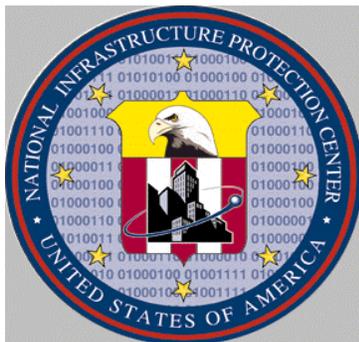


NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

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



Issue 6-01
June 15, 2001

Editors: Linda Garrison
Martin Grand

-
- **Cyberterrorism: An Evolving Concept**
 - **Threat Assessment: Lion, Adore, and Sadmin/IIS Worms**
 - **Globalization of Software Development: Concerns Surrounding Control and Access**
 - **Security Patches: Risks and Recommendations**

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

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

This issue has an overall classification of "Unclassified." This publication may be disseminated further without express permission.

Cyberterrorism: An Evolving Concept

With the advent of the Information Age, the definition of terrorism must evolve to reflect the type of activity that goes beyond traditional physical violence.

In the “cyber” world, computers and their related equipment, not people, will generally be the targets of terrorists, and remote, computer generated disruption and/or distortion may be a viable option to destruction. While the disruption and/or distortion of data or services are not considered to be a violent act and will not always endanger a human life, they do present unacceptable risks to complex information dependent societies such as ours.

Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.
(Proposed by the NIPC, Analysis and Information Sharing Unit)

... telecommunications capabilities, ... in this context telecommunications capabilities refers to specialized knowledge and skill used to manipulate telecommunications systems thereby allowing individuals to obtain an extensive level of control over a penetrated system.

... to create fear by causing confusion and uncertainty within a given population, ... terrorist organizations generally use symbolic means to attack the sanctity of the society in which it exists. If attacks on these symbolic targets are successful, the terrorists will have accomplished their goal of isolating individuals from the society in which those individuals formerly felt secure. Such actions result in confusion and uncertainty about a government's ability to protect its citizens. This is when citizens are most vulnerable to influence by others.

Terrorist use of information technology to formulate plans, spread propaganda, support terrorist recruiting, raise funds, and communicate is not regarded as cyberterrorism within this definition. Cyberterrorism is when the destructive nature of the “act” itself is carried out via computers or other cyber/electronic means through techniques such as infected e-mail attachments. Delivery of the terrorist's message via the Internet **does not** constitute a cyberterrorism event.

Terrorism in the world today is changing. While we have yet to see an instance of cyberterrorism, cyber attacks by terrorists resulting in physical or psychological distress to targeted governments or civilian populations by disrupting critical systems will likely occur in the future. We must look beyond traditional boundaries in anticipating new terrorist threats that likely cannot be eliminated, only limited and managed. Terrorists are becoming more diverse and creative and will require a well-orchestrated mandate of close coordination among civilian, intelligence, law enforcement, and military organizations.

THREAT ASSESSMENT: LION, ADORE, and SADMIND/ IIS WORMS

Three worms recently appearing exhibit a new trend in system exploitation in terms of the speed in which vulnerabilities are exploited.

In March 2001, the NIPC began tracking reports of an unusually high number of scans or probes to several specific ports. Initial analysis by the NIPC determined that a new type of Internet worm was making its way through the Web looking for unpatched versions of BIND.¹ This activity was attributed to the Lion Worm and its variants, the Adore Worm, and the Sadmind/Internet Information Server (IIS) Worm. A worm is one type of software attack that replicates itself on one computer and attempts to infect others that may be attached to the same network.

New Trends in Exploitation

These worms mark a new trend in system exploitation in terms of the speed in which vulnerabilities are exploited. For the Lion, Adore and Sadmind/IIS Worms, these probes are fast and extremely noisy, indicating an automated attack (i.e., performed without human intervention). While Internet worms are not new, these three worms incorporate new techniques that combine exploits and automated propagation to add new tools and new exploits with “snap-on” simplicity.

In addition, a well-defined life cycle common to all three worms has been observed:

- Stage 1 - Potential vulnerabilities are identified, most recently highlighted by the buffer overflow in BIND.
- Stage 2 - Leads to individual automated exploit scripts being written and released in the wild (in the past these needed to be leveraged on an individual basis by an attacker).
- Stage 3 - The final stage is a spike in the scans or probes to ports searching for hosts running services with any of the previously defined vulnerabilities.

Recent Activity Serves as Possible Indications of Future Attacks

These trends are illustrated in the recent cyber attacks between U.S. and Chinese hackers. Activity of this nature shows how a future attack might look and the warning signs to watch for (i.e., increased scanning activity). It also illustrates the importance of soliciting support from those private sector individuals who have reached out to federal government contacts and foreign ISPs to better understand the activity.

¹ www.cert.org/advisories/CA-2001-02.html

Globalization of Software Development: Concerns Surrounding Control and Access

A significant amount of U.S. based commercial software is developed by teams working in countries around the world. Foreign nations that a few years ago had nascent information technology (IT) industries are now emerging as software developers.

Integrity, Control, and Access Concerns

Market researchers at IDC recently estimated that U.S. based spending on offshore IT outsourcing would experience a compound annual growth rate of 26% over the next several years. The increase in foreign based programmers makes vetting and controlling key IT employees more difficult. A shortage of IT workers in Ireland, a major software producer, has led the government to actively recruit foreign workers from areas such as South Asia and Eastern Europe. Last year the German government introduced a special “Green Card” regime that is expected to attract tens of thousands of computer specialists to the country.

The majority of your IT staff are honest professionals. However, one cannot ignore the fact that the level of access to business enterprise applications or critical infrastructure control systems afforded them during software development or integration, could attract the attention of Foreign Intelligence Services seeking to exploit this access for malicious purposes. As the National Security Council recently noted, lower-paid foreign programmers appear to be ripe for exploitation by criminal organizations.

One long-standing concern has been the possibility for source code manipulation, e.g., the insertion of malicious functionality or backdoor system access. Another issue especially pertinent to offshore outsourcing involves access to sensitive business information on processes and operations provided to foreign developers. Respondents to one industry survey on offshore outsourcing expressed concern over the possible exploitation of proprietary information shared in such relationships.

Mitigation Strategies

Organizations can take steps to assure critical information systems integrity during external software development and integration. Some of which are:

- Clarify issues such as personnel vetting during the contract negotiation process.
- Exercise rigorous supervision of projects during the production period.
- Ensure that development includes separation of duties so that no one person is responsible for writing code, reviewing it, and testing it.
- Ensure that developers enforce appropriate access controls on proprietary information as well as the communications channels used during development.
- Insist upon the destruction or return of all proprietary information and software after conclusion of the contract.
- Ensure that the security policies of the outsourced entity are up to the standards of your company.

Security Patches: Risks and Recommendations

Installing the latest available software patches is one of the easiest and most effective ways to ensure that your systems are protected from computer viral infections and vulnerabilities. It is important to remember, however, that there can be problems associated with these fixes.

Some issues associated with security patches are illustrated in the following examples:

Virus Infections

A security patch from a major software producer was infected with the FunLove virus. This resulted in the company halting specific downloads and issuing an alert. Fortunately, the FunLove virus was a known threat and was found by most virus detectors.

Timeliness

Customers who install patches should not assume simply downloading the latest patch protects them. As in the case of the Melissa virus, soon after the patch was released, the virus mutated and began to circulate without a subject line. The initial fix had been circumvented because it filtered the e-mail by the content in the subject line.

Reliability

A fix for the vixie-cron package was released that created a new vulnerability, thereby opening up the possibility of a root compromise. Fortunately, an engineer discovered the flaw during an audit and a new fix was subsequently released.

Trustworthiness

An e-mail with the subject "FW: Symantec Anti-Virus warning" was reported to be circulating. The e-mail claimed its attachment contained a description of a virus when in fact it actually contained a VB script virus.

Installation

Many users had trouble applying a patch for a popular Internet browser designed to fix a critical hole in security. Customers who attempted to download it apparently received the message "This update does not need to be installed on this system."

Authentication

A security company recently queried 27 vendors as to whether or not their patches were released using authentication techniques such as digital signatures. Surprisingly, the company found that some of these vendors employed no authentication when releasing fixes. The concern is that if a vendor's machine were to be compromised, a Trojan-horse patch could be uploaded on the

compromised server. Another issue is that when companies do make authentication available, customers seldom take advantage of it.

Conclusion

Despite the issues mentioned above, the installation of updated security patches remains a primary means of system protection. The following measures are suggested as a way to minimize possible problems:

- Keep up with latest patches to ensure that any problems with earlier versions of patches are corrected. NIPC's publication *CyberNotes* (available at <http://www.nipc.gov/cybernotes/cybernotes.htm>) will assist in this endeavor.
- Network security administrators should have established points of contact with vendors in case of a problem with a particular update.
- Downloaded software (to include patches) should be scanned for viruses and virus definitions files should be updated regularly.
- Remember that patches often do not support older versions of software, so upgrades are recommended when feasible.
- Download, whenever possible, from authenticated, trusted sources and use the provided authentication as a means to verify the trustworthiness of the information.