procedures manual to an address in Hungary; and on May 13, 2010, Knapp exported an additional three CSU-13 Anti-Gravity flight suits to an address in Hungary. On a third occasion, Knapp sold the UC an F-14 (GRU-7A) ejection seat, which the UC indicated would be forwarded to Iran. On March 17, 2010, Knapp delivered the seat to a shipping company located in California. Knapp identified the item to the shipping company as a "museum display chair," and he provided the shipping company with a consignee's address in Denmark. After Knapp left the shipping company HSI agents seized the ejection seat prior to its export outside the United States.

Knapp first broached the idea of obtaining an F-5 fighter jet from a source in California to sell to the UC in January 2010. Knapp told the UC that the "Iranians" might be interested in various items, including the F-5 fighter jet, and stated that he was not concerned whether the jet or the other items ended up in Iran. According to Knapp, he was able to "compartmentalize" selling the UC products that would end up in Iran because the United States would "shoot down" anything provided to them. During a January 2010 meeting in California, Knapp took the UC to an airport to inspect the aircraft, and, over the course of the next several months, the UC and Knapp had several conversations regarding transporting the aircraft from California to a freight forwarder in Delaware; determining appropriate transshipment points to Iran; and devising a payment scheme. They also arranged to meet in Budapest, Hungary, to discuss the purchase.

On April 29-30, 2010, the UC and another undercover law enforcement officer posing as an Iranian intermediary, met with Knapp in Budapest. During the meetings, Knapp explained that he would have a contact fly the F-5 from California to the East Coast, where it would subsequently be crated and shipped to Hungary for transshipment to Iran. Knapp also displayed additional photographs of the F-5 on his laptop computer.

On July 9, 2010, Knapp sent a contract for the F-5 fighter jet to the UC via the United States mail. The body of the contract (titled "Contract for acquisition and

transport of F-5B from CA to DE") set forth in detail the purchase price and terms for the sale of the aircraft. The contract further set forth the timing (approximately four weeks) in which the aircraft would be flown to Delaware after UCA1 transferred $3.25 million into a bank account specified by Knapp. In addition, the contract provided terms for insurance, registration, and operational costs of flying the aircraft from California to Delaware. Knapp further noted that his requested commission would be $500,000, "with 50% paid on the date of arrival and landing of the aircraft at the DE (New Castle) or other agreed on airport, and 50% paid at the time of arrival at destination."
On July 20, 2010, Knapp met with the UC at a location in Wilmington, Del. Knapp brought to the meeting various defense items, including the four AN/PRC-149 handheld search and rescue radios, which the UC agreed to purchase for $11,000. The UC informed Knapp that the radios would be shipped to Russia.

Knapp and the UC then discussed the logistics of flying the F-5 fighter jet from California to Delaware, and preparing the jet for transshipment to Iran. UC told Knapp that the Iranians expected Knapp to make a personal guarantee that the aircraft would arrive in Iran and that it would be operational. Knapp explained that the Iranians would know that it was in working order based upon his transport of the plane from California to Delaware. He further stated that what the Iranians had already seen in photographs was what they would get. According to Knapp, the only thing he would not be able to test was the weapons systems. The UC asked whether he could tell the Iranians that Marc Knapp personally guaranteed the aircraft, to which Knapp replied that he could. The parties then signed the contract. Following the meeting, HSI and DCIS agents placed defendant under arrest.

The Information is merely an accusation, and all defendants are presumed innocent unless proven guilty. This case is being prosecuted by David L. Hall and Robert F. Kravetz, assistant U.S. attorneys

TECHNIQUES, METHODS, TARGETS

China's Culture of Secrecy Brands Research as Spying

http://online.wsj.com/article/SB10001424052748704584804575644470575141314.html#printMode

By JAMES T. AREDDY

SHANGHAI—As a "scout" for IHS Inc., a U.S. petroleum industry research firm, geologist Xue Feng won plaudits from his managers for obtaining a trove of rare data.

China's oil industry was undergoing a tumultuous period as Xue Feng, a Shaanxi province-born, naturalized American geologist, began his career as a "scout" for Colorado-based IHS Inc., and ultimately was convicted in Beijing for stealing Chinese national secrets.

Xue Min, center, sister of geologist Xue Feng, and her daughter, Guo Jie, wait outside a Beijing courthouse before Mr. Xue was sentenced to eight years for spying.

IHS databases are populated with such information about every country in the world. The data help oil companies decide where to explore and give traders a sense of energy price trends. Among subscribers to the IHS databases are Chinese oil companies that drill in Africa and buy natural gas from Australia. But more than two years after Mr. Xue's scoop in 2005, China declared the data on its fields state secrets. Now, the 45-year-old U.S. citizen is in a Beijing jail serving an eight-year sentence following a conviction this summer for spying. U.S. President Barack Obama and Washington's Ambassador to Beijing, Jon Huntsman, have called on China to release him.

Earlier this week, Mr. Xue's appeal was heard at the Beijing High People's Court. No U.S. Embassy representative was permitted to attend. But outside the court, Deputy Chief of Mission Robert Goldberg called for Mr. Xue's immediate release and urged the court to ensure the hearing was fair. It's unclear when the court will rule.

Mr. Xue is one of the latest foreigners to fall afoul of Chinese laws that classify as espionage what much of the rest of the world considers normal market research. Even as China's economic pulse is felt through the world—it is the world's No. 1 consumer of energy—Beijing seems determined to block independent efforts to measure it.

China doesn't clearly define secrets but its state security apparatus makes clear a danger zone exists: the prosecutor's basic charge against Mr. Xue wasn't simply that he found secret data, but that he facilitated its movement out of China. Mr. Xue's lawyer,

Lobbying on Mr. Xue's behalf were U.S Deputy Chief of Mission Robert Goldberg, pictured, and lawyer Tong Wei.

China's culture of secrecy is at odds with its invitation to foreign companies to help modernize its business sector. They face an economy increasingly consolidated around massive government-owned business groups, a situation that has blurred the lines between commercial and official data. Some foreign companies say China's official secrecy compounds distrust of Chinese data in

general. It has also hindered Chinese companies intent on pursuing international business opportunities, for instance, by road-blocking due diligence efforts that are basic to deal-making.

Chilled by cases like Mr. Xue's but unsure what to do, foreign companies in China are scrambling to draft internal guidelines. Some require double and triple checks of whether information is emerging from an authorized source. Others are deciding to limit their risks by outsourcing data collection to local analysts. Companies note the trickiest issues are for their ethnic Chinese employees, the targets of most Chinese prosecutions and those most likely to obtain information because they speak the language. Some firms say research jobs are getting tough to fill.

Earlier this year, four employees of Anglo-Australian miner Rio Tinto PLC were sent to jail in large part for learning how much production certain Chinese steel makers were planning and passing it to superiors, information arguably central to their jobs selling iron ore, as well as other "secrets" never publicly revealed. Rio Tinto, which wasn't a party in the case, subsequently dismissed the employees and sought to repair its business relations in China.

China puts enormous resources into disguising its demand for commodities, in part because its own purchases are a key factor in moving global prices. Market talk that Chinese demand was more than expected in 2004 was the catalyst that sent crude futures prices to records in nominal terms of around $50 per barrel. (Crude oil futures are now around $85 a barrel.)

This account of how Mr. Xue ended up in jail is based on recent interviews with analysts as well as Mr. Xue's colleagues, friends and others with knowledge of the situation. It also draws from a document published by Beijing Number One Intermediate People's Court when it sentenced Mr. Xue on July 5.

A Shaanxi Province native, Mr. Xue is the product of China's pursuit of science and its quest for an energy strategy.

As an English-speaking geology student at Xi'an's Northwest University in the late 1980s and early 1990s, Mr. Xue was assigned to be interpreter and guide for visiting geologists. One of them, David Rowley of the University of Chicago, was so impressed by the young geologist's skill and forthrightness, that he invited Mr. Xue to pursue a Ph.D. in Chicago.

At the University of Chicago, Mr. Xue had specialized in a phenomenon known as ultra-high pressure metamorphism and exhumation, a process by which rocks go from the earth's surface, down toward its core and then back out again over a 250 million year period. Mr. Rowley, who has advocated for Mr. Xue's release,

said he was so gifted as a geologist he could often identify minerals in a rock by looking at it with the naked eye.

A year after he obtained his doctorate in Chicago, Mr. Xue left academia in 1999 to work for IHS Energy in its Houston office. Mr. Xue became a petroleum "scout," collecting data on China's oil industry that was then compiled and sold by the Colorado-based publisher.

Petroleum scouting is steeped in tradition: it's a mix of scientist, journalist, sleuth and diplomat. A key task for Mr. Xue on trips to Beijing was leading oil industry geologists and other experts in small group information exchanges.

Jeremy Bowden, a former IHS researcher based in Singapore, remembers a Chinese oil company executive offering Mr. Xue information by saying, "if we can see America," in the IHS database, "we don't mind anyone seeing China." The collection of Chinese oil data "never really seemed sensitive," said Mr. Bowden. When Mr. Xue joined IHS, China's government was carving the best parts out from what were essentially government bureaus in order to list them as energy companies on stock markets. The restructuring of the Chinese oil industry gave IHS fresh opportunity to collect data.

The biggest oil group, China National Petroleum Corp., began to digitize handwritten data on 30,000 onshore oil wells in 1996.

By 2000, CNPC had put its crown jewels into a subsidiary named PetroChina Co., which went public in Hong Kong and New York, attracting investors like Warren Buffett. But PetroChina didn't absorb certain portions of CNPC, impaling some projects, such as the oil well digitization plan.

A researcher assigned to the digitization task, Xu Xu, surreptitiously made a copy of the 30,000 well coordinates, reserves and other data, according to his testimony at Mr. Xue's trial. He used a nickname and advertised energy sector information for sale on the Internet.

Two years later, Mr. Xu received an expression of interest by email from a former college classmate of Mr. Xue, Li Yongbo, according to the court's sentencing statement. By the end of 2005, prosecutors alleged, IHS had paid $228,500 for Mr. Xu's information and a handful of other sector reports. The data went through various intermediaries, including Mr. Li and another Chinese oil company, before it got to IHS, according to the court document.
Mr. Xue was lauded in an internal IHS email, recalled a former senior member of the IHS Beijing team, Xu Jin, in court testimony.

As IHS was instructing its sales staff to peddle Mr. Xue's data trove, Beijing was moving to plug information leaks. In mid-2005, the government appointed Harvard University trained lawyer, Xia Yong, to lead the National Administration for the Protection of State Secrets and begin codifying fresh controls. For instance, in 2006 the government deemed certain weather data off-limits to foreigners.

In the oil industry, analysts say, state-sanctioned publications inexplicably pruned certain data from long-standing charts. Chinese energy company executives increasingly directed industry analysts to channel questions through official spokesmen. Analysts learned that it was best to avoid researching anything about Chinese oil reserves.

By mid-2007, Mr. Xue had quit IHS to consult for another firm. It is unclear when he became a U.S. citizen, but in the fall of 2007, he returned to China using a U.S. passport for the first time.

On Nov. 20, 2007, shortly before he was scheduled to fly back to suburban Houston for Thanksgiving with his wife and two children, Mr. Xue was detained by state security officers at the bare-bones Mengxi Business Hotel adjacent to Beijing's University of Petroleum.

For months, the U.S citizen was held incommunicado under a form of house arrest, in violation of the U.S.-China Consular agreement, legal experts say.

State Security officers interrogated Mr. Xue until the following February, when they classified the oil well information as state secrets and formally arrested him. At the same time, authorities also arrested Mr. Xue's associate, Mr. Li, who was convicted and sentenced on the same charges. Mr. Xu, who initially copied the oil data, was not charged as part of the case against Mr. Xue.

The oil well information was on Mr. Xue's laptop, according to the court. Mr. Xue asked his wife to mail the computer from Houston to Beijing in hopes that he would be exonerated after cooperating with authorities and they saw that the information was not secret.

CNPC declined to comment on Mr. Xue's case. IHS cited Mr. Xue's appeal to decline most comment on the case.

IHS spokesman Ed Mattix said in a statement the company has "never been informed" that the case of Mr. Xue "involves any wrongdoing on the part of IHS and we have never been asked by Chinese authorities to remove any information from our China well information product." Mr. Mattix confirmed that information cited in Mr. Xue's prosecution is part of IHS's database.

"As a result of the issue with Dr. Xue, we have reviewed our China products and data-gathering process," Mr. Mattix said in a written statement. "We are confident that we are operating in accordance with local rules and laws."
As part of his court testimony, Mr. Xue said he was "ignorant" of the government's classification of the data, which he said included many historic, non-functioning wells. He questioned the basis for classifying the information as secret.

"In the oil industry around the world, these should be publicly available," Mr. Xue said. "It is wrong to regard this information as state secrets."

Mr. Xue's appeal challenges the court's determination that the data were state secrets.

Mr. Xue's case has shaken the tight community of researchers that tries to make sense of the country's energy market. "The mood music coming out of China is very disturbing," says a London-based publisher of influential oil-sector reports. A few weeks after Mr. Xue's case became known last year, Platts, a U.S. publisher owned by McGraw Hill Cos., began placing a prominent asterisk on its monthly estimate of Chinese petroleum demand. The star draws attention to an explanation that its data are compiled using published government statistics—in other words, not secrets. Platts says the adjustment was coincidental to Mr. Xue's case.

On Oct. 1, Beijing amended its 1989 law on state secrets, attempting to modernize it with a clearer delineation of how information should be safeguarded. The adjustments don't narrow the range of potential secrets, a list that covers broad areas of national defense, foreign affairs, policy decisions, economic and social development, plus science and technology.

Such legal adjustments herald "more consistent and transparent enforcement, but likely more aggressive prosecutions," says Nicolas Groffman, an attorney in Beijing at Mallesons Stephen Jaques.

China's National Administration for the Protection of State Secrets didn't respond to questions about Mr. Xue's case and its policies.

In Mr. Xue's adopted home of Houston, it was still the July 4 holiday when in a Beijing courtroom—with U.S. Ambassador Huntsman observing—the presiding judge rejected the geologist's arguments. "Making the information available overseas will help foreign sources get an understanding of China's oil and natural gas resources," the court concluded.

Historically, nearly all Chinese court appeals fail. If this one does, Mr. Xue won't be released from jail and expelled from China until Feb. 3, 2016, three days before his fifty-first birthday. According to acquaintances, Mr. Xue's wife is hoping the court will at minimum reduce his sentence. Supporters opine a state visit to Washington early next year by Chinese President Hu Jintao may be the best chance for Mr. Xue's freedom.

Electronic Pickpocketing

http://www.wreg.com/wreg-electronic-pickpocketing-story,0,5841317,print.story

Scott Noll

10:03 AM CST, December 3, 2010

Credit card info swiped with off-the-shelf scanner

Estimates place nearly 140 million customers at-risk
In statements to WREG On Your Side Investigators, card companies downplay the threat

Scott.Noll@wreg.com

(Memphis, 12/03/2010)

Call it high-tech hijacking.

Thieves now have the capabilities to steal your credit card information without laying a hand on your wallet.
It's new technology being used in credit and debit cards, and it's already leaving nearly 140 million people at-risk for electronic pick pocketing.

It all centers around radio frequency identification technology, or RFID.
You'll find it in everything from your passports to credit and debit cards.
It's supposed to make paying for things faster and easier.

You just wave the card, and you've paid.

But now some worry it's also making life easier for crooks trying to rip you off.
In a crowd, Walt Augustinowicz blends right in.

And that's the problem.

"If I'm walking through a crowd, I get near people's back pocket and their wallet, I just need to be this close to it and there's my credit card and expiration date on the screen," says Augustinowicz demonstrating how easily cards containing RFID can be hacked.

Armed with a credit card reader he bought for less than $100 on-line and a netbook computer, WREG On Your Side Investigators put Augustinowicz to the test.

For about an hour he patrolled Beale Street, looking for RFID chips to read, and credit card information to steal.

"There you go," said Augustinowicz scanning one willing participant's wallet. "It's a MasterCard," he explained looking at the man's credit card number and expiration date pop up on the screen.

Even people who thought there was no way we could pick their pocket electronically without laying a hand on them, soon learned they were wrong. "You have a SunTrust card in there," Augustinowicz explained to a second "victim." "And that's your account number and expiration date," he said showing the man the screen.

"That's just too vulnerable for everyone to take advantage of," said another person, who at first doubted she would fall victim to electronic pickpocketing. Even scarier, Augustinowicz says bad guys could work a crowd, stealing numbers and then e-mail them anywhere in the world.

"After a game here I could literally pull couple thousand cards," Augustinowicz explained to a group of women visiting from Chicago.

Using just an off-the-shelf card reader, Augustinowicz explained he could swipe credit card numbers, expiration dates, and in some cases, even people's names. It's enough, Augustinowicz says, to do damage.

"We've done it," he insisted. "We've picked up the phone, called 800 numbers, ordered stuff under a fake name, shipped it to a foreclosed home and the product comes in the mail."
It's not just your credit and debit cards at-risk.

While they are harder to hack, all US passports issued since 2006 contain RFID technology that can be read, and swiped.

"It gives me a lot of personal information like your date of birth, your photo if I wanted to make some sort of ID," said Augustinowicz demonstrating with his reader.

Augustinowicz is the founder of Identity Stronghold (http://www.idstronghold.com).

His company markets secure sleeves, and ID holders designed to block RFID hacking.

Among his customers is the US government.

"As soon as I squeeze it, it can read it," explained Augustinowicz showing off a badge holder. "When I have it closed, it can't read it."

So is Augustinowicz just a boogeyman, trying to scare people into buying a product, or is the threat real?

We showed video of Augustinowicz in action to computer security expert, and University of Memphis professor Mark Gillenson.

"It's potentially a major problem," said Gillenson after watching clips of Augustinowicz wiping people's credit cards number.

Gillenson calls it technology run wild, and calls our findings compelling.
"I think people do need to be concerned and do need to be aware and we'll see if this becomes a major problem," said Gillenson.

And that's the big question.

Experts at the Identity Theft Resource Center tell WREG On Your Side Investigators they've never seen a case of RFID skimming used to steal information.

But Augustinowicz believes that's because the crime could easily go untraced; unsuspecting people, falling victim to just another face in the crowd with a hidden scanner in hand.

"You might as well paint your credit card number across your t-shirt and walk around with it because it's the same difference," warned Augustinowicz.
In our time on Beale Street, Augustinowicz scanned 26 wallets and purses.

Five of them, nearly 20% had cards with RFID chips.

All wallets and purses scanned for our story were scanned with the permission of the credit card holders.

Electronic Pick pocketing Goes Viral
Scott Noll
5:49 PM CST, December 6, 2010

FAST FACTS:

- Electronic Pick pocketing investigation viewed 1.6 million times on-line
- Story has set a record for views on wreg.com
- Better Business Bureau says interest highlights concerns about ID theft

(Memphis, 12/06/2010) It's the latest viral video taking the internet by storm.

In the last three days more than 1.2 million people have watched on-line as WREG On Your Side Investigators exposed the threat of electronic pick pocketing.

Using a card reader bought on the internet for less than $100, our expert, Walt Augustinowicz, founder of Identity Stronghold, shows us how he could swipe credit card information from cards equipped with radio frequency identification technology, or RFID.

Maybe the only thing more incredible than how easily your information could be stolen is how quickly our video has become an internet phenomenon.

"When we first were looking at the numbers of people watching it and reading it, I actually had to double-click and double-check," admitted George Brown, Web Content Manager for wreg.com. "I thought it was a mistake at first because it definitely sets a new record for the website."

Since the story was posted on November 18, it's been viewed 1.6 million times on wreg.com.

It's been the most-viewed story for more than a week.

The ability of anyone with a card-reader to pick your pocket electronically has caught the attention of CBS news, and countless blogs worldwide.

So why the popularity?

The head of the Better Business Bureau of the Mid-South says it speaks to how common identity theft is.

"Ten, eleven million people a year are victims of it," explained Randy Hutchinson of the BBB. "A big part of this is fraudulent use of credit cards so I think anytime

people get concerned a credit card could be used particularly when they have absolutely no clue."

The BBB has never received a report of a contactless pay card being compromised.

Neither has the Identity Theft Resource Center.

But experts say our story is proof that you need to keep an eye on who's using your credit.

"Crook are adept at exploiting and overcoming technology," said Hutchinson. "So I couldn't rule out that it could happen at some time."

What the bad guys don't realize is that we're a step ahead of them.

We're On Your Side.

"I think a lot more people are seeing that it's not just a slogan," explained Brown. "It's something we actually are using, putting that information out there for people to protect themselves. its news you can use."

There are a number of ways to protect yourself.

You can buy secure sleeves for your cards or specially-lined wallets.

Augustinowicz's ID Stronghold, www.idstronghold.com, specializes in those products.

Aluminum foil will also block scanners.

Also, if you carry two cards with radio-frequency identification embedded in them, those signals will cancel each other, and protect you from electronic pickpockets.

Spooked: The spies who loved me

December 2008

http://www.theatlantic.com/magazine/print/2008/12/spooked/7143/

By Joshua Kucera

"Would you be interested in writing stories about what we are doing in the Russian government?" Vladimir asked me. We were eating lunch at Cactus Cantina, a sprawling Mexican restaurant near the Russian Embassy; he was having fajitas, I was having enchiladas. His English, by diplomatic standards, wasn't great, so I couldn't tell exactly what he was getting at. Then he added: "We would pay you, of course." Ah. Now it was clear.

I had met Vladimir (not his real name) a week before, at a conference in Washington. He had seen my name on the registration list and sought me out, which was unusual: Russian government officials don't often seek out journalists. The embassy's public-relations officer had never even returned any of the calls I'd made; Vladimir significantly outranked him.

Vladimir had said he'd been following my stories on eurasianet.org, a news Web site primarily about the former Soviet Union to which I regularly contribute, and wanted to talk to me. So he'd invited me out for lunch, and there we were.

I had no intention of taking his money, but I tried to be noncommittal; I enjoyed his company and the rare chance to talk about Russian-U.S. relations with a high-ranking Russian diplomat. Kosovo had just declared independence—a clear precedent, he argued, taking a sip of his Dos Equis, for Abkhazia and South Ossetia, the pro-Russia separatist regions in Georgia, to do the same. I replied that one could make the same case, then, for Chechnya. He looked genuinely puzzled. "But no one in Chechnya wants to be independent," he said.

After Vladimir paid the bill and we left the restaurant, I pointed out a nearby pizza place that was one of my favorites in D.C. and recommended that he try it some time. So when he next called, about a month later, he proposed that we eat there.

I ordered first, a pizza puttanesca. His eyes brightened. "Ah, Putin! I also will have puttanesca!" he told the waitress.

And he told me more about what he wanted. Giving me the names of two Web sites, russianpeacekeeper.com and inforos.com, he said that I could take any stories on those sites and post them on EurasiaNet. He would pay me "$300 or $400," he said, though I was given to believe that that was only his initial offer. Back at home, I checked out the Web sites. One top story was headlined "Timoshenko Is a Playboy's Star" (referring to Ukraine's prime minister, Yulia Timoshenko, who had said something vaguely positive about the nudie mag in an interview with the Ukrainian edition of Elle). Another was "U.S. Navy: Spies, Deserters, Maniacs," which collected various unrelated misdeeds by American sailors. It ended ominously: "One can only guess what the next 'frolic' by U.S.

sailors assigned to a cruising nuclear-powered submarine stuffed with ballistic missiles may lead to …" (Foreboding ellipsis original.)

All of this was fun, and a good story to tell my friends. But apparently some people were taking it more seriously. A few months later, I got a call on my cell phone from a man who identified himself as an FBI agent. "We want to talk to you about someone you've been in contact with," he said. He proposed that we meet at a Starbucks near my home.

On my way to meet him the next morning, I realized that I didn't know what he looked like. Not to worry: I was in Adams Morgan, D.C.'s original hippie/hipster neighborhood, and he and his colleague were FBI agents straight out of central casting, with dark-blue suits and close-cropped hair. They wanted to know everything I knew about Vladimir. I had assumed that he was a spy. But I was pretty confident that there was nothing illegal about our conversations. So I spent about 45 minutes telling them what I could. I learned my experience was not that unusual: Cactus Cantina, the agents told me, was the favorite haunt of Russian spooks (and the cringe-worthy tipping I had observed was standard practice).

"Do you have any questions for us?" one of the agents asked at the end of our conversation. Yes: How did you find out about me and get my cell-phone number? "I know you're the FBI," I said, "but—" "Exactly," he said, cutting me off.

He asked me to call him whenever I met again with Vladimir. I balked. I didn't want to be an FBI mole any more than I wanted to be a Russian spy. "Yeah, I know you have your 'journalistic ethics,'" he said, making air quotes around the words.

I left Starbucks with my heart pounding. How did they know I was meeting Vladimir? Did they have their own spy in the Russian Embassy looking at his appointment book? Were they reading his e-mail? Listening to his phone conversations? And were they now reading my e-mail and listening to my phone conversations? And what would happen if I didn't become a mole?

I'll never know. I met with Vladimir a few more times (without telling the FBI). But when I told him I couldn't take his money, he stopped calling. I'm not sure that means, though, that the U.S. government has stopped listening.

This article available online at:
http://www.theatlantic.com/magazine/archive/2008/12/spooked/7143/

Spying in a changing world

http://www.moscownews.ru/russia/20101220/188296966.html

by Anna Arutunyan at 20/12/2010 20:19

As Russia's Foreign Intelligence Service this week marks 90 years since its founding, the country's spies are seeking to shrug off one of the organisation's most embarrassing scandals – when 10 deep-cover agents were betrayed and arrested in the United States this summer.

"This year, like many others, was a difficult one for foreign intelligence," President Dmitry Medvedev told SVR officers as he congratulated them ahead of the service's 90th anniversary on Monday, reminding them that they should draw lessons from the spy exchange and investigate why it happened.

Prime Minister Vladimir Putin was, as usual, more categorical.

"I assure you, they will expire on their own," he said of the supposed traitors during last week's call-in show with the public. "Just think! A person dedicates his whole life to serving his motherland, and some cad turns up and betrays him. How will he look into the eyes of his children, the swine?"

Loyalty and betrayal

Gennady Yevstafiyev, a retired SVR lieutenant general who spent decades working under diplomatic cover in Japan, Pakistan and India (among other places), knows first hand the devastation of betrayal for an agent who is driven by zeal.

"Everyone has their own path towards betrayal," he told The Moscow News in an interview at his Moscow apartment last week. "It is very different each time. Sometimes it is forced, when a person is blackmailed and turns out that he is weak."

Unsurprisingly, Yevstafiyev would not disclose exactly when he joined the First Chief Directorate of the KGB, the foreign intelligence service that Vladimir Putin also served in during the 1980s. But a career of some 40 years made him well placed to observe the change in morale of fellow agents, he said.

And those 10 agents "who wound up in the situation they were in not because of something they did, but because of betrayal," certainly deserved a meeting with Putin, Yevstafiyev said.

"The meeting was telling – after all, it had a political cost for [Putin],"

Yevstafiyev said, adding that support from the top was crucial to reward loyalty.
Ideological zeal

To this day, the SVR advertises a job with the service for the "romance". But is spy work really that alluring any more?

"There's one law for all intelligence services: I know that you know that I know that you know," Oleg Nechiporenko, a retired KGB colonel who served in Mexico, told The Moscow News. "But if there's a break in the chain – I know that you know that I don't know – that's when either intelligence or counter-intelligence tries to correct the problem."

For Nechiporenko – who described a sense of professional camaraderie with CIA officers with everyone knowing that the other knew – the KGB differed little from the Americans.

But others admit that ideology was a powerful driving force that historically set Russian agents aside, with even the CIA marvelling at their zeal.

"Clandestine service officers are all driven by mission," Mark Lowenthal, a former CIA agent, told The Moscow News in an e-mail interview. "But some of the statements coming from those arrested in the US – like putting service above family – are not things that US officers would say."

For Yevstafiyev, putting service above family was just part of the deal – and that was why out of all the people who join the force, only 15-20 per cent are fully dedicated, he said.

"It's not foreign affairs, it's not the military. It demands a lot of training, but first of all it demands a certain type of soul, and the desire to do this kind of work. It's creative work – you take fatal risks. It is not for everyone. But a lot of people go despite this."

A feared organisation

There is another distinguishing factor that sets apart the KGB and its successor agencies – the FSB and the SVR – no other agency has instilled so much fear in the citizens it was charged with controlling.

"It is a special service that controls itself," Kirill Kabanov, a former FSB officer who now heads the National Anti-Corruption Committee, told The Moscow News.

"For historical reasons, from Tsarist times through the NKVD, this has made them feel they can do what they want, and people become afraid."

For Nechiporenko, fear is part of creating the image of the foe – which is the raison d'etre of the service.

It can also be useful in securing funding.

"Traditionally, every year when the CIA would configure its budget, there would be a rise in anti-KGB sentiment," said Nechiporenko. "This influenced Congress to vote for bigger budgets."

Take away the foe, and the whole system crumbles, experts say.
That foe disappeared when the Soviet Union fell apart – and the United States, once the enemy, became at best an ally and at worst an adversary.
But that wreaked havoc in security. For all purposes, Russian intelligence suddenly disappeared – and would only resurface in the late 1990s, Nechiporenko said.

For Yevstafiyev, many of the internal changes undermined morale and the quality of the work. Today, he sounds somewhat dismayed with the gradual transformation of a closely knit, ideologically-motivated force into a swollen bureaucracy that young men increasingly joined for perks like cars, dachas, and apartments.

There was a reason, after all, why the heyday of Russian espionage ended after World War II. The great spies of the 1930s got by on little else but ideological zeal. A smaller staff meant that each agent had to be resourceful and rely on his analytical capabilities rather than gadgets.

"We envied military intelligence for their technology," said Yevstafiyev. "There was a tremendous field of cooperation between the SVR and [the GRU] military intelligence, given that they had a tremendous advantage in technology, particularly in outer space."

For Nechiporenko, it wasn't just a shift for Russia – but transformed the way international intelligence functioned.

"In the 1990s Russia entered a new dimension – ideologically and politically. There was a withdrawal – and it certainly affected the CIA too. They were used to working with a certain foe, and now that foe had disappeared."

Study: No Hacking Needed when Modern Spies Steal Corporate Data

http://www.thenewnewinternet.com/2010/12/06/study-no-hacking-needed-when-modern-spies-steal-corporate-data/

A new study reveals two-thirds of employees expose sensitive data outside the workplace, some even revealing highly confidential information such as customer credit card and Social Security numbers.

Conducted by People Security, the Visual Data Breach Risk Assessment Study also found most companies lack policies or measures to safeguard sensitive information from computer screen snooping when employees are working outside of their offices. Seventy percent of the 800 respondents said their company had no explicit policy on working in public places, and 79 percent reported no company policy on the use of privacy filters to prevent visual data breaches.

With the increase of mobile workers carrying confidential data with them outside the office, snooping is no longer a harmless hobby and may represent a weak link in corporate data security practices, said Dr. Hugh Thompson, chief security strategist of People Security.

"Today's latest smartphones now make it possible for a data thief to take a high-resolution picture of confidential information on a computer screen and retrieve readable data without any hacking necessary," he said. "Information revealed on mobile devices outside the workplace now creates a window into a corporation's most confidential data – whether it is regulated or simply company secrets – and significantly raises the threat level of visual data breaches."

However, more than half of survey respondents are aware of the security issues of using their laptops for work purposes outside their place of employment. Fifty-seven percent said they have stopped working on their laptops because of privacy concerns in a public place, and 70 percent said they would be more productive in public places if they thought no one else could see their screen.

Spy techniques can elicit useful intel

http://www.shreveporttimes.com/fdcp/?1292270711107

December 12, 2010

If you really want to know why the project you and your team just put six months of your life into ended in disaster, this guy can help.

Peter Earnest is a former CIA spy master who knows how to get information from people or — as he and his co-author call it — use elicitation techniques. Which is a nice way of describing the science of interrogation by way of conversation.

In their new book "Business Confidential: Lessons for Corporate Success from Inside the CIA," Earnest, who worked for the CIA 36 years and is now executive director of the International Spy Museum, and business writer Maryann Karinch, explain how techniques of our national espionage and intelligence services apply to business success. The section on gathering intelligence and collecting information on people gets to the heart of getting to the bottom of who did what and what was said.

The authors offer up verbatim psychological approaches that may be more productive than the typical post-mortem meeting taking place in companies every day.

Perhaps these approaches which involve "flattery, criticism and using the leverage of someone's emotions" can be put to work in your office.
For instance, if you are a manager trying to get to the bottom of why the deal of the century fell apart, instead of "Who dropped the ball on this?" you might try "direct questioning," which would sound like this: "What signs did you notice that the deal was falling apart?"

Or there's the "emotional appeal" approach:"Your concern for your team has always been evident, so just do what's best for them. Tell me what went wrong so everyone can learn from it."

There's always the when all-else-fails "futility" proposition:
"I don't see any way for you to get out of this mess without your career taking a hit. Why don't you tell me what happened with the project. Maybe I can make some sense of it."

The "fear down" overture: "You seem very upset about the failure of the project. Don't worry. Just calm down and we'll figure this out and fix the problems."
The "pride and ego down" approach: "I think you've been slipping lately, but maybe other members of the team are making you look bad. Tell me exactly what happened with this project."

Or the "we know all" position: "A few of the team members have sent me e-mails about the project, so I have a pretty good idea of what went on. Tell me what you think happened here."

The "silence" approach: "Have a seat. Let's talk about the project."
Then you say nothing, waiting for the person to start blurting things out. Yes, silence is that awkward.

Your technique for obtaining information in business "will be shaped by whether you want an operational relationship or just a quick bit of information from someone you may never see again," the authors say.
For example, you can simply throw someone a bone — which is giving information to get it. I must say, I find this technique a bit underhanded.

Nonetheless, it goes like this:

You say, "There was a proposal talked about at such-and-such meeting" — knowing darn well the proposal was shot down.

But you don't mention that fact.

"When you talk about something that seems to be confidential, that sense of quid pro quo often takes hold," they say.

Sneaky stuff? Perhaps.

But these techniques, based on an understanding of human nature, can get to information without being threatening.

Which goes to show that the intelligence mindset used in the world of espionage can also have value in the world of business.

Andrea Kay is the author of "Work's a Bitch and Then You Make It Work: 6 Steps to Go From Pissed Off to Powerful."

Send questions to her at 2692 Madison Rd., #133, Cincinnati, OH 45208; www.andreakay.com or www.lifesabitchchangecareers.com.
She can be e-mailed at andrea@andreakay.com.

F.B.I. Memos Reveal Cost of a Hacking Attack

http://bits.blogs.nytimes.com/2010/12/14/f-b-i-memos-reveal-cost-of-a-hacking-attack/?pagemode=print

December 14, 2010, 10:58 am

By VERNE G. KOPYTOFF

12/15/10 | Updated

A hacker attack on a company's Web site can be costly, but exactly how much money it takes to repel and recover from a malicious strike is rarely disclosed by besieged companies.

But an attack several years ago on Google cost it $500,000, according to internal F.B.I. memos obtained by The New York Times through a Freedom of Information Act request. The documents also reveal some information about the attacker.

Last week PayPal, Visa and MasterCard tried to deflect a series of attempts to knock its Web sites offline by supporters of WikiLeaks after those companies suspended the processing of payments to the document-leaking Web site. But in 2005, Google was battling the Santy worm, a bit of malicious software that caused infected computers across the globe to automatically enter search queries — so many, in fact, that Google was overwhelmed.

On Dec. 22, 2005, Google complained to the F.B.I. that the attack had slowed its search engine's performance. For much of 2004 and 2005, Google had been plagued by variants of the worm, which used search queries to find vulnerable Web sites and deface them by exploiting a security hole in the community forum software, PHP Bulletin Board. Google had tried to filter queries containing phrases linked to the worm, but with limited success.

"As Google filters out certain string search phrases, within minutes, the subjects modify the search phrase to once again bypass Google's filters," an F.B.I. agent in San Francisco wrote to colleagues, recommending that an investigation be opened. Google's efforts to stop the worm had unintended consequences of blocking legitimate searches, the agent wrote.

In a measure of the seriousness of the attack, Google devoted an entire engineering team to the battle at a cost of $500,000, a figure it arrived at by calculating the hours spent fighting the worm and the lost revenue, the report said. A year earlier, Google suffered a $100,000 loss from the MyDoom virus,

which slowed or stalled Google's search engine for several hours, according to documents from a separate F.B.I. investigation.
Although sizable, the damages are only a fraction of Google's revenue for those years. In 2005, Google reported $6.1 billion in revenue.

Paul Judge, chief research officer for Barracuda Networks, a Web security company, said that it was rare for the monetary damages caused by hackers to become public. In fact, many companies never bother to calculate the total because they are too busy keeping the hackers at bay or they simply never report the incident to law enforcement out of embarrassment, he said.
In any case, Mr. Judge noted that the cost of an attack could rise quickly when the amount of time it took to clean up afterward, reconfigure firewalls and assess the initial response was included.

"Half a million dollars — you can get to that sum really quickly," Mr. Judge said. "When an attack happens, it's all hands on deck."
In examining the software code used in one variant of the Santy worm, Google engineers found a potential lead to the attacker's identity. In the code was embedded a Gmail address for a technical contact that the F.B.I. said might belong to the variant's creator. That e-mail address was redacted from the document, as were the names of any Google employees who had spoken with the F.B.I.

The F.B.I. issued two subpoenas shortly thereafter for an individual or individuals to appear before a federal grand jury in San Jose, Calif. Those names were also redacted.

A few weeks later, Google had a change of heart. On Jan. 31, 2006, the F.B.I. noted that Google's legal department told the agency that the company was no longer interested in any further investigation. "Inasmuch as Google is the victim and their assistance in the form of providing logs is necessary to pursue prosecution, it is recommended this case be administratively closed," the F.B.I. agent wrote.

Ex-intelligence official blasts Pollard lobbying

By Jeff Stein
http://voices.washingtonpost.com/spy-talk/2010/12/former_top_intelligence_offici.html

Jonathan Pollard's ex-wife Anne and her father were settled in Israel by the government there this week, the latest chapter in a renewed campaign to free the confessed spy.

Israel has angled periodically for Pollard's release since 1998, when it admitted, after 13 years of denials, that the former naval intelligence analyst was not a rogue agent but an officially sanctioned spy.

Last September Prime Minister Binyamin Netanyahu relit the fires under the case when, according to Israeli Army Radio, he asked the Obama administration to release Pollard in exchange for a temporary halt in Israel's construction of Jewish settlements.

A month later Lawrence Korb, an assistant secretary of defense at the time of Pollard's arrest in 1985, asked President Obama in a public letter to commute Pollard's sentence to time served -- 25 years. A handful of members of Congress seconded the call, which has been bitterly resisted by U.S. intelligence agencies.

Now another key official at the time of Pollard's arrest, former FBI and Navy lawyer M.E. "Spike" Bowman, is weighing in -- *against* his release -- in a forthcoming article.

"Since I was the only person who actually touched all aspects of the case I thought it was incumbent on me to lay out the facts," Bowman, the top legal adviser to Navy intelligence at the time, and who later worked as senior counsel at the FBI and as deputy director of the National Counterintelligence Executive, told SpyTalk.

In a piece written for a forthcoming journal of the Association of Former Intelligence Officers, founded years ago to support the CIA, Bowman notes that there have been "few rebuttals of this escalation of calls for Pollard's release…mainly because so few were cognizant of the scope of Pollard's disclosures, or the misuses of those disclosures, and the damage they did to our own operations and sources."

The true extent of the spy's damage remains locked in government vaults, Bowman writes, "because when a plea agreement was reached, it was no longer necessary to litigate issues that could have exposed the scope of Pollard's treachery -- and the exposure of classified systems."

But the retired Navy captain singles out three of Pollard's leaks, the first being "the daily report from the Navy's Sixth Fleet Ocean Surveillance Information Facility (FOSIF) in Rota, Spain, a top-secret document filed every morning reporting all that had occurred in the Middle East during the previous twenty-four hours, as recorded by the NSA's most sophisticated monitoring devices."

"Probably the most serious disclosure (of those of which we are aware) was the TOP SECRET NSA RAISIN manual, which lists the physical parameters of every known signal [or electronic communication], notes how we collect signals around

the world, and lists all the known communications links then used by the Soviet Union," Bowman writes.

"It is certainly the thing that stood out in the mind of the sentencing judge; particularly when Pollard alleged at sentencing that there really was no harm done. The judge interrupted and brought him up short, pointing specifically to disclosure of the RAISIN manual."

Bowman also writes that "Pollard disclosed information to the Israelis that could prevent the U.S. from monitoring Israeli activities in the Middle East -- clearly a foreign policy nightmare."

Pollard admitted to prosecutors that his handlers at the Israeli Embassy often goaded him for better-quality information, Bowman says.

"[H]is initial handler told him that they already receive 'SECRET' level material from the United States. What they needed was the TOP SECRET data they were not yet receiving."

Hard copies of the documents Pollard stole in 18 months could "fill a room that is six feet by six feet by ten," Ronald Olive, the top Navy investigator in the Pollard case, told SpyTalk.

"No other spy in the history of the United States stole so many secrets, so highly classified, in such a short period of time," he maintains.

Bowman also takes aim at Korb's contention that Pollard has been unduly punished, arguing in his open letter to Obama that "the average sentence for Pollard's offence" -- stealing secrets for "friendly" countries -- "is two to four years, and under current guidelines the maximum sentence is 10 years."

But Bowman, as well as a counterintelligence officer involved in Pollard's case who insisted on anonymity, says Korb's math is skewed.

"The supporters who claim that the sentence of Pollard was disproportionate to the crime cite three to four cases where Americans sold or gave documents to non-adversary countries like Saudi Arabia, Ecuador and El Salvador," the CIA officer said. "These were a handful of secrets, and those who committed the crime were sentenced proportionately. What Pollard's crew has done is to take these handfuls of cases and then extrapolated the sentences saying that Pollard has served far longer than the 'average' spy who spied for 'friendly services.' "

In fact, the average sentence for those caught spying for the Russians, not counting the 365-year term given to Jerry A. Whitworth, part of the infamous John Walker family spy ring, was over 36 years. Three spies other than Pollard, including Russian mole Aldrich Ames, were given life sentences.

Of course, Pollard didn't just spy for Israel, although that was far and away his main benefactor.

"Intelligence officials have unofficially detailed instances of additional disclosures to other nations," Bowman writes. "These officials said that Pollard had given classified documents to Pakistan, South Africa and two other countries they declined to identify."

Some the documents Pollard gave Israel ended up in Moscow, according to various reports, but as one investigator in the case told SpyTalk, "there are only two countries that know the facts …Russia and Israel. Which leads me to believe we will never know the truth."

Pollard's current wife, Esther, wrote in the Jerusalem Post Monday that the statement of support by Korb, and another from his former Israeli handler Rafi Eitan claiming that Washington had reneged on a verbal pledge to release Pollard after 10 years, "provide Israel with the golden key to open Jonathan's jail cell."

It's long past time, she said, for Netanyahu to go public with a demand to Washington that Pollard be released.

So far, however, the prime minister has refused to pick up the megaphone. And judging by Bowman's forthcoming piece, his private pleas will, likewise, fall short.

Cybercriminals, Insiders May Work Together To Attack Businesses

Gaining access and stealing data from companies is sometimes a joint effort between bad guys and employees, experts say

http://www.darkreading.com/taxonomy/index/printarticle/id/228200983

By Robert Lemos, Contributing Writer, Darkreading
Nov 15, 2010 | 04:26 PM

For 19 months, an employee at Johns Hopkins Hospital allegedly stole patients' identities, feeding the information to four outsiders who used the data to charge more than $600,000 in goods on store credit. Jasmine Amber Smith, 25, has been charged with using her inside access to fuel the identity theft ring.

Employees working with cybercriminals might not be the norm for security breaches, but it's not a rare crime, either, experts say. It's not unusual for cybercriminals to gain inside access through bribery and solicitation -- two

components of social engineering, according to Verizon Business' Data Breach Investigations Report. Social engineering accounted for 28 percent of breaches analyzed in the report, with solicitation and bribery leading to nearly a third of those breaches.

"These were scenarios in which someone outside the organization conspired with an insider to engage in illegal behavior," the report says. "They recruit, or even place, insiders in a position to embezzle or skim monetary assets and data, usually in return for some cut of the score."

While stolen data can cause public relations headaches and lose the goodwill of customers, a company's customer data may not be its most valuable asset. Companies' proprietary knowledge and corporate secrets -- such as business plans, trade secrets, and sales forecasts -- are, on average, twice as valuable, according to a March 2010 report by analyst firm Forrester Research (PDF). Yet the loss of such data is usually not reported, experts say.

Because partnerships between cybercriminals and insiders are still uncommon, companies should focus their defenses on mainstream practices and tools for monitoring employee behavior, says Phil Neray, vice president of security strategy for Guardium, an IBM company.

An employee could stay within their authorized limits and still steal from the company, Neray observes.

"The only way to handle that is to rely on other forms of security than just identity and access management," Neray says. "The bad guys may have someone on the inside -- or a copy of the login credentials for your most sensitive systems -- so you have to start using anomaly detection, not just at the network level, but at the user-activity level."

Most of the cases of insider cooperation analyzed by Verizon Business -- which included data from the U.S. Secret Service -- involved embezzlement from banks, retailers, or the hospitality industry. Companies in those industries should have policies and technology in place to catch insiders focused on cash.

The report from Forrester found that aerospace, defense, electronics, and consulting companies had far more to lose from the theft of corporate secrets. A rogue employee stealing corporate information is generally the most expensive breach, according to that report.

Companies should be wary of signs that could show an employee's intentions. In its report, Verizon Business found that insiders who resort to crime frequently are cited multiple times for violations of corporate IT policies before they ever

commit any illegal action. Doing regular background checks on employees who have access to sensitive systems is a must, experts say.

"We need to move beyond traditional forms of security, such as firewalls and antivirus," Guardium's Neray says, "and instead move to continuous, real-time monitoring of access to sensitive systems."

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

Many malware attacks triggered by USB devices

Antony Savvas

December 6, 2010 (Computerworld UK)

http://www.computerworld.com/s/article/print/352998/USB_Devices_Guilty_in_Many_Malware_Attacks?taxonomyName=Security&taxonomyId=17

One in every eight malware attacks occurs via a USB device, often targeting the Windows AutoRun function, according to Czech security vendor Avast Software.

The company reported that of the 700,000 recorded attacks on computers in the Avast user community during the last week of October, 13.5% came via USB devices such as flash drives.

AutoRun alerts computer users when a new device is connected and helps them choose which application should run the new files.

"AutoRun is a really useful tool, but it is also a way to spread more than two-thirds of current malware," said Avast virus analyst Jan Sirmer. Cybercriminals are taking advantage of people who use USB flash drives to share large files with friends or transfer files at their workplaces, Sirmer said.

Infected USB devices -- which can include portable gaming units, digital cameras, mobile phones or MP3 players -- start executable files that invite a wide array of malware into host computers. The incoming malware copies itself into Windows and can replicate itself each time the computer is started.

Avast urged users not to boot up PCs that already have USB devices attached, because the malware will load before some antivirus programs do.

Tuesday Most Active Day for Malware Distributors, Says SonicWALL

http://www.eweek.com/index2.php?option=content&task=view&id=65774&pop=1&hide_ads=1&page=0&hide_js=1&catid=45

By: Fahmida Y. Rashid

2010-12-27

SonicWALL researchers analyzed the malware and threat landscape of 2010 and found several global trends, including the intriguing finding that Tuesday is typically the most threat-heavy day of the week.

After analyzing the malware and online threats of 2010, SonicWALL security researchers said they found that Tuesday was the most threat-heavy day of the week.

Monday was a close second for threat-related traffic, Ed Cohen, Sonic Wall's vice-president of e-mail security, told eWEEK. It wasn't clear from the analysis why malware activity was the highest on Tuesdays, but Cohen speculated a connection with Microsoft's Patch Tuesday announcements.

SonicWALL researchers noticed this pattern for China, India, Mexico, South Africa, Taiwan, Turkey, the United States, and several European countries, Cohen said.

The end-of-year cyber-security summary is based on an analysis of data collected by the SonicWALL Global Response Intelligent Defense Network during 2010, said Cohen. The data, collected by "millions" of SonicWALL anti-spam and e-mail security sensors, is broken out geographically and includes information of more than 30 countries, the company said.

The researchers also found that the most active time for threat-related traffic in the U.S. was between 10 a.m. and 11 a.m. Pacific time, said Cohen. He said this coincided with the West Coast getting started with the workday and the East Coast just returning from lunch.

Interestingly, the researchers found that malware has a seasonal component, with certain types being more prevalent during specific times of the year, said Cohen. According to the analysis, Trojans tend to peak in September and December, corresponding with the proliferation of back-to-school offers and holiday greeting cards. However while worms spike in December just in time for the holidays. As expected, adware threats peak over September, October, and December, as online advertisers serve up more ads during the holiday season.

However, there was also a "second wave" of threats, as attackers send follow-up scams in January, when bills come due, said Cohen.

Malware activity was high during the 2010 holiday season and the researchers expect distribution levels twice what was seen in 2009 and 2008, said SonicWALL. The top three threats were Trojans, video-based malware and PDF-based exploits.

The amount of malware for the whole year 2010 tripled, compared to 2009, as well, said SonicWALL. Along with PDF-exploits, Java-based exploits were very common during the year, said Cohen. He expects a rise in mobile malware, as he saw several proof-of-concept attacks, such as one for the iPhone. The other top threats for the year included the Conficker worm, Zeus Trojan, FakeAV scams, and Web exploits kits such as Gumbla and Phoenix.

Phishing fraud continues to be a serious problem, SonicWALL said. In fact, most of the threats the researchers found in 2010 were not "brand-new" types of malware, nor were they "super-intelligent," said Cohen. The number of e-mails soliciting people to go to bogus Web sites have increased, but still fell under the category of "traditional" phish and spam attacks, he said.

Even though China has often been cited as one of the countries responsible for sending out malware and spam, SonicWALL researchers found that China and Taiwan were now the most heavily hit by threats, Cohen said. Taiwan topped the list as the country most heavily hit with malware, while China was the country most heavily hit with intrusion related and multimedia threats, according to the research analysis.

In an analysis of poisoned Google search terms, the researchers found that terms related to the Oscar awards were the most common, such as "what time do the Oscars start," "Oscars winners 2010 list" and "academy awards 2010 time," said Cohen.

"These findings serve as a tool to give IT insight into how best to prepare their networks for the upcoming year," said Boris Yanovsky, vice-president of software engineering at SonicWALL.

Possible New Threat: Malware That Targets Hardware

Researchers demonstrate proof-of-concept for developing malware that attacks specific hardware processors with 'surgical' precision

http://www.darkreading.com/taxonomy/index/printarticle/id/228300082

By Kelly Jackson Higgins, Darkreading
Nov 17, 2010 | 03:54 PM

French researchers say it's possible to write malware that attacks specific hardware processors rather than operating systems or applications.

Anthony Desnos, Robert Erra, and Eric Filiol, of Ecole Sup?rieure d'Informatique Electronique Automatique (ESIEA) in Paris, have developed a proof-of-concept for hardware-specific malware, which they consider a step up from Stuxnet and a potentially key weapon in cyberwarfare. The malware can easily identify and target specific hardware systems based on the on-board processor chip, the researchers say.

They used the so-called floating point arithmetic (FPA) to help identify processors, including AMD, Intel Dual-Core and Atom, SPARC, Digital Alpha, Cell, and Atom. Hardware malware doesn't exploit vulnerabilities in hardware -- it preys on actual features: "We just exploit differences in processor features. There will be always such differences," Filiol says.

In order to pinpoint the type of processor, the malware would see how a processor handles certain mathematical calculations. This breed of malware is not any more difficult to create than malware that targets software vulnerabilities, Filiol says. "The malware algorithm is the same. You just have to know which processor-specific information to use to trigger the attack," he says. The tricky part is that information is often a closely held secret, he says.

The researchers maintain that targeted attacks like Stuxnet are a major threat, but it's not always so simple for the attacker to be sure what software is running on a targeted machine. "While it can be very difficult to forecast and envisage which kind of applications is likely to be present on the target system (it can be a secret information), the variety in terms of hardware -- and especially as far as processors are concerned -- is far more reduced due to the very limited number of hardware manufacturers," the researchers wrote in their paper on the malware research.

Hardware malware gives cyberwarfare another weapon. "You can arrange things in such a way that effectively Iran buys a set of computers with Intel processor

of a given type and family. Then you can strike them selectively -- and only these computers -- whatever Iran has installed on those computers, [whether it's] Linux, Windows, or any application," Filiol says.

Marc Maiffret, chief technology officer at eEye Digital Security, says he doesn't see hardware malware posing a major threat anytime soon. "While it is interesting to perform this sort of processor fingerprinting, malware will still need to look at other factors to make sure it is hitting the right target, as there is plenty of overlap in systems and what processors they use," Maiffret says. "To put it another way, I think we will continue to see targeting happening more in the way that Stuxnet did it than via processor fingerprinting."

Filiol, meanwhile, says he and his colleagues decided to publish part of their research to raise awareness about this threat. "Even rogue countries and bad guys are doing research. So attacks using those techniques can strike our own countries. That is why we have decided to publish part of our research: to make people aware of the threat," he says.

The malware could be used to wage Distributed Denial-of-Service (DDoS) and any other attack software malware can execute. The idea is for "far more precise and targeted attacks, at a finer level (surgical strikes) in a large network of heterogeneous machines but with generic malware," the research paper says.

There's no way for a processor manufacturer to mitigate such a targeted attack by "patching," either, "unless manufacturers would accept to use the same computation techniques and the same processor designs," he says. But that's obviously not a realistic option, he says.

A full copy of the research is available here (PDF) for download.

The golden hour of phishing attacks

http://www.net-security.org/secworld.php?id=10244

Posted on 02 December 2010.

Trusteer conducted research into the attack potency and time-to-infection of email phishing attacks. One of their findings was that 50 per cent of phishing victims' credentials are harvested by cyber criminals within the first 60 minutes of phishing emails being received.

Given that a typical phishing campaign takes at least one hour to be identified by IT security vendors, which doesn't include the time required to take down the phishing Web site, they've dubbed the first 60 minutes of a phishing site's existence is the critical 'golden hour'.

The fact that so many Internet users visit a phishing website within such a short period of time means that blocking a phishing Web site - which is sometimes a cracked legitimate site - within this golden hour has become absolutely critical.
During the golden hour, the research suggests that:
More than 50 per cent of stolen credentials are harvested
Within five hours, more than 80 per cent are collated and become usable by cybercriminals

The first 10 hours produce more than 90 per cent of the total credentials that will be stolen by any given phishing site.

Therefore, blocking a phishing site after 5-10 hours is almost irrelevant.
A more effective model would prevent users from being directed to a phishing site and/or prevent them from entering their credentials if they do end up on a criminal site.

"As an industry, our goal should be to reduce the time it takes for institutions to detect they are being targeted by a phishing attack from hours to within minutes of the first customer attempting to access a rogue phishing page. We also need to establish really quick feeds into browsers and other security tools, so that phishing filters can be updated much more quickly than they are today. This is the only way to swiftly takedown phishing websites, protect customers, and eliminate the golden hour," said Amit Klein, Trusteer's CTO.

Microsoft warns on IE browser bug

http://www.bbc.co.uk/news/technology-12067295

Microsoft's workaround for the IE bug will not protect all users of its web browser.

Microsoft has issued a warning about a serious vulnerability in all versions of its Internet Explorer (IE) browser.

If exploited by a booby-trapped webpage the bug would allow attackers to take control of an unprotected computer.

Code to exploit the bug has already been published though Microsoft said it had no evidence it was currently being used by hi-tech criminals.

A workaround for the bug has been produced while Microsoft works on a permanent fix.

Code injection

The bug revolves around the way that IE manages a computer's memory when processing Cascading Style Sheets - a widely used technology that defines the look and feel of pages on a website.

Hi-tech criminals have long known that they can exploit IE's memory management to inject their own malicious code into the stream of instructions a computer processes as a browser is being used. In this way the criminals can get their own code running and hijack a PC.

Microsoft has produced updates that improves memory management but security researchers discovered that these protection systems are not used when some older parts of Windows are called upon.

In a statement Microsoft said it was "investigating" the bug and working on a permanent fix. In the meantime it recommended those concerned use a protection system known as the Enhanced Mitigation Experience Toolkit.

Installing and applying the toolkit may require Windows XP users to update the version of the operating system they are using. But even if they do that some of the protection it bestows on Windows 7 and Vista users will not be available. "We're currently unaware of any attacks trying to use the claimed vulnerability or of customer impact," said Dave Forstrom, the director of Microsoft's Trustworthy Computing group, in a statement.

"As vulnerabilities go, this kind is the most serious as it allows remote execution of code," said Rik Ferguson, senior security analyst at Trend Micro, "This means the attacker can run programs, such as malware, directly on the victim's computer."

He added: "It is highly reminiscent of a vulnerability at the same time two years ago which prompted several national governments to warn against using IE and to switch to an alternative browser."

Security researcher warns on fake trojan removal kit

30 November 2010

http://www.infosecurity-magazine.com/view/14302/security-researcher-warns-on-fake-trojan-removal-kit/

Security researcher Christopher Boyd has issued a warning about a fake trojan removal kit that infects Windows users with the ThinkPoint Rogue malware. Writing in his security blog last night, Boyd - aka Paperghost on Twitter and other sites - says that the `Windows Trojan Removal Kit' effectively hijacks users PCs using the ThinkPoint Rogue malware.

This malware, the Sunbelt Software/GFI Software researcher says, only has a close to 50% detection rate in the IT security software stakes.
The file, he says, is currently being offered up by your typical 'fake security scan' pages, such as microsoftwindowssecurity152(dot)com.

"Those familiar with this particular rogue will be aware that it tends to stick with domains similar to the one above", he said.
Installing the executable can potentially give you a bit of a headache, he goes on say, with what would appear to the average user to be fake 'Blue Screens of Death' and payment nag screens.

The good news is that Boyd has posted details on his blog about to workaround the supposed locked up desktop and how the malware appears to be flagging itself as Trojan.Win32.Generic.pak!cobra, a malware infection that was originally discovered at the start of this year.

This article is featured in:

Internet and Network Security • Malware and Hardware Security

JANUARY IN COUNTERINTELLIGENCE HISTORY

- January, 1944: Velvalee Dickinson's spy ring for Japan was ended. In writing letters about dolls, she hid messages about damages, repairs, and itineraries of U.S. Naval vessels. She plead guilty to censorship violations and received a 10-year sentence.
- January 1st, 1945: FBI Director Hoover first publicly announced to capture of two German spies. Landing from a submarine at Point Hancock, Maine, William Curtis Colepaugh and Erich Gimpel were captured by the FBI on 11/29/1944.

- January 1st, 1987: U.S. Marine Corp Moscow Embassy security guard Clayton Lonetree is arrested for his involvement with a female KGB agent.
- January 1st, 1999: Theresa Marie Squillacote and her husband Kurt Alan Stand, were convicted of espionage and sentenced to 21 and 17 tears respectively. An associate, James Michael Clark, received a 12 year prison sentence.
- January 2nd, 1992: Former FBI Translator, Douglas Tsou, is sentenced to 10 years for espionage.
- January 4th, 1949: An investigation was initiated on Department of Justice employee Judith Coplon on suspicion of espionage. She was observed with Soviet national Valentine Gubitchev. Decryption of Soviet signals, by the NSA as a part of the Venona Project, identified Coplan as a Soviet agent codenamed SIMA. Coplan and Gubitchev were arrested together in march 1949.
- January 5th, 2000: Four Pillars Enterprises, a Taiwanese company, was fined $5 million dollars for stealing trade secrets from Avery Dennison Corporation. This was the first time a foreign company had been convicted under the Economic espionage Act of 1996. For eight years, Four Pillars had secretly paid an Avery research scientist to provide them with confidential formulas and technical information.
- January 6th, 1942: President Roosevelt directed the FBI to be responsible for Foreign Intelligence work in the Western Hemisphere, thus originating the work of the Special Intelligence Service.
- January 7th, 1977: Andrew Daulton Lee, the "Snowman" of the "Falcon and the Snowman" spy duo, was arrested at the U.S. Mexican border and found to be in possession of microfilm containing secret U.S. materials.
- January 8th, 1998: former U.S. Army sergeant Clyde Lee Conrad, convicted of espionage in 1990 for selling NATO and American secrets to the Soviet bloc, died in a German prison where he was serving a life sentence.
- January 31st, 1978: US Information Agency employee Ronald Humphrey and Vietnamese national David Truong were arrested and charged with espionage on behalf of Viet Nam. Humphrey was ultimately sentenced to 15 years for espionage and other charges.

PRESENTATIONS AND OUTREACH

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

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

Our Solution: to foster communication and build awareness through partnerships with key public and private entities, by educating, and enabling our partners to identify what is at counterintelligence risk and how to protect it. We call it "knowing your domain"—identifying the research, information and technologies that are targeted by our adversaries, and establishing an ongoing dialog and information exchange with partners, the goal of which is to change behaviors and reduce opportunities that benefit the opposition's efforts.

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

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

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

The FBI's Domain/Strategic Partnership Program seeks to interface with private industry, high tech companies, research institutes, any stakeholder and/or contractor that design, develop, produce, and distribute critical information and technologies. Our job is to establish contact with these "Domain entities" in our territory, and assist them to better understand the foreign intelligence threat, and improve their ability to institute protective mechanisms. In addition to hosting an annual Research Technology Protection (RTP) Conference for security professionals, we also provide security awareness threat

briefings to our defense contractor partners, high tech companies and research institutes. To schedule CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

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

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000