Ethical Hacking and Countermeasures

Version 6

Module XLVIII

Corporate Espionage by Insiders

News

Chinese trainee goes on trial as French industry fears espionage

Adam Sage in Paris

A Chinese trainee will go on trial in France today charged with pirating her employer's computer system, in a case that has raised Gallic fears over industrial espionage by Beijing.

Li Li Whuang, 24, is accused of copying confidential data from Valeo, the French automotive equipment supplier, on to her personal computer.

Dubbed the Chinese Mata Hari by the French media, she has been portrayed as the symbol of an Asian plot aimed at obtaining secret commercial and technical information. "She was seen as the foot soldier who came to steal France's industrial secrets," Le Parisien newspaper said.

Her arrest in 2005 came as the French authorities set up an Economic Intelligence Unit to help businesses to fight industrial espionage, with China denounced as one of the prime culprits. Counter-espionage experts believe that among the growing number of Chinese students

EXPLORE LAW

- CORPORATE LAW
- PUBLIC LAW
- COLUMNISTS
- LAW PANEL
- STUDENT LAW
- LAW REPORTS
- YOUR SHOUT

TIMES RECOMMENDS

- Future stars of the regions
- Ten laws every employer needs to know
- The UK's most high profile lawyers

MORE LAW NEWS

- OFT attack on drugs distribution deals
- Conrad Black is sentenced to 6½ years in jail – after festive season is over
- Plan to reduce legal fees 'jeopardises terror trials'
- No damages for 'shaken baby' mother
- Legal fears left Atlantic Conveyor defenceless

Source: *http://business.timesonline.co.uk/*

Update: Oracle Says No Settlement Talks In SAP Case

Posted by Eric Savitz

Oracle (ORCL) is not in settlement talks regarding its corporate espionage suit against SAP (SAP) and its TomorrowNow division, Oracle spokesperson Deborah Hellinger said in a statement today. She said that "such discussions are premature."

In a post earlier today, I noted that a federal court judge overseeing Oracle's case had issued an order referring the case to a mediator. But Oracle says that doing that is routine, and that Oracle plans to file an amended complaint with additional claims.

Here is the full text of the statement:

> *Most cases are referred to ADR [alternative dispute resolution], no date for mediation has been set, and we are not currently in settlement discussions. In fact, such discussions are premature. As set forth in Oracle's current claims, it appears that SAP infringed Oracle's intellectual property on a daily basis over a course of many years, in ways that Oracle is only beginning to discover. In addition, Oracle has uncovered a broader program of copyright infringement that is entirely different from the scheme alleged in the current complaint. Based on this evidence, Oracle will file an amended complaint that will include these new claims.*

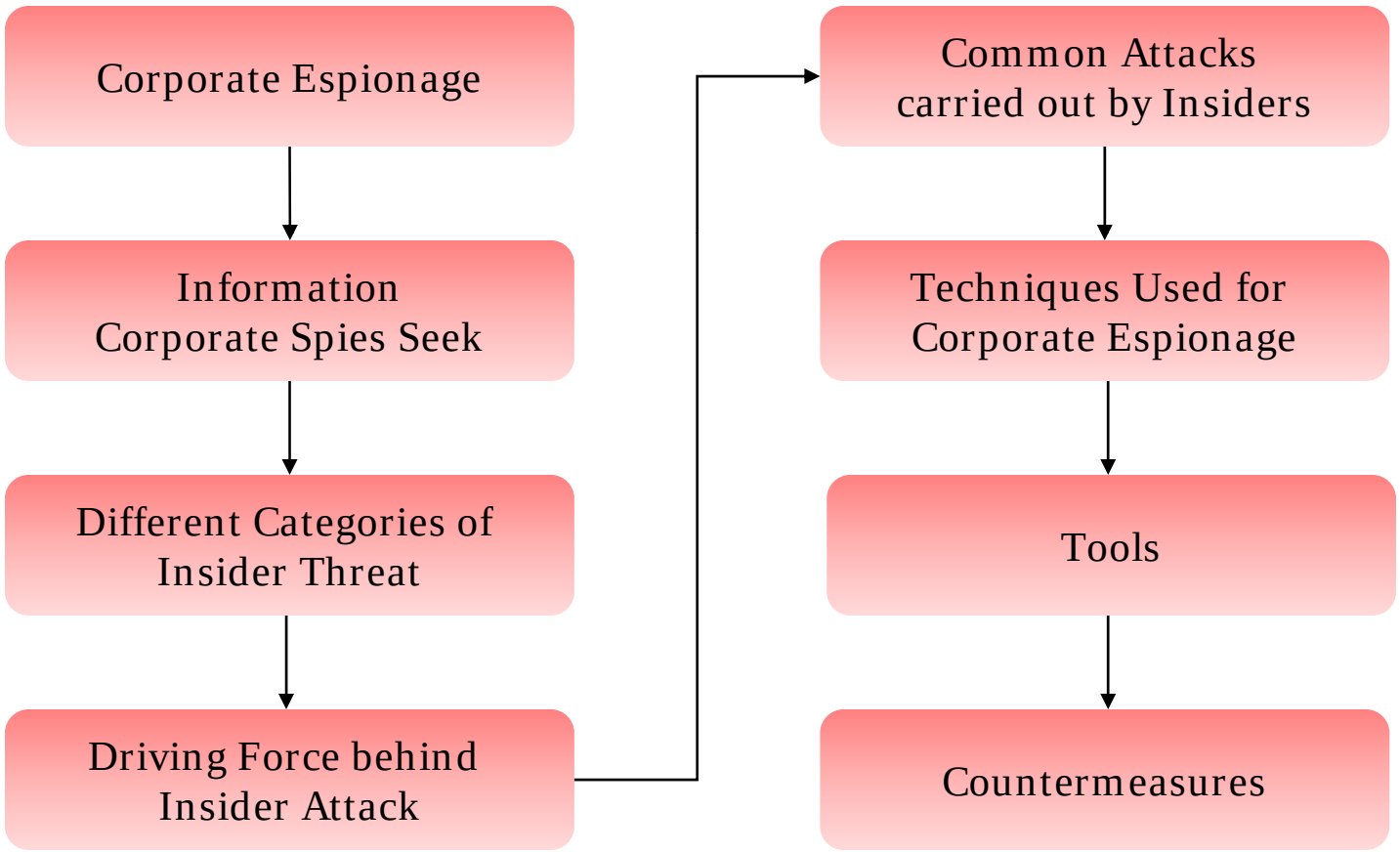
Source: *http://blogs.barrons.com/*

Module Objective

This module will familiarize you with:

- Corporate Espionage
- Information Corporate Spies Seek
- Different Categories of Insider Threat
- Driving Force behind Insider Attack
- Common Attacks carried out by Insiders
- Techniques Used for Corporate Espionage
- Tools
- Countermeasures

Module Flow



Introduction To Corporate Espionage

"Espionage is the use of illegal means to gather information“
Source: www.scip.org

Term ‘Corporate espionage’ is used to describe espionage conducted for commercial purposes on companies, governments, and to determine the activities of competitors

Information Corporate Spies Seek

- Marketing and new product plans
- Source code
- Corporate strategies
- Target markets and prospect information
- Usual business methods
- Product designs, research, and costs
- Alliance and contract arrangements: delivery, pricing, and terms
- Customer and supplier information
- Staffing, operations, and wage/ salary
- Credit records or credit union account information

Insider Threat

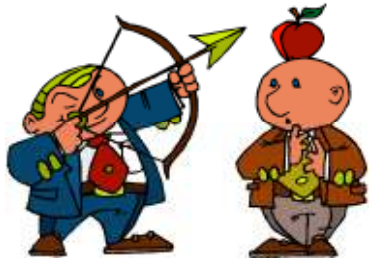
The **Insider Threat** to critical infrastructure is an individual with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm

- *National Infrastructure Advisory Council (**NIAC**)*

Different Categories of Insider Threat

Pure Insider

- An employee with all the rights and access associated with being employed by the company
- Elevated pure insider is an insider who has additional privileged access such as, administrator access



Insider Associate

- People with limited authorized access are called Insider Associate
- Contractors, guards, and cleaning and plant services all comes under this category

Different Categories of Insider Threat (cont'd)

Insider Affiliate

- Insider affiliates do not have direct access to the organization but illegally use the employee's credentials to gain access
- An insider affiliate is a spouse, friend, or even client of an employee

Outside Affiliates

- They are non-trusted outsiders who use open access to gain access to an organization's resources
- The best way of outside affiliate is accessing unprotected wireless points

Privileged Access

- Insiders enjoy two critical links in security
  - Trust of the employer
  - Access to Facilities

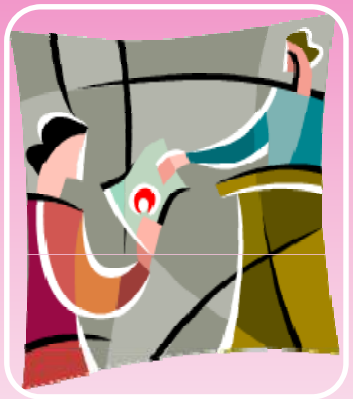
Driving Force behind Insider Attack

- Work related grievance
- Financial gain
- Challenge
- Curiosity
- Spy (Corporate Espionage)

Common Attacks carried out by Insiders

- Sabotage of information/ systems
- Theft of information/ computing assets
- Injecting bad code
- Viruses
- Installation of unauthorized software/ hardware
- Manipulation of Protocol/ OS Design Flaws
- Social engineering

Techniques Used for Corporate Espionage



Social Engineering

- Social engineering is defined as a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures

Dumpster Diving

- Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network

Techniques Used for Corporate Espionage (cont'd)

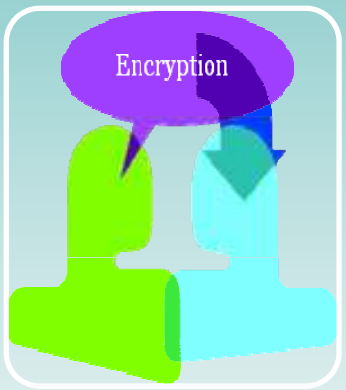
Information extraction

- The information can be extracted through:
  - Hidden files
  - Removable media
  - Wireless exfiltration
  - Laptops
  - PDAs/ Blackberrys

Network leakage

- The network traffic that are allowed in an organization is Web and email
- Insiders can use these techniques to disclose the organization's information

Techniques Used for Corporate Espionage (cont'd)



Cryptography

- Cryptography garbles a message in such a way thatits meaning is concealed
- It starts off with a plaintext message and then an encryption algorithm is used to garble a message which creates cipher text

Steganography

- Steganography is data hiding, and is meant to conceal the true meaning of a message
- It is referred to as a secret communication and covert communication

Techniques Used for Corporate Espionage (cont'd)

Malicious attacks

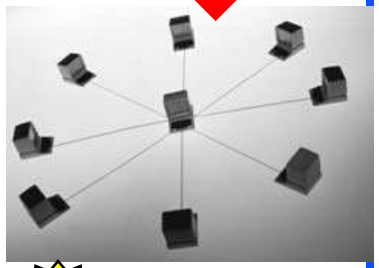
- Malicious attacks are used to gain additional access or elevated privileges
- These attacks usually involve running exploit code against a system

Process of Hacking

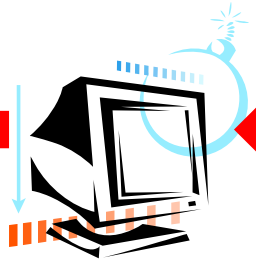
1 Gathers Information of Target Organization

2 Scans the target network for Vulnerabilities

3 Exploits Known Vulnerabilities to breach defense mechanisms



4 Breaks Network Defense using exploits for known vulnerabilities



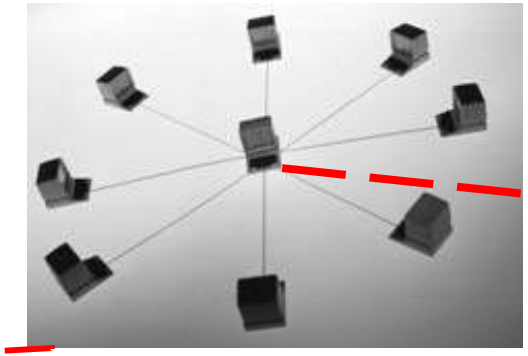
5 Exploits System Resources

6 Plants Malicious programs for backdoor acc

7 Clears Evidence by erasing tracks

Hacker following the 7 habits to attack the target organization

Process of Hacking (cont'd)



Network Defense Mechanisms

Target Organization's Internal Network

Internal attack

Internet

8 Launches an attack from the Organization's Internal Network

Case Study : Disgruntled System Administrator

A system administrator, angered by his diminished role in a thriving defense manufacturing firm whose computer network he alone had developed and managed, centralized the software that supported the company's manufacturing processes on a single server, and then intimidated a coworker into giving him the only backup tapes for that software.

Following the system administrator's termination for inappropriate and abusive treatment of his coworkers, a logic bomb previously planted by the insider detonated, deleting the only remaining copy of the critical software from the company's server.

The company estimated the cost of damage in excess of $10 million, which led to the layoff of some 80 employees.

Source: U.S Secret Service and CERT Coordination Center/ SEI
Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors

Former Forbes Employee Pleads Guilty

In 1997, George Parente was arrested for causing five network servers at the publishing company Forbes, Inc., to crash. Parente was a former Forbes computer technician who had been terminated from temporary employment.

In what appears to have been a vengeful act against the company and his supervisors, Parente dialed into the Forbes computer system from his residence and gained access through a co-worker's log-in and password. Once online, he caused five of the eight Forbes computer network servers to crash, and erased all of the server volume on each of the affected servers. No data could be restored.

Parente's sabotage resulted in a two day shut down in Forbes' New York operations with losses exceeding $100,000.

Parente pleaded guilty to one count of violating Computer Fraud and Abuse Act, Title 18 U.S.C. 1030

Source: *http://www.usdoj.gov/criminal/cybercrime/vatis.htm*

Former Employees Abet Stealing Trade Secrets

Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China

First Conviction in the Country for Foreign Economic Espionage

SAN JOSE United States Attorney Kevin V. Ryan announced that Fei Ye and Ming Zhong pleaded guilty today to two counts each of economic espionage. Ming and Zhong were arrested at the San Francisco International Airport on November 23, 2001, with stolen trade secret information in their luggage while attempting to board an aircraft bound for China. The defendants today admitted to possessing stolen trade secrets from Sun Microsystems, Inc. and Transmeta Corporation with the intent to benefit the Peoples Republic of China. These guilty pleas mark the first convictions in the country for economic espionage under 18 U.S.C. 1831, and are the result of an investigation by the Federal Bureau of Investigation, with assistance from U.S. Immigration and Customs Enforcement and Customs and Border Protection.

U.S. Attorney Kevin V. Ryan stated, "These guilty pleas represent the first convictions in the country under this section of the Economic Espionage Act of 1996, a law that was enacted by Congress against a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage. Silicon Valley generates so many of the ideas and innovations in technology that give this country an economic edge and we are committed to working with and protecting the companies who are robbed of their valuable trade secrets."

Mr. Ye and Mr. Zhong today admitted that they intended to utilize the trade secrets in designing a computer microprocessor that was to be manufactured and marketed by a company that they had established, known as Supervision, Inc. In pleading guilty, Mr. Ye and Mr. Zhong admitted that Supervision was to have provided a share of any profits made on sales of chips to the City of Hangzhou and the Province of Zhejiang in China, from which Supervision was to receive funding. Mr. Ye and Mr. Zhong further admitted that their company had applied for funding from the National High Technology Research and Development Program of China, commonly known as the "863 Program."

Source: *http://www.usdoj.gov/*

California Man Sentenced For Hacking

California Man Sentenced for Recklessly Damaging a Protected Computer Owned by his Former Employer

United States Attorney Carol C. Lam announced that Jay Vern Heim was sentenced today by United States District Judge Roger T. Benitez in federal court in San Diego. Judge Benitez first accepted as final Mr. Heim's previously tendered plea of guilty to a charge of recklessly damaging a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(ii).

According to Assistant U.S. Attorney Mitch Dembin, who prosecuted the case, in connection with his guilty plea Mr. Heim admitted that he was a founding partner and employee of Facility Automation Systems ("FAS"), a San Diego company that installs and maintains building automation systems. He left FAS in March 2005. Mr. Heim further admitted that on January 26, 2006, he used the username and password assigned to FAS for its Internet domain, facilityautomationsystems.com, and redirected all FAS Internet traffic, including electronic mail, to a server at Mr. Heim's new employer, the Moreno Valley Unified School District. Mr. Heim knew that redirecting the traffic to that server would make FAS' web site and electronic mail services inaccessible. The cost to FAS in lost productivity and restoring services exceeded $6,000.

Mr. Heim was sentenced to two years of probation and required to pay a $500 fine in addition to having to make restitution to his victim, Facility Automation Systems, in the amount of $6,050.

This case was investigated by Special Agents assigned to the Cybercrime Squad of the San Diego Division of the Federal Bureau of Investigation.

Source: *http://www.usdoj.gov/*

Federal Employee Sentenced for Hacking

Former Federal Computer Security Specialist Sentenced for Hacking Department of Education Computer

WASHINGTON -- Kenneth Kwak, 34, of Chantilly, Va., was sentenced today by U.S. District Judge Royce Lamberth to five months in prison followed by five months of home confinement, based upon Kwak's conviction for gaining unauthorized access to and obtaining information from a Department of Education computer system, the Department of Justice announced today.

Kwak's sentence results from his March 2006 guilty plea to one count of intentionally gaining unauthorized access to a government computer and thereby obtaining information. In his plea, Kwak, who had been working in an office responsible for ensuring the security of Department of Education computer systems, admitted that he had placed software on a supervisor's computer which enabled him to access the computer's storage at will. He later used that access on numerous occasions to view his supervisor's intra-office and Internet email as well as his other Internet activity and communications; Kwak then shared this information with others in his office.

As part of today's sentence, Judge Lamberth also ordered Kwak to pay restitution to the U.S. government in the amount of $40,000 and serve a three-year term of supervised release. The five months of home confinement with electronic monitoring was ordered as a special condition of this term of supervised release.

The matter was investigated by the Computer Crime Investigations Division of the Department of Education Inspector General's Office. The case was prosecuted by Senior Counsel William Yurek, cross-designated as a Special Assistant U.S. Attorney in the U.S. Attorney's Office for the District of Columbia, with assistance by Trial Attorney Howard Cox, both of the Computer Crime and Intellectual Property Section of the Criminal Division. The prosecution was part of the "zero-tolerance policy" recently adopted by the U.S. Attorney's Office regarding intrusions into U.S. government computer systems.

Source: *http://www.usdoj.gov/*

CEH Certified Ethical Hacker™ Facts

Internal breaches included:

- Viruses/ Worms outbreaks – 21%
- Wireless network breach – 1%
- Loss of customer data/ privacy issues – 12%
- Internal financial fraud involving information systems – 18%
- Theft or leakage of intellectual property (e.g. customer leakage) – 10%
- Accidental instances – 18%
- Other form of internal breach – 12%
- Do not know – 5%

Internal breach experience

	One occurrence (%)	Repeated occurrences (%)
Viruses/Worms outbreaks	8	13
Wireless network breach	1	0
Loss of customer data/privacy issues	4	8
Internal financial fraud involving information systems	7	11
Theft or leakage of intellectual property (e.g. customer leakage)	3	7
Accidental instances	5	13
Other form of internal breach	2	10
Do not know	3	2

Source: Deloitte, 2007 Global Security Survey

Key Findings from U.S Secret Service and CERT Coordination Center/ SEI study on Insider Threat

- A negative work-related event triggered most insiders' actions
- The most frequently reported motive was revenge
- The majority of insiders planned their activities in advance
- Remote access was used to carry out the majority of the attacks
- Insiders exploited systemic vulnerabilities in applications, processes, and/ or procedures, but relatively sophisticated attack tools were also employed

Key Findings from U.S Secret Service and CERT Coordination Center/ SEI study on Insider Threat (cont'd)

- The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks
- The majority of attacks took place outside normal working hours
- The majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable
- The majority of attacks were accomplished using company's computer equipment
- In addition to harming the organizations, the insiders caused harm to specific individuals

Tools

NetVizor

NetVizor is a powerful network surveillance tool, that allows to monitor the entire network from one centralized location

It enables to track workstations and individual users who may use multiple PCs on a network

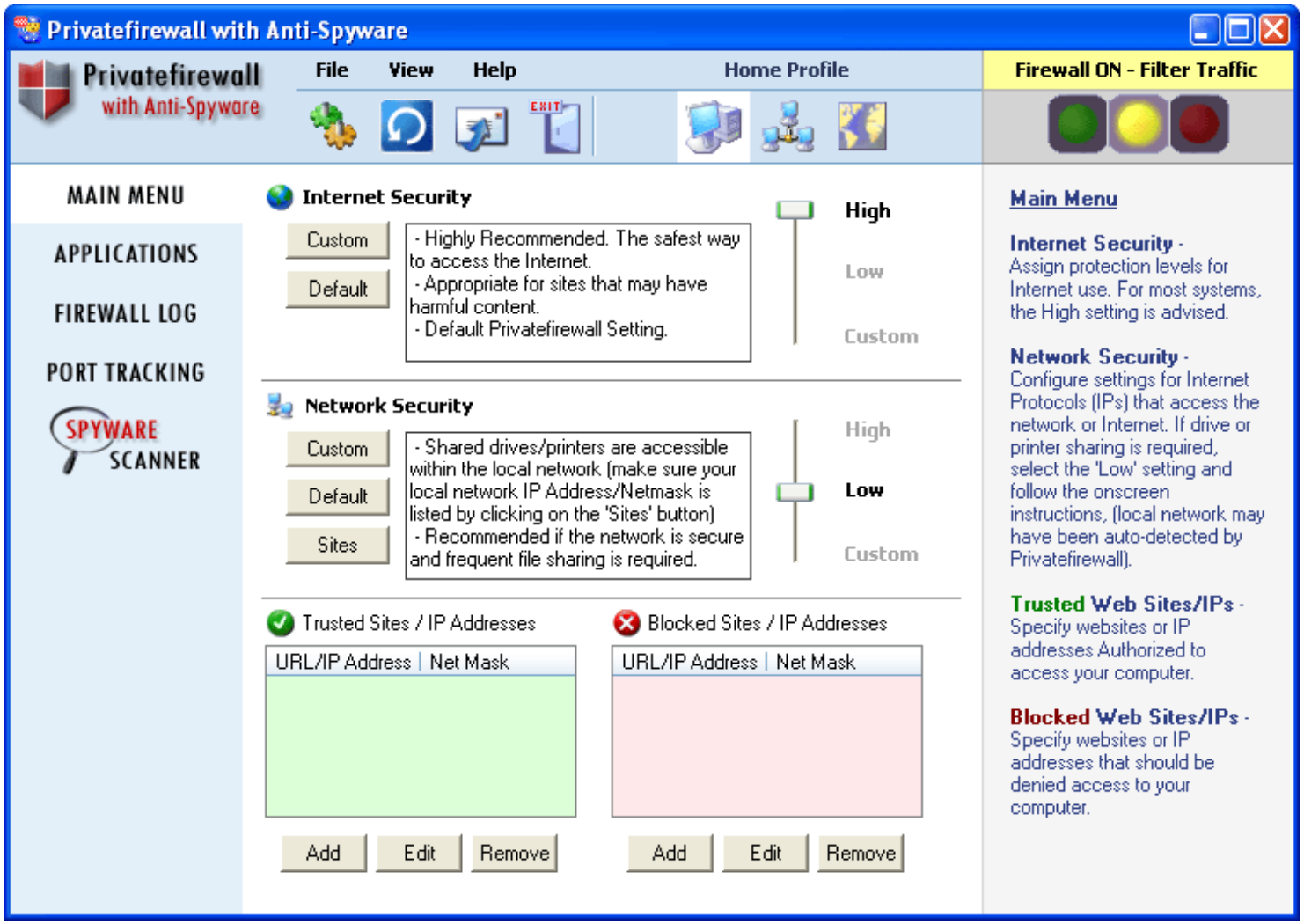
NetVizor: Screenshot

Privatefirewall w/ Pest Patrol

Privatefirewall is a Personal Firewall and Intrusion Detection Application that eliminates unauthorized access to the PC

It provides solid protection "out of the box" while allowing advanced users to create custom configurations

Privatefirewall w/ Pest Patrol: Screenshot



Countermeasures

Best Practices against Insider Threat

- Monitor employee's behavior
- Monitor computer systems used by employees
- Disable remote access
- Make sure that unnecessary account privileges are not allotted to normal users
- Disable USB drives in your network
- Enforce a security policy which addresses all your concerns
- Physical security check should not be ignored

Best Practices against Insider Threat (cont'd)

- Verify the background of new employees
- Cross-shred all paper documents before trashing them
- Secure all dumpsters and post 'NO TRESPASSING' signs
- Conduct security awareness training programs for all employees regularly
- Place locks on computer cases to prevent hardware tampering
- Lock the wire closets, server rooms, phone closets, and other sensitive equipments
- Never leave a voice mail message or e-mail broadcast message that gives an exact business itinerary

Understanding and Prioritizing Critical Assets

- Determine the criteria that is used to determine the value as monetary worth, future benefit to the company, and competitive advantage
- According to the criteria determined, score all assets of the organization and prioritize them
- List all the critical assets across the organization which needs to be properly protected
- Understand the likely attack points by analyzing the threats to the organization

Countermeasures (cont'd)

Defining Acceptable Level of Loss

- The possibility for loss is all around and risk management will determine what efforts should be focused on by an organization and what can be ignored
- Cost-benefit analysis is a typical method of determining acceptable level of risk
- The two methods to deal withpotential loss are: prevention and detection

Countermeasures (cont'd)

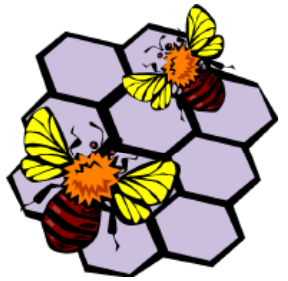
Controlling Access

- Controlling the access of the employees according to the requirement of their job
- The best way for securing an organization's critical information is by using Principle of Least Privilege
- Principle states that you give someone the least amount of access they require for their job
- Encrypt the most critical data
- Never store sensitive information of the businesson the networked computer
- Store confidential data on a stand alone computer which has no connection to other computers and the telephone line
- Regularly change the password of confidential files

Countermeasures (cont'd)

Bait: Honeypots and Honeytokens

- Catching the insiders when they are stealing the information is called honeypots and honeytokens
- Honeypots and Honeytokens are traps which are set at the system level and file level respectively
- Honeypot on he network looks attractive to attackers and lures them in
- It is used when someone wanders around the network looking for something of interest
- Honeytoken is done at a directory or file level instead of the entire system
- Display an attractive file on a legitimate server used to trap the insider



Countermeasures (cont'd)

Mole detection

- In this, a piece of data is given to a person andif that information makes its way to the public domain, then there is a mole
- It can be used to figure out who is leaking information to the public or to another entity

Profiling

- It controls and detects the insiders by understanding behavioral patterns
- The two types of profiling are individual and group profiling

Countermeasures (cont'd)

Monitoring

- Watching the behavior by inspecting the information
- It provides a starting point for profiling
- The types of monitoring that can be performed are:
  - Application-specific
  - Problem-specific
  - Full monitoring
  - Trend analysis
  - Probationary

Countermeasures (cont'd)

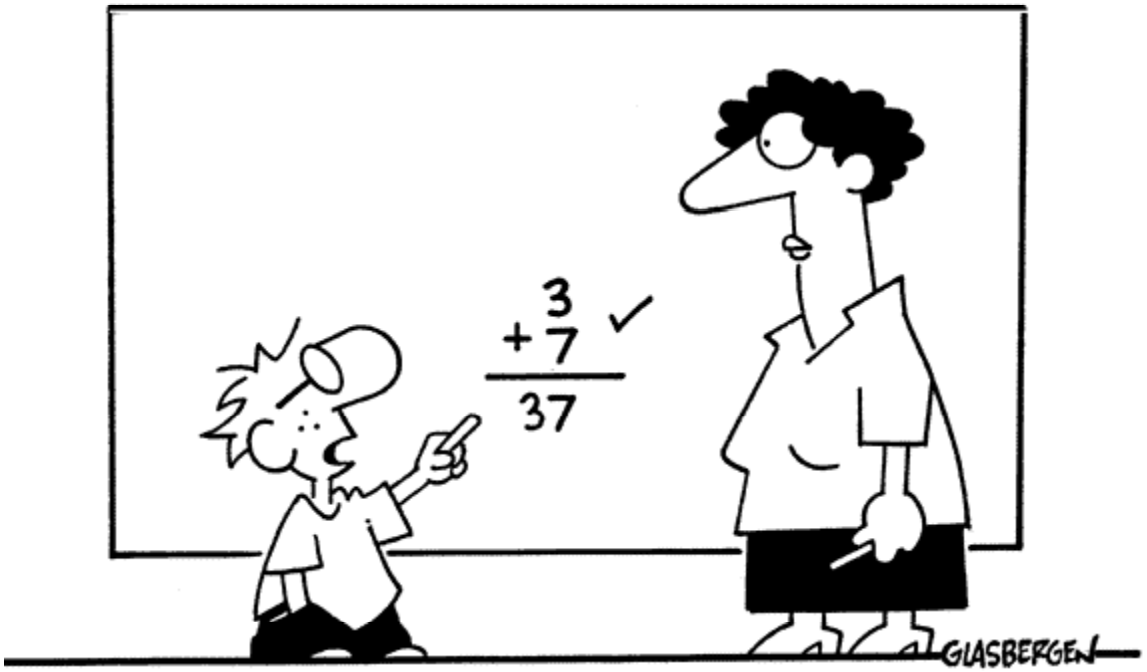
Signature Analysis

- It is an effective measure for controlling insiderthreat or any malicious activity
- It is also called as pattern analysis because it looks for a pattern that is indicative of a problem or issue
- It catches only known attacks and the attacks which occurs same way all the time

Summary

- Term 'Corporate espionage' is used to describe espionage conducted for commercial purposes on companies, governments, and to determine the activities of competitors
- People with limited authorized access is called Insider Associate
- Insiders can use Web and email to disclose the organization's information
- Cryptography garbles a message in such a way that its meaning is concealed
- Make sure that unnecessary account privileges are not allotted to normal users

"It's the latest innovation in office safety.
When your computer crashes, an air bag is activated
so you won't bang your head in frustration."



"In the corporate world they pay you big bucks for thinking outside of the box!"