DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND

CYBER THREAT SUMMARY

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

CYBER THREAT 011-02
26 April 2002
CIOP-ACE (195)

190001R April –252400R April 2002

WARNING

1. The Cyber Threat Summary (CTS) is intended to provide a periodic update of information of interest to law enforcement, security personnel, supported commanders, intelligence analysts, and others with force protection duties. It intentionally does not include any classified information.

2. Because the CTS is FOUO and potentially contains information protected by the Privacy Act, further distribution of these summaries is restricted to DOD and law enforcement agencies only, unless approval from HQ, USACIDC has been obtained beforehand. Violations of the Privacy Act make both the releasing organization **and the person involved in the unauthorized release** liable in civil suits. Information should not be released to the media, or others within DOD without a valid need to know.

3. Some information is law enforcement sensitive. These sections are marked as (LES). Release of LES material could adversely affect or jeopardize follow-up investigative and law enforcement activities. Other portions of this report are unclassified and are marked as (U). These portions can be distributed outside law enforcement, security and intelligence channels to others with a need to know.

3. Persons/organizations found violating the distribution restrictions would be banned from receiving all future USACIDC summary reports.

CIOP-ACE (195)
SUBJECT: Cyber Threat Summary 011-02

A. POTENTIAL VULNERABILITIES:

1. (U) Safe and Sound: Cyber terrorism, corporate espionage, natural disasters, fires, malware, and other risks should be considered in the creation of a cyber security plan. Additionally, companies should also consider potential risks of insider damage to computers and proprietary information during the hiring process. Industry specific risks to cyber attacks and damage should also be considered; for example, those companies that might be targets of environmentalists may be at risk of becoming a target of electronic protests (21 Apr 02, Augusta Chronicle). http://augustachronicle.com/stories/042102/bus_risk1.shtml

2. (U) User Privileges Vulnerability in Oracle9i Database Server: SecuriTeam.com reports a potential vulnerability in the Oracle9i Database Server, version 9.0.1.x that might allow access to privileged data. A patch is available from Oracle (21 Apr 02, SecuriTeam.com). http://www.securiteam.com/securitynews/5PP0L0A6UO.html

3. (U) Army Proxy Server Closes Web Back Door: The US Army has set up a proxy server to limit access to internal systems while allowing access to web site content. This new tool will eliminate any "back doors" for hackers and decrease the possibility of web content attacks from 67 percent to 5 percent (22 Apr 02, Federal Computer Week). http://www.fcw.com/fcw/articles/2002/0422/news-army-04-22-02.asp

B. VIRUS

1. (U) W32.Maldal.K@mm: W32.Maldal.K@mm is a variant of W32.Maldal@mm. It is a mass-mailing worm that is written in Visual Basic. The worm attempts to send itself to all contacts in the Microsoft Outlook address book and the MSN Messenger contact list. It also searches for email addresses in all .html files. It creates several registry keys and files on the system (22 Apr 02, Symantec).

2. (U) W32.DSS.Trojan (also known as Trojan.Win32.DSS): W32.DSS.Trojan is a Trojan horse that inserts a small Web page onto your system. This Web page is then launched in a hidden Internet Explorer window (24 Apr 02, Symantec).

3. (U) Backdoor.RemoteNC: Backdoor.RemoteNC is a backdoor Trojan that can allow a hacker to gain access to your system. The hacker then can delete, copy or execute files on your computer (24 Apr 02, Symantec).

CIOP-ACE (195)
SUBJECT: Cyber Threat Summary 011-02

C. CYBERCRIME

1. (LES) Web Page Defacement: On 18 Apr 02, the ACERT reported a web page defacement of a US Army Civilian Personnel Office web server. Person(s) unknown, (claiming to be with the Brazilian Hackers Sabotage Crew), by unknown means, gained root level access on the computer and altered the web page (19 Apr 02, 0022-CID221).

2. (LES) Web Page Defacement: On 18 Apr 02, the ACERT reported a web page defacement of the US Army Publications Server. Person(s) unknown, by unknown means, gained administrator/root level access on the server and altered the web page (19 Apr 02, 0021-CID221).

3. (U) Digging for Computer Dirt: The importance of recovering data from out-dated, even archaic data storages has spurred a new niche in computer forensics. One company, Computer Conversions, specializes in conducting examinations of electronic storage devices for lawsuits. Data removal and eradication from computers does not seem to be well understood by those willing to commit criminal or terrorist acts. For example, electronic data has been an important aspect of the evidence for use in criminal cases being built against Enron and Arthur Andersen (22 Apr 02, salon.com).
http://www.salon.com/tech/feature/2002/04/22/computer_forensics/index.html

4. (U) Waging Peace on the Internet: The editorial at the below listed site includes a list of governments participating in censorship of content and material on the Internet. Hacktivism is an emerging trend of utilizing electronic means to perform demonstrations or other activities to raise awareness or support for causes and actions. The article examines the trend of hacktivism (19 Apr 02, The Register). http://www.theregister.co.uk/content/55/24946.html

5. (U) CIA Warns Of Chinese Plans For Cyber-Attacks On US: US intelligence officials believe the Chinese military is working to launch wide-scale cyber-attacks on American and Taiwanese computer networks, including Internet-linked military systems considered vulnerable to sabotage, according to a classified CIA report.

(U) Moreover, US authorities are bracing for a possible wave of hacking attacks by Chinese students against the United States in coming weeks, according to the analysis. The confidential alert, which was reviewed by The Times, was sent to intelligence officials a week ago. Although US officials have voiced concerns about individual hackers in China who have defaced federal and private Web sites, the United States has resisted publicly linking the Chinese government to those attacks or to broader cyber-style warfare.

(U) The new CIA report, however, makes clear that US intelligence analysts have become increasingly concerned that authorities in Beijing are actively planning to damage and disrupt US computer systems through the use of Internet hacking and computer viruses.

(U) Although the assessment concludes that China has not yet acquired the technical sophistication to do broad damage to US and Taiwanese systems, it maintains that this is the "intended goal" of the People's Liberation Army in China. "The mission of Chinese special forces includes physical sabotage" of vulnerable systems, the report, says--which some analysts said is driven by China's hostility toward Taiwan (25 Apr 02, Los Angeles Times).

6. (U) 'Rent-A-Hacker' Site Says It Offers Cracking For Hire: A group of Chicago Web site operators say they will break into school, government and corporate computers and alter records, for fees starting at $850. But at least one security expert thinks the operation probably is a scam. Among the services promised by Chicago-based 69 Hacking Services, is changing "bad grades" and other records on elementary, high school or college computer systems. The site is co-owned by a 23-year-old identifying himself as Akbar "Andy" HOODA. William KNOWLES, a computer security expert and editor of InfoSec News, said the hacking service most likely is a scam aimed at snaring "script kiddies" or young, naive computer users. "I'd be curious if there is a money back guarantee if they can't get in," said KNOWLES.

(U) Even if the operation is legitimate, unauthorized access to computer systems is a violation of federal and state computer crime laws, according to Matt YARBOROUGH, an attorney with Fish & Richardson and a former US Department of Justice prosecutor. The organization, which also goes by the name "Be A Hacker" (BAH), operates a Web site at: http://www.BeAHacker.com. It employs "about 15" people, according to Hooda, who said he co-owns the business with an undisclosed partner.

(U) A scrolling banner at the top of the BAH site's home page reads, "Got bad grades in college/high school? We can change them! Want passwords? We will get them! Rent-a-hacker. Will do the job. Reasonable prices." Hooda said his organization charges $2,100 and requires a down payment of $799 for "cracking" into college or university computers, but does not guarantee success. "The down (payment) is for the time we put in to hack the desired box. If we complete the case, we ask for the rest of the payment," said Hooda in an interview.

(U) An online database of registered corporations maintained by the Illinois Secretary of State's office did not include listings for BAH or 69 Hacking Services. Hooda declined to reveal how many clients the hacking group has served since it launched last year, nor would he disclose BAH's revenues, except to say "it started to become a pretty big business." In addition to hacking services, BAH offers several mail-order products, including hacking software for $69. "With this you can hack passwords, control computers, edit settings on computers, edit data on computers, delete data from computers, make another computer print from your computer, and also shut off/restart the other person's computer. This is REAL hacking," reads a description of

the software, which can be purchased online using the PayPal service. While "brash," BAH's site is unlikely to prompt action by law enforcement, according to Yarborough. "Because of free speech laws, Web sites can advertise just about anything. But if these guys are actually involved in unauthorized computer access, that's a crime that state or federal prosecutors are going to pursue," said Yarborough. He added that BAH's products could also violate the Digital Millennium Copyright Act.

(U) According to PayPal's page for BAH, the group has been a member of the online payment service for 19 months and has served 26 verified buyers. Hooda claimed BAH had around 80 sales on PayPal and made about $6,000 on sales of its products. BeAHacker.com is hosted by Virginia-based XO Communications. A spokesperson for XO, which is reportedly about to file for bankruptcy, had no immediate comment on whether the hacking site violated its terms of service.

(U) According to its site, other services provided by BAH include hacking into password-protected accounts, including AOL, CompuServe, Yahoo and Hotmail, "so you can have access to it all the time and the owner of the account cannot find out that you have access." BAH's fees for password hacking begin at $399 and are payable in installments.

(U) In the mid-1990s, a notorious hacking group called the Phone Masters also operated a Web site that offered "professional" services such as hacking into telephone and credit reporting databases for a fee, according to Yarborough, who was involved in the US government's prosecution of the case. In September 1999, the leaders of Phone Masters were convicted on hacking charges and sentenced to more than two years in prison (USCG, Newsbytes). BAH is at http://www.beahacker.com/caseinfo2.htm. The US computer fraud statute is at http://www.cybercrime.gov/1030_new.html

D. OTHER

1. (U) Software Enables CCTV and Computers to Prevent Crime: Scientists at Kingston University in London have developed a software system that analyzes patterns of behavior captured from images from closed-circuit television (CCTV) cameras. The Cromatica software relies on mathematical algorithms to predict criminal or potentially harmful behavior. The computer sends the prediction to a human monitoring the system to make a determination on what action should be taken (21 Apr 02, Ananova).
http://www.ananova.com/news/story/sm_571906.html

2. (U) 75 Billion Text Messages Sent so Far This Year: Mobile Data Association claims that seventy-five billion text messages, a 50 percent increase over the same period last year, were sent in the first quarter of 2002. The total predicted messages for 2002 is 360 billion messages, a 110 billion rise over 2001 (22 Apr 02, Ananova).
http://www.ananova.com/news/story/sm_572599.html

CIOP-ACE (195)
SUBJECT: Cyber Threat Summary 011-02

3. (U) The Invisible Lightness of Beams: A Los Angeles company, Terabeam, delivers high-speed Internet access though laser beams aimed through office windows. The company utilizes technology developed during the Cold War that enabled submarines to communicate through blue-green lasers linked to satellites. An infrared version enables the company to install laser transmitters on the top of high-rises to send data without wires. The service costs about $2,000 per month (19 Apr 02, Los Angeles Times). http://www.latimes.com/technology/la-000027771apr19.story

4. (U) US Army to Centralize Network Security Scanning: The US Army and the Harris Corporation signed a contract to implement the centralized network security vulnerability assessment tool, Security Threat Avoidance Technology scanner, to increase website security. The tool will automate the process of applying software patches for around 1.5 million workstations. Alan Paller of SANS believes the automatic system will increase the likelihood of a more secure system (22 Apr 02, Computerworld). http://www.computerworld.com/storyba/0,4125,NAV47_STO70379,00.html

5. (U) Justice Program Looks for Ways to Share Crime Data With States: SEARCH members, a program sponsored by the Justice Department's National Criminal History Improvement Program, have taken steps recently to educate law enforcement and policymakers on technology that will greatly upgrade the criminal justice system in light of the Bush administration's information sharing initiatives. Members of SEARCH primarily include "state-level justice officials responsible for operational decisions and policymaking on the management of criminal-justice information" (19 Apr 02, Federal Computer Week). http://www.govexec.com/dailyfed/0402/042202td1.htm

6. (U) Gates Testifies: Microsoft Chairman Bill GATES took the witness stand on 22 Apr 02, in the on-going anti-trust case. GATES demonstrated how the settlement proposal of the nine states involved in the suit would undermine the Microsoft Windows operating system. He explained that removal of blocks of code, such as the code of Internet Explorer, would undermine the stability of other functions of the system. GATES also claimed that releasing the source code of the system would allow competitors to develop copycat systems. GATES' questioning is expected to last two days (22 Apr 02, Wired News). http://www.wired.com/news/antitrust/0,1551,52019,00.html

7. (U) Picking up the Pace at the Border: Over 60 companies recently agreed to equip their trucks with transponders in exchange for quicker processing time by the US Customs Service. The agreement will increase border security by electronically transmitting information about the cargo via the transponders to stations in Detroit and Port Huron, Michigan and Laredo, Texas. Imports will be processed in seconds rather than hours. Participating companies, which include General Motors Corporations, Target Corporation, and Sara Lee Corporation, also agreed to increase their own security measures of goods, and perform more rigorous background checks for employees. More than 100 companies are still awaiting application processing to participate

in the nationwide plan (22 Apr 02, Federal Computer Week).
http://www.fcw.com/fcw/articles/2002/0422/pol-custom-04-22-02.asp

8. (U) Senate Passes Border Tech Bill: The Senate unanimously approved a $3.2 billion bill sponsored by Senate Judiciary Immigration Subcommittee Chairman Edward KENNEDY (D-Mass) on 19 Apr 02. The bill will increase US border security through the use of biometric technologies and various other security technologies. Goals of the bill include: the ability to generate a database from law enforcement sources that will aid immigration officials to prohibit entrance of possible terrorists; the utilization of biometric identifiers, such as fingerprints or retinal scans, that will be required in all travel documents for anyone entering the country; the ability for the government to track foreign students on temporary visas; and the ability to scan overseas jetliners' passenger lists entering the country as well for possible terrorists. President BUSH is expected to sign the new bill into law after both the House and the Senate make additional revisions (19 Apr 02, Federal Computer Week).
http://www.fcw.com/fcw/articles/2002/0415/web-border-04-19-02.asp

9. (U) Plans For Secure Federal Intranet Moving Forward: The Bush administration received confirmation on 19 Apr 02, that a government-wide Intranet could be created, which will be called "GovNet". The next step in the GovNet project is to determine whether the new system will be cost effective, and what form the new system should take (19 Apr 02, Newsbytes). http://www.newsbytes.com/news/02/176029.html

10. (U) Can Search Engines Track Down Terrorists: Several search companies are offering technology to help government agencies organize their records. It could stop anti-terrorist information from falling through the cracks.

(U) Some US government officials engaged in the so-called war on terror would like to see privacy laws relaxed so they can get better access to email and other sensitive material exchanged over the Internet. Tracking down terrorists, after all, does not necessarily require intercepting top-secret conversations. Sometimes it is a more mundane task of making sure one government agency can share its records with another.

(U) Speculation has been rife, for instance, that 11 September hijacker Mohammed ATTA might not have been allowed back into the United States last year if officials at the INS had known about an outstanding warrant for his arrest resulting from a Florida traffic violation. There is also the curious case of Ziad Samir JARRAH, the hijacker believed to have seized the controls in the United Airlines flight that crashed in Pennsylvania. JARRAH remained on the FAA mailing list long after 11 September, and just this month the FAA sent a newsletter to his old address in Florida.

(U) Communication between different agencies is not the only problem. Some government agencies cannot even access critical documents produced by their own employees, if those

records have never been transferred out of email. Yet another problem is that foreign-language documents can fall through the cracks because many computers are not advanced enough to read them.

(U) Several Internet search engines and software makers are trying to address those challenges. Companies like CMGI's AltaVista and Inktomi, which started out organizing the billions of documents on the Web, today are selling similar technologies to help government agencies organize all the material they have collected over the years. These companies say many government offices that are bogged down in paper and old computer records constitute a promising market for their services, especially at a time that so many private-sector businesses are cutting back on tech spending (23 Apr 02, ZDNet News).

11. (U) Secret Service Targets Cyber-Criminals: The US Secret Service is establishing an Electronic Crimes Task Force in nine cities, aimed at helping businesses combat cyber-crimes. The task force is a public-private partnership between federal, state, and local law enforcement, as well as private industry experts in many fields, including telecommunications and financial services. The goal is to reach out to local industry and law enforcement experts to create a network that businesses and the agency can rely on for prevention of cyber-crimes. The task force will operate in Boston, Charlotte, Chicago, Miami, New York, Las Vegas, Los Angeles, San Francisco, and Washington, DC. (22 Apr 02, USCG/Miami Herald).

12. (U) Search Engine Removes Link to Railway Sabotage Guide: AltaVista Corporation removed from its search engine hyperlinks to a Web site with articles detailing how to sabotage railway systems after Deutsche Bahn AG, the German national railway operator, threatened to take legal action. The Web address for the site, which contains articles from Radikal, a German-language, left-wing extremist publication that is illegal in Germany, will be put on AltaVista's "banned list," AltaVista spokesman Karl Gregory said. Deutsche Bahn announced that it would sue the Palo Alto, CA based AltaVista and Yahoo Incorporated and Google Incorporated, if they didn't remove hyperlinks to two articles published under the headline "A handbook for destruction of railroad transport of all kinds." If it files suit, Deutsche Bahn will do so in Germany, where all three search engine companies have subsidiaries. The company feels it wouldn't stand a chance in a US courtroom because of the First Amendment to the US Constitution (22 Apr 02, USCG/IDG.net).

CID COMMENT: In the interest of national safety and security, government agencies are reminded to review their publicly accessible Websites to ensure all content is accurate and credible and authorized for public release.

CIOP-ACE (195)
SUBJECT: Cyber Threat Summary 011-02

E. CYBERTERRORISM-INFRASTRUCTURE PROTECTION

1. (U) Hijacked Web Sites Can Become Weapon in Terrorists' Arsenal: Atlanta security consultant Jim CAVANAGH demonstrates the ease with which the steganography technique can be used to hide secret messages or plans in data transmitted through the Internet. He teaches students to take a digital picture, encrypt the image with freely downloadable tools, and hide the image on websites with poor security. CIA director George TENET claims that Osama bin Laden utilizes this technique to hide coded messages for his followers (21 Apr 02, Augusta Chronicle). http://augustachronicle.com/stories/042102/bus_risk2.shtml

2. (U) Technology Being Used to Root Out al-Qaeda: United States intelligence agency officials have noted that there is increased Internet communication, largely originating in northwest Pakistan, between members of the al-Qaeda organization. Monitoring and interception electronic and other forms of communication has led to the arrest of Abu ZUBAYDAH of al-Qeada as well as the suspected kidnappers of Wall Street Journal reporter Daniel PEARL. Additionally, laptops of suspected al-Qaeda members have been analyzed and plans of future activities have been uncovered. However, the Internet continues to be a tool for terrorist and extremist groups, and the United States government has released warnings that critical or sensitive information regarding the critical infrastructure systems should be removed from unauthorized access (19 Apr 02, USA Today).
http://www.usatoday.com/life/cyber/tech/2002/04/19/al-qaida-online.htm

3. (U) Federal Cybersecurity Agency Gets New Name: Bureau of Export Administration, which is part of the US Department of Commerce, was renamed the "Bureau of Industry and Security" on April 19, 2002. Prominent responsibilities include coordinating all of the Commerce Department's homeland security tasks, acting as liaison between the federal government and the private sector on critical infrastructure protection and cyber security issues, and guaranteeing that specific cutting-edge technologies are not exported to countries hostile toward US interests (19 Apr 02, Newsbytes). http://www.newsbytes.com/news/02/176030.html

POC for this report is SA Sharmila Vaswani, (703) 806-4909.