FBI TAMPA CI STRATEGIC PARTNERSHIP NEWSLETTER

August 1, 2011
Volume 3 Issue 8

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

INSIDE THIS ISSUE:

Individuals interested in subscribing to this publication, or interested in further information, should send an email to James "Pat" Laflin at James.Laflin@ic.fbi.gov
For additional information please call Patrick Laflin 813-253-1029

COUNTERINTELLIGENCE (CI) TRENDS

Best Practices for Keeping Your Home Network Secure; Some Suggestions on Dealing with a Cyber Attack; Please read about the FBI's partnership with the Aerospace, Defense, and Information Technology sectors; For those of you interested in negating and preventing the so-called INSIDER THREAT

Best Practices for Keeping Your Home Network Secure

Growing penetration of computer systems maintained and operated by cleared defense contractors, businesses, financial institutions, universities, and government, among many other entities is a major concern. Of equal concern of readers should be the protection and security of home networks. Many of you connect to work systems or work email systems from your home networks. The principles described below have been promulgated by the National Security Agency. These are excellent recommendations and could help prevent computer intrusions onto your home networks. Those of you working at smaller companies and organizations may also want to discuss these recommendations with your work Information-Technology staff and implement some or all of these measures on your office or business networks.

This document, in its original form, complete with illustrations and links may be obtained at the below link:

http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf

It is also located on the National Counterintelligence Executive web site at www.ncix.gov .

Those of you with responsibilities or interests in these areas are encouraged to view this publication in its original .pdf format.

Best Practices for Keeping Your Home Network Secure

The cyber threat is no longer limited to your office network and work persona. Adversaries realize that targets are typically more vulnerable when operating from their home network since there is less rigor associated with the protection, monitoring, and maintenance of most home networks. Home users need to maintain a basic level of network defense and hygiene for both themselves and their family members when accessing the Internet.

Host-Based Recommendations

Windows Host OS

1. Migrate to a Modern OS and Hardware Platform

Both Windows 7 and Vista provide substantial security enhancements over earlier Windows workstation operating systems such as XP. Many of these security features are enabled by default and help prevent many common attack vectors. In addition, implementing the 64-bit mode of the OS on a 64-bit hardware platform substantially increases the effort of an adversary to attain a system or root compromise. For any Windows-based OS, verify that Windows Update is configured to provide updates automatically.

2. Install a Comprehensive Host-Based Security Suite

A comprehensive host-based security suite provides support for anti-virus, anti-phishing, safe browsing, Host-based Intrusion Prevention System (HIPS), and firewall capabilities. These services work collaboratively to provide a layered defense against most common threats. Several security suites today provide access to a cloud-based reputation service for leveraging corporate knowledge and history of malware and domains. Remember to enable any automated update service within the suite to keep signatures up-to-date.

3. Limit Use of the Administrator Account

The first account that is typically created when configuring a Windows host for the first time is the local administrator account. A nonprivileged "user" account should be created and used for the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and reconfigure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host. Within Vista or Windows 7, administrative credentials can be easily accessed by right clicking on any application, selecting the "Run as Administrator" option, then providing the appropriate administrator password. Furthermore, all passwords associated with accounts on the host should be at least 10 characters long and be complex (include upper case, lower case, numbers, special characters).

4. Use a Web Browser with Sandboxing Capabilities

Several currently available third party web browsers now provide a sandboxing capability that can contain malware during execution thereby insulating the host operating system from exploitation. Most of these web browsers also provide a feature to auto-update or at least notify you when updates are available for download. Also, promising approaches that move the web browser into a virtual machine (VM) are starting to appear on the market but are not yet ready for mass consumer use.

5. Update to a PDF Reader with Sandboxing Capabilities

A sandbox provides protection from malicious code that may be contained in a PDF file. PDF files have become a popular technique for delivering malicious executables. Several commercial and open source PDF readers now provide sandboxing capabilities as well as block execution of embedded URLs (website links) by default.

6. Migrate to Microsoft Office 2007 or Later

If using Microsoft Office products for email, word processing, spreadsheets, presentations, or database applications, upgrade to Office 2007 or later and its XML format for storing documents. By default, the XML file formats do not execute embedded code when opened within Office 2007 or later products thereby protecting the user from malicious code delivered via Office documents. The Office 2010 suite also provides "Protected View" mode which opens documents in read-only mode thereby potentially minimizing the impact of a malicious file.

7. Keep Application Software Up-to-Date

Most home users do not have the time or patience to verify that all applications installed on their workstation are fully patched and up to-date. Since many applications do not have an automated update feature, attackers frequently target these applications as a means to exploit a targeted host. Several products exist in the market which will quickly survey the software installed on your workstation and indicate which applications have reached end-of-life, require a patch, or need updating. For some products, a link is conveniently provided in the report to download the latest update or patch.

8. Implement Full Disk Encryption (FDE) on Laptops

Windows 7 Ultimate as well as Vista Enterprise and Ultimate provide support for Bitlocker Full Disk Encryption (FDE) natively within the OS. For other versions of

Windows, third party FDE products are available that will help prevent data disclosure in the event that a laptop is lost or stolen.

Apple Host OS

1. Maintain an Up-to-Date OS

Configure any Mac OS X system to automatically check for updates. When notified of an available update, provide privileged credentials in order to install the update. The Apple iPad should be kept up-to-date as well and requires a physical connection (e.g., USB) to a host running iTunes in order to receive its updates. A good practice is to connect the iPad to an iTunes host at least once a month or just prior to any travel where the iPad will be used.

2. Keep Third Party Application Software Up-to-Date

Periodically check key applications for updates. Several of these third party applications may have options to automatically check for updates. Legacy applications may require some research to determine their status.

3. Limit Use of the Privileged (Administrator Account)

The first account that is typically created when configuring a Mac host for the first time is the local administrator account. A non-privileged "user" account should be created and used for the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and reconfigure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host.

4. Enable Data Protection on the iPad

The data protection feature on the iPad enhances hardware encryption by protecting the hardware encryption keys with a pass code. The pass code can be enabled by selecting "Settings," then "General", and finally "Pass code." After the pass code is set, the "Data protection is enabled" icon should be visible at the bottom of the screen. For iPads that have been upgraded from iOS 3, follow the instructions at: http://support.apple.com/kb/HT4175 .

5. Implement FileVault on Mac OS Laptops

In the event that a Mac laptop is lost or stolen, FileVault (available in Mac OS X, v10.3 and later) can be used to encrypt the contents of a user's home directory to prevent data loss.

Network Recommendations

1. Home Network Design

The Internet Service Provider (ISP) may provide a cable modem with routing and wireless capabilities as part of the consumer contract. To maximize the home user's administration control over the routing and wireless device, deploy a separate personally-owned routing device (a) that connects to the ISP provided router/cable modem. Figure 1 (SEE ORIGINAL WEB POSTING AT HYPERLINK) depicts a typical home network configuration that provides the home user with the network infrastructure to support multiple systems as well as wireless networking and IP telephony services (b).

2. Implement WPA2 on Wireless Network

The wireless network should be protected using Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy). Using current technology, WEP encryption can be broken in minutes (if not seconds) by an attacker, which afterwards allows the attacker to view all traffic passed on the wireless network. It is important to note that older client systems and access points may not support WPA2 and will require a software or hardware upgrade. When researching for suitable replacement devices, ensure that the device is WPA2-Personal certified.

3. Limit Administration to Internal Network

Administration of home networking devices should be from the internal-facing network. When given the option, external remote administration should be disabled for network devices. Disabling remote administration prevents an attacker from changing and possibly compromising the home network.

Figure 1: Typical SOHO Configuration (SEE ORIGINAL WEB POSTING AT HYPERLINK)

4. Implement an Alternate DNS Provider

The Domain Name Servers (DNS) provided by the ISP typically don't provide enhanced security services such as the blocking and blacklisting of dangerous

and infected web sites. Consider using either open source or commercial DNS providers to enhance web browsing security.

5. Implement Strong Passwords on all Network Devices

In addition to a strong and complex password on the wireless access point, a strong password needs to be implemented on any network device that can be managed via a web interface. For instance, many network printers on the market today can be managed via a web interface to configure services, determine job status, and enable features such as email alerts and logging.

Operational Security (OPSEC)/Internet Behavior

Recommendations

1. Traveling with Personal Mobile Devices

Many establishments (e.g., coffee shops, hotels, airports, etc.) offer wireless hotspots or kiosks for customers to access the Internet. Since the underlying infrastructure is unknown and security is often lax, these hotspots and kiosks are susceptible to adversarial activity.

The following options are recommended for those with a need to access the Internet while traveling:

a. Mobile devices (e.g., laptops, smart phones) should utilize the cellular network (e.g., mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.

b. Regardless of the underlying network, users can setup tunnels to a trusted VPN service provider. This option can protect all traffic between the mobile device and the VPN gateway from most malicious activities such as monitoring.

c. If using a hotspot is the only option for accessing the Internet, then limit activities to web browsing. Avoid accessing services that require user credentials or entering personal information. Whenever possible, maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time. If a laptop must be left behind in a hotel room, the laptop should be powered down and have Full Disk Encryption enabled as discussed above.

2. Exchanging Home and Work Content

Government maintained hosts are generally configured more securely and also have an enterprise infrastructure in place (email filtering, web content filtering, IDS, etc.) for preventing and detecting malicious content. Since many users do not exercise the same level of security on their home systems (e.g., limiting the use of administrative credentials), home systems are generally easier to compromise. The forwarding of content (e.g., emails or documents) from home systems to work systems either via email or removable media may put work systems at an increased risk of compromise. For those interactions that are solicited and expected, have the contact send any work-related correspondence to your work email account.

3. Storage of Personal Information on the Internet

Personal information which has traditionally been stored on a local computing device is steadily moving to the Internet cloud. Examples of information typically stored in the cloud include webmail, financial information, and personal information posted to social networking sites. Information in the cloud is difficult to remove and governed by the privacy policies and security of the hosting site. Individuals who post information to these web based services should ask themselves "Who will have access to the information I am posting?" and "What controls do I have over how this information is stored and displayed?" before proceeding. Internet users should also be aware of personal information already published online by periodically searching for their personal information using popular Internet search engines.

4. Use of Social Networking Sites

Social networking sites are an incredibly convenient and efficient means for sharing personal information with family and friends. This convenience also brings some level of risk; therefore, social network users should be cognizant of what personal data is shared and who has access to this data. Users should think twice about posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you. If available, consider limiting access to posted personal data to "friends only" and attempt to verify any new sharing requests either by phone or in person. When receiving content (such as third-party applications) from friends or new acquaintances, be wary that many recent attacks have leveraged the ease with which content is generally accepted within the social network community. This content appears to provide a new capability, when in fact there is some malicious component that is rarely apparent to the typical user. Also, several social networking sites now provide a feature to opt-out of exposing your personal information to Internet search engines. A good recommendation is to

periodically review the security policies and settings available from your social network provider to determine if new features are available to protect your personal information.

5. Enable the Use of SSL Encryption

Application encryption (also called SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit. SSL also prevents people who can see your traffic (for example at a public WiFi hotspot) from being able to impersonate you when logging into web based applications (webmail, social networking sites, etc.). Whenever possible, web-based applications such as browsers should be set to force the use of SSL. Financial institutions rely heavily on the use of SSL to protect financial transactions while in transit. Many popular applications such as Facebook and Gmail have options to force all communication to use SSL by default. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser.

6. Email Best Practices

Personal email accounts, either web-based or local to your host, are common attack targets.

The following recommendations will help reduce your exposure to email-based threats:

a. In order to limit exposure both at work and home, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.

b. Setting out-of-office messages on personal email accounts is not recommended, as this can confirm to spammers that your email address is legitimate and also provide awareness to unknown parties as to your activities.

c. Always use secure email protocols if possible when accessing email, particularly if using a wireless network. Secure email protocols include Secure IMAP and Secure POP3. These protocols, or "always use SSL" for web-based email, can be configured in the options for most email clients. Secure email prevents others from reading email while in transit between your computer and the mail server.

d. Unsolicited emails containing attachments or links should be considered suspicious. If the identity of the sender can't be verified, consider deleting the

email without opening. For those emails with embedded links, open your browser and navigate to the web site either by its well-known web address or search for the site using a common search engine. Be wary of an email requesting personal information such as a password or social security number. Any web service that you currently conduct business with should already have this information.

7. Password Management

Ensure that passwords and challenge responses are properly protected since they provide access to large amounts of personal and financial information. Passwords should be strong, unique for each account, and difficult to guess. A strong password should be at least 10 characters long and contain multiple character types (lowercase, uppercase, numbers, and special characters). A unique password should be used for each account to prevent an attacker from gaining access to multiple accounts if any one password is compromised. Disable the feature that allows programs to remember passwords and automatically enter them when required. Additionally, many online sites make use of password recovery or challenge questions. The answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.

8. Photo/GPS Integration

Many phones and some new point-and-shoot cameras embed the GPS coordinates for a particular location within a photo when taken. Care should be taken to limit exposure of these photos on the Internet, ensure these photos can only be seen by a trusted audience, or use a third-party tool to remove the coordinates before uploading to the Internet.

These coordinates can be used to profile the habits and places frequented for a particular individual, as well as provide near-real time notifications of an individual's location when uploaded directly from a smart phone. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Enhanced Protection Recommendations

The following recommendations require a higher level of administrative skills to implement and maintain on home networks than the previous recommendations. These recommendations provide additional layers of security but may impact your web browsing experience or require some iteration to adjust settings to the appropriate thresholds.

1. Enhanced Wireless Router Configuration Settings

Additional protections can be applied to the wireless network to limit access. The following security mechanisms do not protect against the experienced attacker, but are very effective against a less experienced attacker.

a. MAC address or hardware address filtering enables the wireless access point to only allow authorized systems to associate with the wireless network. The hardware address for all authorized hosts must be configured on the wireless access point.

b. Limiting the transmit power of the wireless access point will reduce the area of operation (signal strength) of the wireless network. This capability curtails the home wireless network from extending beyond the borders of a home (e.g., parking lot or adjacent building).

c. SSID cloaking is a means to hide the SSID, the name of a wireless network, from the wireless medium. This technique is often used to prevent the detection of wireless networks by war drivers. It is important to note that enabling this capability prevents client systems from finding the wireless network. Instead, the wireless settings must be manually configured on all client systems.

d. Reducing the dynamic IP address pool or configuring static IP addresses is another mechanism to limit access to the wireless network. This provides an additional layer of protection to MAC address filtering and prevents rogue systems from connecting to the wireless network.

2. Disable Scripting Within the Web Browser

If using third party web browsers such as Firefox or Chrome, use NoScript (Firefox) or NotScript (Chrome) to prevent the execution of scripts from untrusted domains. Disabling scripting can cause usability issues, but is an effective technique to reduce web born attacks.

3. Enable Data Execution Prevention (DEP) for all Programs

By default, DEP is only enabled for essential Windows programs and services. Some third party or legacy applications may not be compatible with DEP, and could possibly crash when run with DEP enabled. Any program that requires DEP to execute can be manually added to the DEP exemption list, but this requires some technical expertise.

Additional Published Guidance

Social Networking
http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf

Mitigation Monday #2 – Defense Against Drive By Downloads
http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf

Mitigation Monday – Defense Against Malicious E-mail Attachments
http://www.nsa.gov/ia/_files/factsheets/MitigationMonday.pdf

Mac OSX 10.6 Hardening Tips
http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

Data Execution Prevention
http://www.nsa.gov/ia/_files/factsheets/I733-TR-043R-2007.pdf

---

The following are some unclassified suggestions recently published by DHS discussing an organizations possible responses to some kind of cyber attacks or incidents. This material is not directive or guidance, it merely reflects some potential courses of action in the event of a cyber related incident.

Some Suggestions on Dealing with a Cyber Attack

Should a cyber attack occur, ensure backup and recovery procedures are in place and enabled. Be prepared to execute a full spectrum defensive plan that includes contact information for external sources to draw on for assistance. Collect and centrally manage detailed aspects of the attack so you can provide accurate information to Operations, Security, and Law Enforcement personnel as necessary. Such a plan may also include materials identifying who to contact at your Internet service provider, possibly via alternate means, and at any time of day or night to minimize the duration and effect of a cyber attack. Similarly, have contact information readily available for public and private entities to draw on for assistance: the NCCIC, US-CERT, FBI Joint Terrorism Task Force, local FBI Field Office, applicable Information Sharing Analysis Center (ISAC), and Sector Specific Agency.

For the situational awareness, below are URLs to the National and Cyber Threat Levels the NCCIC monitors:

NCRAL: Contact NCCIC Watch & Warning (NCCIC@HQ.dhs.gov)

MS-ISAC: http://www.msisac.org/index.cfm MULTISTATE INFORMATION SHARING AND ANALYSIS CENTER

National Terrorism Advisory System: http://www.dhs.gov/alerts NATIONAL TERRORISM ADVISORY SYSTEM

ES-ISAC: http://www.esisac.com/ ELECRICITY SECTOR

FS-ISAC: http://www.fsisac.com/ FINANCIAL SERVICES

IT-ISAC: https://www.it-isac.org/ INFORMATION TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

ADDITIONAL INFORMATION

While the U.S. Government doesn't endorse a particular solution, identifying vendors with experience combating such an attack may reduce the time it takes to get assistance mitigating such an attack and restoring service or operations. Additionally, the US-CERT web page offers a wide variety of technical and non-technical information to make use of both before and after an incident: http://www.us-cert.gov/nav/t01/

A variety of documents with information regarding defensive measures to combat a computer network attack are available at: http://www.cert.org/tech_tips/

Many organizations can suffer financial loss as a result of a cyber attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement.

Data breaches which involve a monetary loss or include a financial nexus such as a compromise to your financial, credit or debit accounts, or personal information can be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.

http://www.secretservice.gov/field_offices.shtml

U.S. persons and companies interested in pursuing an investigation of a cyber attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact information web page:

http://www.fbi.gov/contactus.htm

Non-U.S. entities may need to discuss malicious cyber activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

U.S. Federal Government Departments and Agencies should report cyber attacks and incidents to US-CERT. Non-U.S. F/S/L/T/T Government Departments and Agencies interested in determining the source of certain types of cyber attacks may require the cooperation of your internet service provider and the administrator of the attacked networks. Tracking an intruder this way may not always be possible. If you are interested in trying do to so, contact your service provider directly, as the US-CERT is not able to provide this type of assistance.

We do encourage you to report your experiences, however. This helps the NCCIC and US-CERT understand the nature and scope of security incidents on the Internet, and we may be able to relate your report to other activity that has been reported to us.

Please read about the FBI's partnership with the Aerospace, Defense, and Information Technology sectors of business and industry within the United States. Full details can be read at the below link.

http://www.fbi.gov/about-us/investigate/counterintelligence/us-business

Some of the highlights of this partnership (as included at the above link) are illustrated below:

If invited, the FBI will collaborate with a business on a broad array of topics relating to:

- Cyber security
- Economic espionage
- Trade secret / intellectual property protection
- Sensitive and classified information (i.e. is export controlled or has publication restrictions)
- Keeping employees from being recruited by foreign intelligence services or terrorist organizations (the insider threat)
- "Hardening the target" around technologies deemed valuable to national security
- Personal and sensitive information (identity theft, fraud, stolen research, etc.)
- Safety and security awareness when traveling abroad

The FBI is also willing to:

- Provide a counterintelligence vulnerability assessment
- Provide awareness training to employees, lawyers, and managers
- Provide brochures and literature about threats
- Serve as a resource for questions and concerns (such as matters involving export controls)
- Provide specific threat information, if available
- Provide invitations to regional counterintelligence meetings with the other businesses, academics, and US intelligence community personnel

What the FBI would like in return:

- Introduction to departments or personnel that could benefit from our message
- Implementation of more robust security procedures, if needed
- Details of suspicious incidents
- Access to subject matter experts to aid FBI investigations
- Willingness to work with the FBI on security concerns
- Tips and feedback about our efforts

If you are interested in discussing any of the preceding, please contact one of the individuals named within this newsletter as FBI Strategic Partnership Program points of contact. We will be more than happy to schedule an appointment with you to discuss these topics in person.

For those of you interested in negating and preventing the so-called INSIDER THREAT (the concept that trusted insiders within an organization pose the greatest risks to the security of an organization and its information), the National Counterintelligence Executive has posted the " Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1".

http://www.ncix.gov/issues/ithreat/csg-v3.pdf

For a small flavor of this publication, please see the below extract. Again, we encourage personnel security professionals and others with interest to link to the .pdf version of this document, located in its entirety at the above link (all 88 pages!!).

INTRODUCTION

In 2005, the first version of the *Common Sense Guide to Prevention and Detection of Insider Threats* was published by Carnegie Mellon University's CyLab. The document was based on the insider threat research performed by

CERT, primarily the *Insider Threat Study* **(1)** conducted jointly with the U.S. Secret Service. It contained a description of twelve practices that would have been effective in preventing or detecting malicious insider activity in 150 actual cases collected as part of the study. The 150 cases occurred in critical infrastructure sectors in the U.S. between 1996 and 2002.

A second edition of the guide was released in July of 2006. The second edition included a new type of analysis – by type of malicious insider activity. It also included a new section that presented a high-level picture of different types of insider threats: fraud, theft of confidential or proprietary information, and sabotage. Also, in addition, it contained new and updated practices based on new CERT insider threat research funded by Carnegie Mellon CyLab **(2)** and the U.S. Department of Defense Personnel Security Research Center. **(3)** Those projects involved a new type of analysis of the insider threat problem focused on determining high-level patterns and trends in the cases. Specifically, those projects examined the complex interactions, relative degree of risk, and unintended consequences of policies, practices, technology, insider psychological issues, and organizational culture over time.

This third edition of the Common Sense Guide once again reflects new insights from ongoing research at CERT. CyLab has funded the CERT Insider Threat Team to collect and analyze new insider threat cases on an ongoing basis. The purpose of this ongoing effort is to maintain a current state of awareness of the methods being used by insiders to commit their attacks, as well as new organizational issues influencing them to attack. This version of the guide includes new and updated practices based on an analysis of approximately 100 recent insider threat cases that occurred from 2003 to 2007 in the U.S.

In this edition of the guide, CERT researchers also present new findings derived from looking at insider crimes in a new way. These findings are based on CERT's analysis of 118 theft and fraud cases, which revealed a surprising finding. The intent of the research was to analyze cases of insider theft and insider fraud to identify patterns of insider behavior, organizational events or conditions, and technical issues across the cases. The patterns identified separated the crimes into two different classes than originally expected:

- Theft or modification of information for financial gain – This class includes cases where insiders used their access to organization systems either to steal information that they sold to outsiders, or to modify information for financial gain for themselves or others.

- Theft of information for business advantage - This class includes cases where insiders used their access to organization systems to obtain

information that they used for their own personal business advantage, such as obtaining a new job or starting their own business.

It is important that organizations recognize the differences in the types of employees who commit each type of crime, as well as how each type of incident evolves over time: theft or modification for financial gain, theft for business advantage, IT sabotage, and miscellaneous (incidents that do not fall into any of the three above categories). This version of the guide presents patterns and trends observed in each type of malicious activity. There have been minor updates to the IT sabotage information in this guide; however, the most significant enhancements in this edition were made to the theft and modification sections.

Some new practices were added in this edition that did not exist in the second edition. In addition, every practice from the second edition has been modified—some significantly, others to a lesser degree—to reflect new insights from the past year's research at CERT. Case examples from the second edition were retained in this edition for the benefit of new readers. However, a *Recent Findings* section was included for all updated practices. It details recent cases that highlight new issues not covered in the previous edition of this guide.

1 See http://www.cert.org/insider_threat/study.html for more information on the *Insider Threat Study*.

2 A report describing the MERIT model of insider IT Sabotage, funded by CyLab, can be downloaded at http://www.cert.org/archive/pdf/08tr009.pdf .

3 A report describing CERT's insider threat research with the Department of Defense can be downloaded from http://www.cert.org/archive/pdf/06tr026.pdf .

ARRESTS, TRIALS AND CONVICTIONS

Brookline Man to Plead Guilty to Foreign Economic Espionage

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

U.S. Attorney's Office

July 21, 2011

District of Massachusetts

(617) 748-3100

BOSTON—A Brookline man has agreed to plead guilty to foreign economic espionage for providing trade secrets over an 18-month period to an undercover agent posing as an Israeli intelligence officer. This is the first prosecution in Massachusetts for foreign economic espionage and only the eighth in the nation.

ELLIOT DOXER, 42, a former Akamai Technologies, Inc. employee, was charged in an information and has agreed to plead guilty to foreign economic espionage for providing Akamai trade secrets to an undercover agent posing as an Israeli intelligence officer. The plea hearing is scheduled for August 29 at 3:15 p.m.

United States Attorney Carmen M. Ortiz said, "Economic espionage poses a tremendous risk, not only to corporate America, but to the safety and well being of our nation's security. I want to thank Akamai Technologies, Inc. for their outstanding cooperation in this matter, which played an important role in assisting law enforcement with bringing Mr. Doxer to justice."

"The Boston area is a worldwide leader of innovative technology and research. Preventing those intent on stealing trade secrets and American technology from local industry leaders, regardless of their motivation, is a high priority for the FBI," said Richard DesLauriers, Special Agent in Charge of the FBI in Boston.

"Mr. Doxer's criminal actions are an affront to the dedicated workers in the thriving technology industry. The arrest of Mr. Doxer is a significant achievement by the FBI and the USAO, District of Massachusetts, to thwart Mr. Doxer's goal of attempting to deprive Akamai Technologies of valuable business technology and confidential business information."

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

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

Included in the trade secret information that DOXER provided the undercover agent were an extensive list of Akamai's customers; contracts between Akamai

and various customers revealing contact, services, pricing, and termination date information; and a comprehensive list of Akamai's employees that revealed their positions and full contact information. DOXER also broadly described Akamai's physical and computer security systems and stated that he could travel to the foreign country and could support special and sensitive operations in his local area if needed.

We also acknowledge the government of Israel for their cooperation in this investigation, and underscore that the information does not allege that the government of Israel or anyone acting on its behalf committed any offense under U.S. laws in this case.

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

That charge will be dismissed as part of the plea agreement. The charge of foreign economic espionage carries a maximum penalty of 15 years in prison, a three-year term of supervised release and a $500,000 fine.

The case is being prosecuted by Assistant U.S. Attorneys William D. Weinreb and Scott Garland respectively in Ortiz's Antiterrorism and National Security Unit and Cybercrimes Unit, and trial attorneys Kathleen Kedian and David Recker of the Department of Justices' Counterespionage Section. Akamai Technologies cooperated fully in the investigation.

The defendant is presumed to be innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

Two Charged with Conspiring to Act as Unregistered Agents of Pakistani Government

http://www.fbi.gov/washingtondc/press-releases/2011/two-charged-with-conspiring-to-act-as-unregistered-agents-of-pakistani-government

U.S. Department of Justice

July 19, 2011 Office of Public Affairs

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

— filed under: Press Release, Washington Field Office Top Stories

WASHINGTON—Two individuals have been charged with participating in a long-term conspiracy to act as agents of the Pakistani government in the United States without disclosing their affiliation with the Pakistani government as required by law.

The charges were announced by Lisa Monaco, Assistant Attorney General for National Security; Neil MacBride, U.S. Attorney for the Eastern District of Virginia; and James McJunkin, Assistant Director in Charge of the FBI Washington Field Office.

Syed Ghulam Nabi Fai, 62, a U.S. citizen and resident of Fairfax, Va., and Zaheer Ahmad, 63, a U.S. citizen and resident of Pakistan, are charged in a one-count criminal complaint in the Eastern District of Virginia. The complaint alleges that the defendants have conspired to: 1) act as an agent of a foreign principal without registering with the Attorney General in violation of the Foreign Agents Registration Act (FARA); and 2) falsify, conceal, and cover up material facts they had a duty to disclose in matters within the jurisdiction of Executive Branch agencies of the U.S. government.

Fai was arrested this morning. Ahmad remains at large and is believed to be in Pakistan. Both face a potential sentence of five years in prison if convicted. "FARA is designed to ensure that the U.S. government and American public know the underlying source of information and identity of persons attempting to influence U.S. policy and laws. The defendants are accused of thwarting this process by concealing the fact that a foreign government was funding and directing their lobbying and public relations efforts in America," said Assistant Attorney General Monaco.

"Mr. Fai is accused of a decades-long scheme with one purpose—to hide Pakistan's involvement behind his efforts to influence the U.S. government's position on Kashmir," said U.S. Attorney MacBride. "His handlers in Pakistan allegedly funneled millions through the Kashmir Center to contribute to U.S. elected officials, fund high-profile conferences, and pay for other efforts that promoted the Kashmiri cause to decision-makers in Washington."

"Foreign governments who try to influence the United States by using unregistered agents threaten our national security," said FBI Assistant Director in Charge McJunkin. "Mr. Fai's alleged conduct illustrates the risk to our fair and open government. The charges underscore the dedication of special agents who enforce laws—like the FARA violations charged here—that are designed to detect and defeat those who attempt to surreptitiously exert foreign influence on our government by using agents who conceal their foreign affiliations."

According to an affidavit filed in support of the criminal complaint, Fai serves as the director of the Kashmiri American Council (KAC), a non-governmental organization located in Washington, D.C., that was founded in 1990 and also goes by the name "Kashmir Center." The KAC describes itself in educational materials as a "not-for-profit organization dedicated to raising the level of knowledge in the United States about the struggle of the Kashmiri people for self-determination."

The affidavit alleges that, although the KAC held itself out to be a Kashmiri organization run by Kashmiris and financed by Americans, the KAC is one of three "Kashmir Centers" that are actually run by elements of the Pakistani government, including Pakistan's military intelligence service, the Inter-Services Intelligence Agency (ISI). The two other Kashmir Centers are in London, England and Brussels, Belgium.

According to the affidavit, a confidential witness told investigators that he participated in a scheme to obscure the origin of money transferred by Pakistan's ISI to Fai to use as a lobbyist for the KAC in furtherance of Pakistani government interests. The witness explained that the money was transferred to Fai through Ahmad, an American living in Pakistan. A second confidential witness told investigators that the ISI created the KAC to propagandize on behalf of the government of Pakistan with the goal of uniting Kashmir. This witness said ISI's sponsorship and control of KAC were secret and that ISI had been directing Fai's activities for the past 25 years.

When questioned by the FBI about these relationships in March 2007, Fai allegedly stated that he had never met anyone who identified himself as being affiliated with the ISI. In March 2010, the Justice Department sent Fai a letter notifying him of his possible obligation to register as a foreign agent with the Justice Department. In his written response to the Justice Department, Fai asserted that neither he nor KAC had ever engaged in any activities for or provided any services to Pakistan or any foreign entity. In a March 2011 interview with the FBI, Fai again denied having any relationship with anyone in the Pakistani government.

The affidavit alleges that Fai has acted at the direction of and with the financial support of the Pakistani government for more than 20 years. The affidavit alleges that four Pakistani government handlers have directed Fai's U.S. activities and that Fai has been in touch with his handlers more than 4,000 times since June 2008. Fai's handlers have also allegedly communicated with Ahmad regularly.

For example, the affidavit alleges that Fai repeatedly submitted annual KAC strategy reports and budgetary requirements to his Pakistani government

handlers for approval. One document entitled "Plan of Action of KAC/Kashmir Center for Fiscal Year 2009" laid out Fai's intended strategy to secure U.S. Congressional support in order to encourage the Executive Branch to support self-determination in Kashmir; his strategy to build new alliances in the State Department, the National Security Council, the Congress and the Pentagon, and to expand KAC's media efforts.

According to the affidavit, Fai also set forth KAC's projected budgetary requirements from the Pakistani government for 2009, including $100,000 for contributions to members of Congress. There is no evidence that any elected official who received financial contributions from Fai or the KAC was aware that the money originated from any part of the Pakistani government.

According to the affidavit, Fai and the KAC have received at least $4 million, from the Pakistani government since the mid-1990s through Ahmad and his funding network. The money is allegedly routed to Fai through Ahmad and a network of other individuals connected to Ahmad. Ahmad allegedly arranges for his contacts in the United States to provide money to Fai in return for repayment of those amounts in Pakistan.

To date, neither Fai nor Ahmad nor the KAC has registered as an official agent of the Pakistani or Kashmiri governments with the Attorney General as required by FARA.

This investigation is being conducted by the FBI's Washington Field Office. The prosecution is being handled by Assistant U.S. Attorneys Gordon Kromberg and Daniel Grooms of the U.S. Attorney's Office for the Eastern District of Virginia and Trial Attorney John Gibbs of the Counterterrorism Section of the Justice Department's National Security Division.

The public is reminded that an indictment and criminal complaint contain mere allegations and that defendants are presumed innocent unless and until proven guilty.

Phony Army Commander Pleads Guilty, Sentenced

http://da.co.la.ca.us/mr/062911a.htm

June 29, 2011

FOR IMMEDIATE RELEASE

Contacts: Sandi Gibbons, Public Information Officer Jane Robison, News Secretary; Shiara Dávila, Assistant PIO

(213) 974-3525

POMONA – The self-appointed "Supreme Commander" of a phony Army unit who outfitted more than 200 recruits with uniforms and provided them bogus documents for a fee pleaded guilty today and was sentenced to prison, the District Attorney's office announced.

Yupeng Deng, a 51-year-old Chinese national from El Monte, pleaded guilty to three felony counts -- theft by false pretenses, manufacturing deceptive government documents and counterfeit of an official government seal, said Deputy District Attorney Lalit Kundani.

In a separate case, Deng also pleaded guilty to one count of possession of child pornography stemming from a search warrant executed at his home.

Deng, who also goes by David Deng, was immediately sentenced by Judge Jack Hunt to three years in state prison and ordered to pay restitution. The amount will be determined later, although Kundani said estimates are around $200,000. In exchange for his plea, the remaining 10 counts were dismissed, Kundani said. Special Agents with the FBI and the Defense Criminal Investigative Service jointly investigated the case and presented it to the D.A.'s office. Several agencies assisted during the investigation, including the Los Angeles County Sheriff's Department, United States Customs and Immigration Service, Immigration and Customs Enforcement and the United States Army.

Deng created a fake unit he called the U.S. Army/Military Special Forces Reserve unit ("MSFR") in October 2008. He recruited more than 200 Chinese nationals around the country and charged them initiation fees ranging from $300 to $450 with renewal fees set at $120 each year. Recruits could increase their rank in the "MSFR" by making cash donations to the defendant, prosecutors said.

Recruits, who received fraudulent military ID cards in addition to Army uniforms, were told that belonging to the bogus unit was a path to U.S. citizenship. Deng decorated his Temple City office to look like an official U.S. military recruiting center. He used the office to conduct military training and indoctrination, authorities said. He also had MSFR offices in Oakland and Atlanta, Ga.

"Yupeng Deng made a hobby of lying about himself," Kundani said. "He called himself the "Supreme Commander" when, in reality, he was the "Supreme Con Artist. He wanted to wear the king's robe, ride on the king's horse and wear the

king's crown but he didn't have the courage to walk a day in the king's shoes. It was easy for him to put on his uniform to get an airline discount, but he certainly wasn't willing to put on a uniform to jump out of fighter plane. This was his idea of patriotism."

Steven Martinez, Assistant Director in Charge of the FBI's Los Angeles Field Office said, "FBI and DCIS agents who investigated the immigrant fraud scheme, as well as the child pornography found in Deng's residence should be commended for the collaborative effort that led to the successful prosecution by the District Attorney's Office.

"In addition to his crime against children, Mr. Deng dishonored the brave men and women of the United States military and defrauded a vulnerable immigrant population, many of whom legitimately hoped and believed they were on a path to American citizenship," Martinez said.

Chris Hendrickson, Special Agent in Charge of the Defense Criminal Investigative Service, Western Field Office, said, "Deng's greed and corrupt practices victimized innocent immigrants and compromised our national security.

"The Defense Criminal Investigative Service places a special focus on protecting our Warfighters both in theater and at home. Deng compromised the safety of our men and women serving in the U.S. military by creating and selling bogus military identification cards, which falsely represented the bearers as members of the U.S. Armed Services. Deng also exploited for profit and power well intentioned immigrants who were conned by Deng into believing they were members of the U.S. Armed Forces and that their service would lead to U.S. citizenship. Finally, Deng's possession of child pornography is reprehensible. This investigation should serve as a warning for those intent on defrauding the U.S. military and harming innocent victims that the DCIS and our law enforcement partners will pursue these crimes relentlessly."

Former Managing Director of PPG Paints Trading (Shanghai) Co., Ltd., Charged with Illegally Exporting High-Performance Coatings To Nuclear Reactor in Pakistan

http://www.justice.gov/usao/dc/news/2011/apr/news.html

U.S. Department of Justice

Ronald C. Machen Jr. United States Attorney for the District of Columbia

Judiciary Center 555 Fourth St. N.W. Washington, D.C. 20530

PRESS RELEASE

FOR IMMEDIATE RELEASE For Information Contact:
Public Affairs (202) 252-6933

Friday, July 8, 2011

WASHINGTON - Xun Wang, a former Managing Director of PPG Paints Trading (Shanghai) Co., Ltd., a wholly-owned Chinese subsidiary of United States-based PPG Industries, Inc., has been indicted on a charge of conspiring to violate the International Emergency Economic Powers Act and the Export Administration Regulations, and other related offenses, announced Ronald C. Machen Jr., U.S. Attorney for the District of Columbia, and Eric L. Hirschhorn, U.S. Department of Commerce Under Secretary for Industry and Security.

Wang, 51 made her initial appearance on July 7, 2011 in the U.S. District Court for the District of Columbia. On June 7, 2011, a federal grand jury in the District of Columbia returned a sealed indictment charging her with one count of conspiracy and three counts of violating export laws under the International Emergency Economic Powers Act (IEEPA). The indictment was unsealed following Wang's arrest.

She is accused of conspiring to export and reexport, and exporting and reexporting specially designed, high-performance epoxy coatings to the Chashma 2 Nuclear Power Plant (Chashma II) in Pakistan, a nuclear reactor owned and/or operated by the Pakistan Atomic Energy Commission, an entity on the Department of Commerce's Entity List.

Wang was arrested on the indictment on June 16, 2011, at Atlanta Hartsfield-Jackson Airport and transferred to the District of Columbia on July 6, 2011. Wang remains in custody pending a detention hearing on July 12, 2011 before United States Magistrate Judge Deborah A. Robinson. She is a Chinese national and lawful permanent resident of the United States. The United States is seeking to have her held without bond pending trial. The indictment is related to the December 21, 2010, guilty plea of PPG Paints Trading (Shanghai) Co., Ltd. ("PPG Paints Trading"), to a four-count information in the U.S. District Court for the District of Columbia. Together, PPG Paints Trading and its parent company, PPG Industries, Inc., paid $3.75 million in criminal and administrative fines and over $32,000 in restitution. The combined amount of criminal and civil fines represented one of the largest monetary penalties for export violations in the history of the U.S. Department of Commerce's Bureau of Industry and Security.

The Pakistan Atomic Energy Commission is the science and technology organization in Pakistan responsible for Pakistan's nuclear program, including the

development and operation of nuclear power plants in Pakistan. In November 1998, following Pakistan's first successful detonation of a nuclear device, the Commerce Department's Bureau of Industry and Security added the Pakistan Atomic Energy Commission, as well as its subordinate nuclear reactors and power plants, to the list of prohibited end users under the Export Administration Regulations.

As a restricted end-user, a United States manufacturer seeking to export or reexport any items subject to the Export Administration Regulations to the Pakistan Atomic Energy Commission, or its nuclear power plants or reactors, would first need to obtain a license from the Department of Commerce in the District of Columbia.

According to the indictment against Wang, in January 2006, PPG Industries sought an export license for the shipments of coatings to Chashma II. In June 2006, the Department of Commerce denied that license application. Following that denial, Wang and her co-conspirators agreed upon a scheme to export and reexport the high-performance epoxy coatings from the United States to Chashma II, via a third-party distributor in People's Republic of China, without first having obtained the required export license from the Department of Commerce.

The indictment further alleges that from around June 2006 through around March 2007, Wang and other co-conspirators intentionally concealed from PPG Industries that the paint would be delivered to Chashma II. Specifically, they falsely stated that the coatings were to be used at a nuclear power plant in China, the export of goods to which would not require a license from the Department of Commerce. The indictment alleges that, through these means, Wang and her coconspirators took part in three shipments of coatings from the United States to Chashma 2 without the required Department of Commerce license.

An indictment is merely a formal charge that a defendant has committed a violation of criminal law and is not evidence of guilt. Every defendant is presumed innocent until, and unless, proven guilty.

This case is being investigated by the Department of Commerce's Bureau of Industry and Security, Office of Export Enforcement, New York Field Office, and prosecuted by Assistant U.S. Attorneys G. Michael Harvey and John Borchert.

11-288

Libertyville Man Arrested for Theft of Trade Secrets from CME Group

http://www.fbi.gov/chicago/press-releases/2011/libertyville-man-arrested-for-theft-of-trade-secrets-from-cme-group

FBI Chicago

July 02, 2011 Special Agent Ross Rice

(312) 829-1199

— filed under: Press Release

A 49-year-old Libertyville resident, who was employed as a senior software engineer with the Chicago based CME Group, was arrested yesterday after being charged with theft of trade secrets. The arrest was announced today by Robert D. Grant, Special Agent in Charge of the Chicago Field Office of the Federal Bureau of Investigation (FBI).

CHUNLAI YANG, who is a naturalized United States citizen, was taken into custody yesterday morning at his CME office, located at 550 West Washington Street in Chicago, without incident, by FBI special agents. YANG was charged in a criminal complaint filed yesterday in U.S. District Court in Chicago with one count of theft of trade secrets, which is a felony offense.

According to the complaint, YANG has been employed at the CME since 2000, and is responsible for writing computer code. Beginning in May of this year, CME security personnel began monitoring YANG's computer activity. They discovered that thousands of files had been downloaded to his computer, and some were then copied to removable storage devices, such as thumb drives. Many of the downloaded files were critical to the operation of the CME group and are considered proprietary in nature and contain protected source code.

Subsequent investigation by the FBI determined that YANG had also been in e-mail contact with the assistant director of the Logistics and Trade Bureau for the Zhangiagang Free Trade Zone. One of the e-mails sent by YANG contained an attachment, which was a CME document containing protected source code and proprietary information.

It was also determined that YANG had booked travel to China on a commercial airline flight, scheduled to depart from O'Hare International Airport on July 7th. YANG appeared before Magistrate Judge Michael T. Mason in Chicago, late yesterday, at which time he was formally charged. YANG was ordered held without bond, pending his next court appearance, which is scheduled for

Wednesday, July 6th. Until then, YANG will be housed at the Metropolitan Correctional Center in Chicago. If convicted of the charge pending against him, YANG faces a possible sentence of up to 10 years' incarceration, a $250,000 fine, and three years of supervised release.

The public is reminded that a complaint is not evidence of guilt and that all defendants in a criminal case are presumed innocent until proven guilty in a court of law.

EDITOR'S NOTE: Copies of the criminal complaints filed in this case are available from the Chicago FBI's press office at (312) 829-1199.

New Jersey-based Defense Contractor Pleads Guilty to Violating Arms Export Control Act, Conspiracy with Chinese Company

http://www.justice.gov/usao/nj/Press/files/Swiss%20Tech%20Plea%20PR.html

FOR IMMEDIATE RELEASE

July 12, 2011

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

Office of Public Affairs

(973) 645-2888

Swiss Technology Inc. Consents to $1.1 Million in Restitution

NEWARK, N.J. – New Jersey-based defense contracting company Swiss Technology, Inc. ("Swiss Tech"), admitted today to conspiring to violate the Arms Export Control Act by exporting U.S. Department of Defense drawings and specifications to the People's Republic of China, U.S. Attorney Paul J. Fishman announced.

Swiss Tech, once located in Newark and now in Clifton, N.J., pleaded guilty through its managing member to an Information charging one count of conspiracy to commit an export control violation. The company entered the guilty plea before U.S. District Judge Jose L. Linares in Newark federal court.

"We simply can't risk that companies trying to manufacture military equipment on the cheap will expose our troops to more danger than they already face," said U.S. Attorney Fishman.

"Our armed forces deserve the very best equipment to perform their missions in these difficult times," said Edward T. Bradley, Special Agent in Charge, Department of Defense, Defense Criminal Investigative Service (DCIS), Northeast Field Office. "Fraudulent practices, designed to illegally enrich a corporation, and which could compromise the integrity and reliability of that vital equipment is inexcusable. The Defense Criminal Investigative Service is committed to vigorously investigating such violations of law."

"This case underscores ICE's commitment to work tirelessly with our law enforcement partners to investigate individuals or corporate organizations that circumvent federal regulations in the name of greed," said Peter T. Edge, Special Agent in Charge of U.S. Immigration and Customs Enforcement's Homeland Security Investigation (ICE HSI) in Newark. "When our troops' safety is put in jeopardy, our national security is also compromised."

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

From August 2004 through June 2009, Swiss Tech entered into contracts with the U.S. Department of Defense (DOD) to manufacture defense articles and parts for use in military operations. Rather than manufacture the parts, Swiss Tech exported DoD drawings, specifications, and sample parts to the People's Republic of China without obtaining a license from the U.S. State Department. The company contracted with a company in the People's Republic of China which manufactured the items at a much cheaper price per unit than they would have cost to make in the United States using domestic product. The items included parts to be used with M4 and M16 rifles and M249 machine guns, some of which were to be used in U.S. military operations.

Swiss Tech admitted that it entered into the agreement with the company in the People's Republic of China for the financial benefit of Swiss Tech and its co-conspirators and to hide its activities from the U.S. government. As a result of the conspiracy, Swiss Tech caused the DoD to sustain losses of more than $1.1 million in connection with the fraudulent contracts.

Under the terms of the plea agreement, Swiss Tech consented to the court ordering restitution in the amount of $1,148,051.80 to the DoD. Sentencing is currently scheduled for November 15, 2011.

U.S. Attorney Fishman credited special agents of DCIS, under the direction of Special Agent in Charge Edward T. Bradley; and ICE HSI, under the direction of

Special Agent in Charge Peter T. Edge, for the investigation leading to the guilty plea. He also thanked attorneys from the U.S. Department of Justice's National Security Division, Counterespionage Section, under the direction of Assistant Attorney General Lisa O. Monaco, for their assistance; as well as DoD's Air Force Office of Special Investigations, under the direction of Special Agent in Charge Mark Walker; and Army Criminal Investigation Division, under the direction of Special Agent in Charge Forrest Woodward.

The government is represented by Assistant U.S. Attorney Zahid N. Quraishi of the U.S. Attorney's Office in Newark.

11-272 **###**

TECHNIQUES, METHODS, TARGETS

A detailed analysis of a Spear-Phishing attack against senior level executives of the Defense Industrial Base is published by Invincea at the below link:

http://www.invincea.com/blog/2011/07/dissecting-an-active-campaign-targeting-america%E2%80%99s-defense-industrial-base-and-intel-communities/

A brief extract of the analysis follows:

The attack starts as an in-bound spear-phish to individuals in the Defense Industrial Base purporting to come from the US Intelligence Advanced Research Projects Activity (IARPA). The spear-phish contains a URL to a zip archive file with a roster of Defense Industrial Base attendees to an IARPA Program conference. The roster is an active list of 163 senior level executives participating in a recent IARPA Project Day, including Directors and Presidents, and CEOs of premier defense and intelligence companies.

- Once the attachment is opened, it presents the promised roster while running another program it extracted — a custom http client beacons a server then signals how long it will go to sleep. It places itself on the list of programs that runs at system startup.

- After a re-boot the custom http client initiates a GET request to a command & control server. The returned page has an encoding in the HTML. It decodes the encoding in memory to produce a new program that it writes to the user's disk. This program is a remote command & control Trojan. Since the encoded program is hosted on a website, this can be updated over time with more sophistication.

- The new Trojan app gives complete control of the victim machine to the adversary. It will also change Internet Settings in the registry to bypass any local proxy settings that may be in place (e.g., for security). It also has built in capability to update the Root Certificates list that can aid in Man-in-the-Middle attacks against SSL based sessions the user may engage in.

- There are other indicators this attack is part of a larger campaign where multiple organizations are targeted. A file with similar characteristics but different type was uploaded to an online analysis platform and the outbound URLs follow the same format as the beaconing URLs presented here.

Please go to the Invincea Blog at the above link for the full and detailed analysis.

An article, discussing the Invincea report is partially extracted below:

New Targeted Attack Campaign Against Defense Contractors Under Way

http://www.darkreading.com/taxonomy/index/printarticle/id/231002455

Researchers at Invincea, ThreatGrid discover stealthy attack that lets attackers quietly steal information from victims

By Kelly Jackson Higgins, Darkreading

Jul 22, 2011 | 04:22 PM

URL - http://www.darkreading.com/taxonomy/index/printarticle/id/231002455

The U.S. Defense industry once again is under siege by cyberspies in an attack that provides a link to a rigged spreadsheet containing a real list of high-level defense industry executives who attended a recent Intelligence Advanced Research Projects Activity (IARPA) event.

A Defense contractor friend of Anup Ghosh, CEO of Invincea, sent him a copy of a targeted yet suspicious email with the attachment he had received unsolicited. "He said he has been a nonstop target of a lot of spear-phishing attempts, but this one was very compelling because it was purported to have names of attendees to a recent IARPA meeting," Ghosh says. It appears that the attackers sent the same email and malicious attachment to the other 163 event attendees, he says.

Please go to http://www.darkreading.com/taxonomy/index/printarticle/id/231002455 to read the full article.

New PDF-Based Targeted Attack against Military Contractors Spotted

http://news.softpedia.com/news/PDF-Based-Targeted-Attack-Against-Military-Contractors-Spotted-212139.shtml

July 18th, 2011, 20:11 GMT| By Lucian Constantin

Security researchers from F-Secure have spotted a new PDF-based email attack that appears to target people working in the defense industry.

According to the Finnish antivirus vendor, the attack was intercepted last week and is still ongoing. It uses the 2012 AIAA Strategic and Tactical Missile Systems Conference as lure…

Please go to the above web link to view this article in its entirety.

Suspected Skimming Activity Spans Three Counties Credit Card Skimming Operation

http://www.highlandssheriff.org/PressReleases/Press%20News%20Release%20Credit%20Card%20Fraud%2007082011%20_2_.pdf

Highlands County Sheriff's Office
Sheriff Susan Benton
434 Fernleaf Avenue
Sebring, Florida 33870
863-402-7200

www.highlandssheriff.org

Dually Accredited
863-214-2533

NEWS RELEASE
July 8, 2011

Additional Information Just Received
We just received a report from another credit card company listing an additional 46 victims. The total amount of charges from this activity is still being calculated.

Suspected Skimming Activity Spans Three Counties

The Highlands County Sheriff's Office has taken 80 reports to date and estimate that over 100 people in Highlands County alone have been victims of credit card fraud during the recent suspected skimming activity. The losses reported in these cases total slightly over $30,000 according to Highlands County Sheriff's Office Detective Sergeant Brian Kramer. In addition, the Sebring Police Department has added 4 reports with a total of approximately $2100 in losses.

Kramer, Detective Hank Smith and Deputy David Lightsey, representing the Highlands County Sheriff's Office attended a meeting yesterday (July 7, 2011) in Winter Haven with representatives from the Polk County Sheriff's Office, the Florida Department of Law Enforcement (FDLE) and the Secret Service.

At that meeting it was determined that only one skimming device was actually recovered and it was not from Highlands County. In all it is estimated that the total claims will exceed $200,000. Investigation of these crimes will be a joint operation between the several Sheriff's Offices, FDLE and the Secret Service. "Due to the amount of the loss and the span of the crimes we will be attempting to seek federal prosecution," Sergeant Kramer said.

The investigation continues to attempt to identify subjects involved in the capture of card numbers, the manufacturing of fraudulent cards and the use of those cards at various locations across Central Florida. Anyone with information about skimming operations or the manufacture and use of fraudulent cards is asked to call Heartland Crime Stoppers at 1-800-226-TIPS (8477), or on the internet at www.heartlandcrimestoppers.com . Anonymity is guaranteed and you may be eligible for a cash reward.

Nell Hays, CPS
Public Information Officer
Highlands County Sheriff's Office
863-402-7369

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

A white paper, prepared for a U.S. Government commission, discusses in some great detail (88 pages worth) Chinese computer intrusions and attacks against networked systems. The paper is titled:

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation

Prepared for the US-China Economic and Security Review Commission
Some quotes from the paper:

"China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and industry by conducting a long term, sophisticated, computer network exploitation campaign."

"A review of the scale, focus, and complexity of the overall campaign directed against the United States ... strongly suggest that these operations are state-sponsored or supported,"

The white paper in its entirety may be read at the following link:

http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

A brief extract that gives a strong flavor of the white paper's content follows:

Hacker-State Collaboration

While the PRC government appears reluctant to use hacktivism as a CNO tool, there may be a willingness to establish direct relationships with highly skilled individuals or small groups in the hacker community. The PRC government may also be able to engage commercial firms comprised of experienced hackers and operating as nominally legitimate information security groups. This engagement ranges from simple job recruitment by government security ministries on hacker Websites to possible support from blackhat code developers for organized intrusions into US Government and commercial networks.

Commercially-based white hat information security researchers (i.e. those pursuing overt legal research in the field) are developing extensive government customer bases for hardware and possibly software support. Many of the most prominent groups from earlier in the decade and their leaders have either disbanded or transformed themselves into seemingly legitimate security firms. Large groups like Xfocus and Black Eagle Base have reshaped themselves into

commercial operations, albeit in close alignment with state security and information security objectives.

• NSFocus, a prominent commercial information security firm, evolved out of the Green Army Alliance, an early—and prominent—hacker group active from 1997 through 2000; the NSFocus Website still retains logos of the Green Army Alliance and the list of its founding members features some of the most prominent hackers in China.
• XFocus, a commercial information security company that grew from a hacker group, annually co-sponsors XCon, one of the largest "hacker conferences" in China in partnership with NSFocus and Venus Technology.

• Henan Provincial Public Security Bureau authorities shutdown The Patriot Hackers-Black Eagle Base Website and arrested its members in February 2006. The group, however, was operational again six months later under the name Black Eagle Honker Base when its members released a statement claiming that the group vowed to focus its efforts on training people for the state and working to improve the state's network security industry, suggesting a possible cooperative relationship with state authorities as a condition of their release.

• The Black Eagle leadership also expressed appreciation to the State Security Bureau (guojia anquan ju) and the Commission of Science and Technology in National Defense (COSTIND, and now renamed SASTIND82) for the educational guidance they provided to members while in custody. The latter, entity, charged with overseeing national defense industry policy, is not typically referenced in connection with hacker groups or their activities.

Individuals, or possibly groups, engaged in computer network exploitation against US networks have obtained malicious software developed by Chinese underground or black hat programmers. The ability to obtain this custom code indicates that these operators have ties to select members of the hacker underground.

In one demonstrated instance, black hat programmers affiliated with Chinese hacker forums provided malicious software to intruders targeting a US commercial firm in early 2009. The techniques and tools employed by this group or individual are similar to those observed in previous penetration attempts against this same company in the previous year, according to their forensic analysis.

• Forensic analysis also suggests this group is comprised of multiple members of varying skill levels, operating with fixed schedules and standard operating procedures and is willing to take detailed steps to mask their activities on the targeted computer.

• Open source research on the screen name of the coder who created the malware used in the early 2009 attack revealed that the individual is likely a native Chinese speaker who posted a keystroke logging program with rootkit elements to a discussion board on a prominent Chinese hacker group Website known as EvilOctal.

• The coder created the PDF document used as the attachment to carry the malicious software with a tool that is only available in Chinese called FreePic2Pdf, version 1.26; this document was modified to covertly install a zero day exploit that targeted a previously unknown vulnerability in Adobe Acrobat.

• Upon successful installation on the victim system after the user opened the attachment, the Trojan horse malware began periodically attempting to connect with another machine overseas, essentially sending a beacon to let the attackers know that a machine had been successfully attacked. The intruders only completed this connection when they were ready to commence the next phase of the operation via encrypted communications with the victim computer.

• The operators worked in a three shift, 24 hour cycle issuing reconnaissance commands identical to those observed in previous attacks.

• When significant differences were recognized between this computer and previously compromised systems on the same network, the attack team extracted small amounts of data to determine the configuration of security software installed and their ability to access targeted data on the company's network.

• The operators installed a rootkit, which gives the attacker privileged access to a victim computer while remaining undetectable, suggesting the attackers intended long-term covert use of the victim computer. The attackers configured the rootkit to execute upon the next system reboot, effectively hiding the operators' files, programs, network connections and registry settings, however, operator error caused a problem in the rootkit execution and locked the attackers out of the targeted computer, ending the operation, according to forensic analysis.

• The rootkit code is still not publicly available, suggesting that the attacker obtained it directly from the coder or someone with direct access to this individual.

The creator of another zero day exploit used to target US companies in the fall of 2008 developed the code in Chinese and on a machine with Chinese set as the default language indicating that this individual was also likely a native or fluent speaker. Little additional detail about the developer's identity is available from

forensic analysis but it reinforces the assertion that a relationship exists between Chinese black hat programmers and individuals responsible for intrusions into US networks.

• US companies began receiving small waves of spam-like emails with a Microsoft WordPad (.wri) file attachment containing a small piece of malicious software that acted as a Trojan, enabling the attackers to gain complete access to the targeted computers, a hallmark of the computer network exploitation tradecraft attributed to China. The malware exploited a zero day vulnerability in Microsoft's WordPad application.

• The attachment sent in these email attacks contained two components: an English language carrier document that appears to be a generic contract template for a defense firm to use with a sub-contractor, and the Chinese language exploit code inserted inside the carrier document.

• When the recipient of the apparent spam email attempted to open the attached .pdf file, the file installed both the malware and a backdoor service on the targeted machine that was designed to execute the next time the user logged in. The malware, sent in a wave of spearphishing attacks against various US companies, was intended to provide the intruder with the ability to remotely access and control the targeted computers, another common characteristic of computer network exploitation activities attributed to China.

• The newly installed service connects to an external host outside of the targeted company's network and allows the intruder to take control of the victim's machine remotely with the same access and operational capabilities as though they were sitting at the user's keyboard.

Programming bugs in the malware used during the fall 2008 campaign and the intruders' ability to quickly obtain an earlier version as a replacement program, strongly suggests this was the first time the newer version was being used by these attackers. Their ability to obtain a replacement version quickly may be the result of having access to the developer or someone managing a repository of the developer's work. If the latter is true, it implies the existence of a support infrastructure for the individuals targeting US Government and commercial networks. However, this is still speculative and requires further research to corroborate.

• The initial version of the malware was compiled in late October 2008 and used within weeks by the intruders. This short time interval between the date of creation and first use implies that the intruder (or intruders) had the means to obtain customized zero-day malware quickly.

• When they encountered operational problems with the code, the intruders quickly obtained an older version of the malware, compiled in January 2008 and resumed their work with little delay.

Government Recruitment from Hacker Groups

Government efforts to recruit from among the Chinese hacker community and evidence of consulting relationships between known hackers and security services indicates some government willingness to draw from this pool of expertise. It does not imply that authorities have established many such relationships or intends to enlist whole groups for large attacks on US systems.

• Between July 2007 and November 2008, an individual using the screen name "City_93" posted job vacancy announcements for the Ministry of Public Security's First Research Institute (posting a Web address www.fri.com.cn) on the discussion board for EvilOctal.com and XFocus.net, two of the largest and in the case of XFocus, most established hacker forums in China.

• "City_93" eventually posted 10 vacancy notices on Evil Octal between 2007 and 2008 and on both sites engaged in lengthy discussion threads on the application procedures and nature of the job with interested users. The job postings were for entry level programmers with experience in the development and implementation of network security system projects.

• The MPS First Research Bureau provides a variety of science and technology research and development to operational elements of the MPS. The Institute has an information security research group according to its Website.

EXTRACT ENDS

Again, the white paper in its entirety may be read at the following link:

http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

DHS: Imported Tech Tainted with Backdoor Attack Tools

http://www.networkworld.com/community/print/76262

By Ms. Smith

Created Jul 12 2011 - 9:03am

When a Homeland Security official admitted to the threat of destructive coding being embedded in imported software and hardware, it caused quite a stir. Yet backdoor malware is no more a secret than the fact that nation states and rogue criminals target the U.S. "by hacking into proprietary data and other sensitive information."
During testimony before the House Oversight and Government Reform Committee, Rep. Jason Chaffetz, R-Utah, questioned a top DHS official about software and hardware that is built overseas, is shipped into the U.S. and comes embedded with spyware or other code meant for sabotage. Chaffetz asked Greg Schaffer, Homeland Security's Assistant Secretary of the Office of Cybersecurity and Communications, about imported devices that pose "security and intellectual property risks."

THIS ARTICLE MAY BE READ IN ITS ENTIRETY AT THE ABOVE LINK

SecurID users targeted by fake NSA email

http://www.net-security.org/malware_news.php?id=1783

Posted on 25.07.2011

RSA's SecurID token users have recently been targeted with fake emails supposedly coming from the US National Security Agency urging them to update their token code.

The address from which the emails are sent has been spoofed and says "protection@nsa.security.gov", but the offered malicious links take the victim to the national-security-agency.com domain …

Please go to the above link to read this article in its entirety.

AUGUST IN COUNTERINTELLIGENCE HISTORY

- August, 1946: Congress passed the Atomic Energy Act, making the FBI responsible for investigating criminal violations of the act, as well as investigating persons having access to restricted data.
- August, 1969: Bill Ayers described the Weathermen as "revolutionary communists."
- August 1st, 1919: On this date the General Intelligence Division (GID) was created within the Bureau of Investigation (the then name for what finally evolved into what has been known since 1935 as the Federal Bureau of

Investigation). The GID was tasked with collecting evidence and data on revolutionary and radical movements. Among the groups investigated from near the beginning of the GID's creation were the Communist Labor Party of America and the Communist Party of America. Upon its creation, the GID was placed under the direct administrative supervision of J. Edgar Hoover.

- August 7th, 1943: On this date the FBI received an anonymous letter in Russian naming Vasilli Zarubin, Boris Morros, Earl Browder and others as Soviet espionage agents. The letter was apparently sent by a disgruntled Soviet Embassy employee named Vasili Moronov.
- August 15th, 1926: On this date, Special Agents James F. Findlay and A.A. Hopkins arrested Major General Enrique Estrada, former Mexican Secretary of War, in California. Simultaneously, other Special Agents assisted the Border Patrol and local officers to capture Estrada's general staff, infantry, armor, artillery and air force, as they prepared to invade Mexico and seize control of the government of Mexico.
- August 25th, 1936: On this date, having been authorized to do so by President Roosevelt, Cordell Hull, Secretary of State, gave the FBI authority to conduct general intelligence investigations of subversive activities. Under existing appropriations bills, only the Secretary of State could grant the FBI such authority.

PRESENTATIONS AND OUTREACH

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

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

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

The United States is a world's leader in innovation. Consider the breakthrough

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

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

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

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

CI, cyber, security, education, training and awareness briefings, contact the Tampa Domain/SPC.

The Tampa Field Office Counterintelligence Strategic Partnership Program Coordinator:

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

Federal Bureau of Investigation

5525 West Gray Street
Tampa, FL 33609
Phone: 813.253.1000