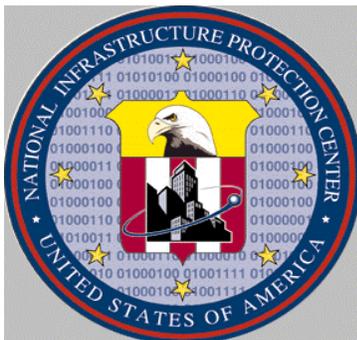


# NATIONAL INFRASTRUCTURE PROTECTION CENTER

## HIGHLIGHTS

Formerly known as *Critical Infrastructure Developments*

*A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.*



**Issue 2-01**  
**February 15, 2001**

*Editors:* Linda Garrison  
Martin Grand

- 
- ! Virus Development and Organizational Security: Challenges for Evolving Networks.
  - ! Internet Banking and Security.
  - ! Trends in Industrial Espionage and the Loss of Proprietary Information: Incidents and Monetary Values on the Rise.
  - ! Spoofing: Deception in Information Attacks.

---

For more information, or to be added to the distribution list, please contact the NIPC Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call (202)323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, please participate in our reader survey, or contact the Editors at (202) 324-0334 or (202) 324-0353. A reader survey form is attached.

## **Virus Development and Organizational Security: Challenges for Evolving Networks**

*New network-connected devices, dynamic virus development tactics, and future technological advances will continue to drive the evolution of anti-virus defensive measures.*

Viruses have historically been one of the most potentially destructive threats to enterprise networks. Virus development, which has grown progressively from low-level system utilization "pranks" to global, high-level system destruction mechanisms, has affected every aspect of Information Technology (IT) planning and operations. In general, most IT managers have understood and reacted to threats presented by viruses, implementing network anti-virus (AV) policies and procedures. However, the major anti-virus products function by obtaining a copy of the virus, examining its signature, and distributing a remedy by electronic means, thus requiring that the program be continually updated to remain effective. The growth of the Internet has directly contributed to a rise in the speed at which malicious code travels the globe and spawns variants which can be inserted in e-mails, downloads, and browser-based applications. In addition, the applications and services that can be targeted by viruses are expanding to include mobile devices such as cellular telephones, personal digital assistant (PDA) devices and computer appliances, which are increasingly interfacing with business and government networks. This expansion of the enterprise network into non-traditional segments challenges system administrators and planners to adapt to increasingly sophisticated AV deployments.

The deployment of AV measures varies from one organization to another and is driven by many factors, including cost and perceived risk. However, surveys of the largest corporate networks indicate that while AV deployment plans vary, the infections are on the increase. A recent ICSA report on virus prevalence stated that the current rate of virus infection grew from 22 PCs infected per 1,000 computers in 1998 to 91 PCs infected per 1,000 in 2000. The large increase, although partially due to the AI Love You@virus and its variants occurred because of significant increases in previously low-level threats, such as mobile code and script viruses.

**Network policies need to be dynamically revised to incorporate additions and changes spawned by virus development and AV technology. In addition, system administrators should implement best practices policies to enforce timely updates of virus definition files. Even though recent advances in virus definition file distribution methods, including Web-site enhanced virus programs and Intranet-based distribution servers have improved the automation of the AV update process, there is usually a certain amount of human interaction required for the procedure. Mobile code continues to challenge the AV vendors with the speed of infection and its growing popularity with virus writers. While e-mail remains the most popular avenue of virus attacks the Web and wireless devices are rapidly becoming areas of concern. Corporate and government AV policies should incorporate all network-connected devices.**

## **Internet Banking and Security**

*The use of the Internet as a remote delivery channel to conduct transactions has proven alluring for both financial institutions and their customers. Security features are an integral part of Internet Banking.*

In May 2000, the **A**On-line Banking Report<sup>®</sup> estimated that 7 million Web banking users in the U.S. conducted \$19 million worth of transactions on average per month. The market research firm International Data Corporation (IDC) has concluded that consumer interest in on-line banking will continue to rise, and the firm projects that the number of households conducting banking on-line will exceed 22 million within a few years. All of the large U.S. banks and many of the smaller financial institutions offer some means of conducting transactions over the Internet. These transactions range from transferring funds, applying for a loan, and electronic bill presentment and payment.

The benefits of Internet banking include: convenience, time and money saving factors, ease of access, and opportunities for aggregation of services. These benefits are offset in part by the exposure to the same risks faced by other on-line activities such as: technical factors, server outages, or malicious activity. Robust authentication of users, combined with the speed and volume at which on-line financial operations are conducted, has the potential to make Internet banks vulnerable to schemes such as those in which large numbers of bogus transactions are submitted in an attempt to defraud the institution. Arrests reportedly involving such a plot against the on-line bank Egg were recently made in the United Kingdom. The security of customer accounts may also be compromised either through user error (e.g., if the customer leaves his banking software active on a computer that others may access) or through poor configuration management on the server. A British on-line bank had to briefly suspend operations this past summer after users reportedly were able to view other customers' account information.

Security features are an integral part of Internet banking. U.S. financial regulatory guidelines mandate review of a bank's information systems as part of its regular auditing process. Federal bank examinations also evaluate key aspects of information technology risk management practices. Most Internet-based banking systems use encryption protocols such as Secure Socket Layer (SSL) to protect sensitive data in transit over the Internet, as well as to prevent a third party from spoofing the bank's identity.

One important Internet banking component which is not subject to the same degree of rigorous security auditing as the other components is the customer's personal computer (PC). Unlike computers on a corporate network, home computers are not subject to a formal security regime, anti-virus measures may be more lax, most data stored on the typical user's computer is not protected by encryption, and a home PC is usually not behind a firewall. These factors collectively make the user's PC the weak link in an on-line banking environment.

In August 2000, a Visual Basic Script (VBS) worm circulating on the Internet affected customers of a Swiss bank. The worm, based loosely on the infamous VBS/Loveletter worm, distributed

itself via e-mail. When a Windows-based computer became infected, the worm attempted to download a Trojan component to the victim's computer via FTP. After the infected computer was restarted, the Trojan accessed the computer's registry and copied sensitive PIN information relating to the on-line banking software used by the bank and sent the information to three e-mail addresses. (For more information on this worm, please refer to NIPC Alert 00-053 of 17 August 2000 at <<http://www.nipc.gov/warnings/alerts/2000/00-053.htm>>.) Although the bank stated that no customers had reported any damage as a result of this attack, the incident gained wide attention as proof that attacks on users of home banking software do not occur only in staged demonstrations.

The financial industry is responding to these types of threats by increasingly supplying their on-line customers with extra security software to help protect their PCs, and offering their customers a personal firewall that will limit access to a user's PC from the Internet. Security-conscious computer users can also select from a wide range of commercial software packages to protect their PCs and the data on them.

**Given the growth forecast for Internet banking, the security of this delivery channel will gain in importance as it becomes an integral part of the banking system. Participants need to ensure that financial information and funds transferred over the Internet are safe from malicious diversion or alteration. The increasing use of home PCs for high-value financial transactions requires adequate measures to secure them from attack via viruses and Trojan horses. An effective anti-virus package as well as personal firewalls can mitigate the risks posed by Internet banking. No single solution will provide an all-encompassing secure environment for a transaction involving two or more parties. Security on the Internet is a shared responsibility borne by all who use the network, including the home PC banker.**

## **Trends in Industrial Espionage and the Loss of Proprietary Information: Incidents and Monetary Values on the Rise**

*As illustrated by three incidents reported during 2000, the loss and exploitation of sensitive information, such as that involved in e-commerce operations and business communications, increasingly results in economic loss and/or damage.*

### **Industrial Espionage and Loss of Proprietary Data**

In 1999, the American Society for Industrial Security (ASIS) and Pricewaterhouse Coopers conducted a survey regarding the loss of trade secrets and other proprietary information. That survey reflected losses to U.S. companies amounting to tens of billions of dollars annually. Of the 97 Fortune 1000 companies participating in the survey, 44 reported a total of over 1000 theft incidents, with the majority of incidents in the High Technology and Services organizations. Those companies also indicated that on-site contractor employees and original equipment manufacturers are the greatest threat to their proprietary information.

#### **Insiders**

Two recent legal actions involving former insiders at a large Information Technology (IT) firm illustrate the damage insiders targeting proprietary information can cause. In one instance, the former employee was convicted for theft of source code, two versions of which were found on his home computers. The IT firm estimated the value of the software at \$2 billion. In an unrelated incident, a second former employee was arrested after allegations that he had copied several CD-ROMs of e-mail and data related to new developmental products. These examples represent just one company's experiences. Numerous other examples have been reported in the open press.

#### **Steganography incident**

On September 11, 2000, MSNBC reported that a French defense contractor had hired a U.S. security consultant to determine whether proprietary designs were being leaked outside the company. Investigation revealed that an employee was using digital steganography (a method used to covertly deliver documents by imbedding them into an electronic image) to steal the company's trade secrets using its web site pictures. The MSNBC report appears to be one of the first reports of actual use of steganography for industrial espionage purposes, due largely to the difficulty in detecting its use.

**The rapidly growing role of e-commerce in the global economy, the proliferation of enterprise information systems connected to critical infrastructures, and the Internet, have significantly increased the opportunities to target sensitive information. The challenge in protecting that information is two-fold: how best to determine the value of proprietary information and how to best to protect it.**

## **Spoofing: Deception used in Information Attacks**

*When conducting on-line communications, things may not always be as they appear.*

Many Internet communications do not utilize strong authentication measures. As a result, the average on-line user cannot be certain with whom he is communicating, or to what Internet host he is connected. Hackers may exploit this inherent weakness with a range of exploits designed to trick a user into accepting a falsehood as fact. Some examples of deceptions referred to as spoofing attacks include the following (along with their definitions):

**E-mail spoofing.** An attacker uses one of several possible mechanisms to forge an e-mail message to make it appear that the message originated from another host or that a third party sent it.

**IP spoofing.** A fairly technical attack in which a person manipulates the data his computer is sending, so as to impersonate the Internet address of another computer. This may defeat any protocols designed to control access to a resource based on Internet Protocol (IP) address (e.g., internal versus external addresses).

**Domain spoofing.** An attacker may corrupt the domain name system so that when users attempt to access a particular host by name, such as <www.example.net>, they are actually directed to a completely different Internet host. In a less technical attack, a person may attempt to deceive by using domain names similar to that of the target site, e.g., <www.examp1e.net>, which uses the number 1 instead of the letter l.

**Frame spoofing.** A malicious Web publisher may construct code that opens an arbitrary page in one frame of a Web browser's window without updating the browser's address bar. This could lead to a user believing he is browsing a trusted site when in fact, he is reading information from a hostile site.

**Web spoofing.** A third party can construct a fake Web site (or group of sites) that looks and functions exactly like another, trusted site or sites. This spoofed site may be used to disseminate false information or to collect sensitive data such as credit card numbers and personal information, that users would normally submit only to a trusted host.

Spoofing can form the basis for an entire range of on-line hostility including laying the groundwork for more technical attacks in the future. Spoofing may also be combined with social engineering techniques or plain old-fashioned fraud and deception to perpetrate hoaxes. A stereotypical spoofing attack involves an attacker crafting a replica of an on-line bank and tricking Internet users into sending their sensitive banking data to the attacker's site. Other types of spoofs, which involve a broader range of issues, are illustrated by the following examples:

In the fall of 2000, political tensions in the Middle East spilled over into cyberspace, resulting in an increased level of hostile on-line activity directed at pro-Israel and pro-

Palestinian Internet sites.<sup>1</sup> Against this background of on-line attacks, a number of media outlets in the United States and Europe were contacted by a group which claimed that hackers had defaced a web site located at [www.hizbolla.org](http://www.hizbolla.org) operated by the pro-Arab group Hezbollah. When journalists accessed the site, they viewed Hebrew messages and Israeli symbols, resulting in several news organizations reporting that the Hezbollah's web site had been defaced by pro-Israeli hackers. Only later were journalists able to determine that the site at [hizbolla.org](http://hizbolla.org) was apparently a fraud that had been established by an unidentified person using an address in Lebanon. (The Hezbollah's real site may be accessed using the domains [hizbollah.org](http://hizbollah.org) or [hizballah.org](http://hizballah.org).)

Another type of spoofing attack was used in connection with the ongoing conflict between Russian authorities and rebel forces in Chechnya. Media accounts indicate that in 1999, unknown persons manipulated the domain name system so that many Internet users in the former Soviet Union trying to connect to the pro-Chechen Kavkaz Center site at [www.kavkaz.org](http://www.kavkaz.org) were instead directed to a phony site. The latter site was designed to give the impression that pro-Russian hackers had broken into and defaced the Kavkaz Center site.

A number of ethnic or political conflicts around the world, have manifested themselves in information-based attacks. Due to the semi-anonymous nature of Internet transactions, one often cannot be certain of the identities, origins, or motivations of the participants in these on-line attacks. This fact opens possibilities for malicious action; e.g., a third party who is interested in fanning the flames of hostility for his own reasons could deface a site with the slogans of one of the hostile parties in a dispute. The variety of spoofing attacks available to malicious hackers adds another layer of uncertainty to the issue of conflict in cyberspace.

**A number of technical countermeasures to spoofing attacks exist. For example, digital signatures can be used to authenticate the true sender of an e-mail message, and network administrators can configure their networks to make IP spoofing attacks much more difficult to launch. However, many types of spoofing attacks focus on tricking or deceiving the end user, and in such cases, awareness remains key. An alert and aware user will be able to detect a spoofing attack and avoid being victimized by it.**

---

<sup>1</sup> For more information, please refer to NIPC Assessment 00-057 Middle East E-mail Flooding and Denial of Service (DoS) Attacks (26 October 2000) and NIPC Advisory 00-058 Cyber Attacks Against U.S. Web Sites in On-going Middle East Conflict (3 November 2000). Both documents are available at the National Infrastructure Protection Center's Web site at [www.nipc.gov](http://www.nipc.gov).

# Survey

## HIGHLIGHTS

February 15, 2001, Issue 2

In order to provide a service, which is relevant to our clients, we would like your opinions on this publication. Please execute this survey and return to the address at the bottom.

Please circle the most appropriate response

1. Highlights presents issues which are \_\_\_\_\_ to my concerns.  
not relevant / relevant

2. The information is presented in a \_\_\_\_\_ fashion.  
jumbled / clear and understandable / too technical

3. The quality of the information presented is \_\_\_\_\_.  
low / adequate / high

4. The frequency of the publication is \_\_\_\_\_.  
too seldom / adequate / too frequent

5. I find the length of the articles to be \_\_\_\_\_.  
too short / appropriate / too long

6. Past articles have been informative.            Yes            No

7. What kind of articles would you find helpful in the performance of your duties?

---

---

---

8. Overall assessment.

---

---

---

What is your job title? \_\_\_\_\_

Would you like to contribute an article? If so, what would the topic be? Yes or No \_\_\_\_\_

Thank you for your time.

Please return this form to:    Editor's, Highlights  
Room 11719, NIPC, Federal Bureau of Investigation  
935 Pennsylvania Avenue, N.W., Washington, D.C. 20535

Fax: (202)324-0311

or E-mail - [lgarrison@fbi.gov](mailto:lgarrison@fbi.gov) or [mgrand@fbi.gov](mailto:mgrand@fbi.gov)

HIGHLIGHTS 2 B01

February 15, 2001