



TECHNOBABBLE

The DCIS Cyber Crime Newsletter



TECHNOBABBLE
Volume 2, Issue 3

May, 2001

This issues suggested computer crime bookmarks:

Pittsburgh Cyber Crime Task Force:
<http://www.cyber-response.org>

Information Systems Security Association (ISSA):
<http://www.issa.org>

High Tech Crime Investigation Association:
<http://www.htcia.org>

Inside this issue:

DoD Employee Indicted in Computer Payroll Scheme.	1
Criminal Splurges on Internet Spending Spree.	1
The Cyber Survey Says-Cost of Cyber-crimes Soaring.	2
Suggested Reading: "High Technology Crime Investigators Handbook."	3
On the Trail of Cybersmugglers.	4
Viruses—Now they are Political.	5

DoD Employee Indicted in Computer Payroll Scheme

On April 18, 2001, a five-count indictment was filed in U.S. District Court for the Eastern District of Virginia, Alexandria, VA, against Tasha Y. Kinney, Suitland, MD. The indictment charges that Kinney committed wire fraud against the Government.

Kinney worked for the Defense Information Systems Agency (DISA) as a secretary and time and attendance (T&A) keeper. DISA is the U.S. Department of Defense's primary Information Systems management agency. As such, DISA manages the majority of Defense Department computer systems located throughout the country.

A Defense Criminal Investigative Service (DCIS) investigation revealed that from approximately April through November 2000, Kinney illegally accessed the Defense Civilian Payment System, a Defense Department Computer Network utilized to issue pay to Department employees.

Kinney allegedly utilized a former T&A keeper's username and password to fraudulently add overtime to her own record. Kinney resigned from DISA after admitting to entering and receiving over \$25,000 in unauthorized overtime pay.

DCIS special agents conducted the investigation in conjunction with investigators from DISA's Office of the Inspector General (OIG). Prosecution of the case is being handled by the U.S. Attorneys Office, Eastern District of Virginia.



Criminal Splurges on Internet Spending Spree

On April 2, 2001, Barry Parks, Jr., pled guilty in the Southern District of New York to one count of use of an unauthorized access device.

The plea was the result of a one-count indictment returned on October 25, 2000.

A Defense Criminal Investigative Service (DCIS) investigation disclosed that Parks utilized stolen DoD officials' Social Security Numbers to obtain First USA Bank Visa cards.

Parks opened 45 Visa accounts with First USA Bank and made purchases in excess of \$20,000. The purchases were made through the Internet at 10 sites, including Amazon.com, Nike, and Damark. The merchandise was delivered to Parks' residence, as well as the residences of associates.

DCIS investigated the case in conjunction with the the U.S. Secret Service and the Social Security Administration, Office of the Inspector General. The U.S. Attorneys

Office, Southern District of New York, is handling the prosecution of this matter.



The Cyber Survey Says... Cost of Cybercrimes Soaring

Reprinted from CSI Press Release dated May 12, 2001

On May 12, 2001, the Computer Security Institute (CSI) announced the results of its sixth annual "Computer Crime and Security Survey."

The "Computer Crime and Security Survey" is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States.

Based on responses from 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2001 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

Highlights of the "2001 Computer Crime and Security Survey" include:

Eighty-five percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.

Sixty-four percent acknowledged financial losses due to computer breaches.

Thirty-five percent (186 respondents) were willing and/or able to quantify their financial

losses. These 186 respondents reported \$377,828,700 in financial losses. (In contrast, the losses from 249 respondents in 2000 totaled only \$265,589,940. The average annual total over the three years prior to 2000 was \$120,240,180.)

As in previous years, the most serious financial losses occurred through theft of proprietary information (34 respondents reported \$151,230,100) and financial fraud (21 respondents reported \$92,935,500).

For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001.

Thirty-six percent of respondents reported the intrusions to law enforcement; a significant increase from 2000, when only 25% reported them. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

Respondents detected a wide range of attacks and abuses. Here are some examples of at-

tacks and abuses on the rise:

Forty percent of respondents detected system penetration from the outside (only 25% reported system penetration in 2000).

Thirty-eight percent of respondents detected denial of service attacks (only 27% reported denial of service in 2000).

Ninety-one percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems). Only 79% detected net abuse in 2000.

Ninety-four percent detected computer viruses (only 85% detected them in 2000).

For the third year, CSI asked some questions about electronic commerce over the Internet. Here are some of the results:

Ninety-seven percent of respondents have WWW sites.

Forty-seven percent conduct electronic commerce on their sites.

Twenty-three percent suffered unauthorized access or misuse within the last twelve months. Twenty-seven percent said that they didn't know if there had been unauthorized access or



"The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. ."

misuse.

Twenty-one percent of those acknowledging attacks reported from two to five incidents. Fifty-eight percent reported ten or more incidents.

Ninety percent of those attacked reported vandalism (only 64% in 2000).

Seventy-eight percent reported denial of service (only 60% in 2000).

Thirteen percent reported theft of transaction information (only 8% in 2000).

Eight percent reported financial fraud (only 3% in 2000).

Patrice Rapalus, CSI Director, remarks that the "Computer Crime and Security Survey," now in its sixth year, has served as a reality check for industry and government:

"Each year, the influ-

ence and impact of the CSI/FBI Computer Crime and Security Survey grows. It is an invaluable tool for information security practitioners in corporations and government agencies struggling to get the attention of their CEOs, CIOs and CFOs as well as for law enforcement officials working to make the case for closer cooperation with the private sector to stave off a cyber crime wave. The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a

comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprise-wide information security."

Bruce J. Gebhardt is in charge of the FBI's Northern California office. Based in San Francisco, his division covers fifteen counties, including the continually expanding Silicon Valley area. Computer crime is one of his biggest challenges.

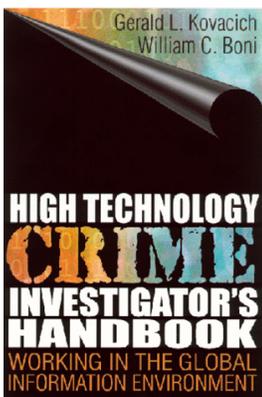
"The results of this year's survey again demonstrate the seriousness and complexity of computer crime. The dynamic vulnerabilities associated with conducting business on-line remain a law enforcement challenge."

For more information, check out :

www.gocsi.com

This Issues Suggested Reading

High Technology Crime Investigators Handbook



Is your Department or organization interested in forming a High Tech Crime Investigation Unit, but doesn't have a clue as to where to start, or how such a unit should be organized and managed. *The High Technology Crime Investigator's Handbook* may be able to provide some suggestions that could help your organization develop a unit in a professional, logical manner.

As one Amazon.com on-line review puts it:

"Whether you're a law enforcement or corporate security professional, this book is one you should not just read but thoroughly digest before stepping off the ledge into high tech crime investigation. I've had both the satisfaction and frustration of managing investigations in both worlds over the last 16 years and have experienced, first hand, the hazards and consequences that await the uninformed. If resources such as the High Technology Crime Investi-

gators Handbook had been available when I first began working high tech crimes in 1981, I would have gratefully traded the experience for the knowledge."

Authors:
Kovacich & Boni

Cost: **\$34.95**

ISBN: **0-7506-7029-0**

Publisher: **Butterworth Heinemann**

On the Trail of Cybersmugglers

Customs Center Hunts Criminals on the Internet

Reprinted from Government Computer News, April 30, 2001

by Preeti Vasishtha, GCN Staff

Submitted by Special Agent Stan Newell, DCIS New Jersey Resident Agency

Federal agents helped rout an alleged Internet child pornography ring last month when four suspects in the United States and five in Russia were arrested.

For the Customs Service's CyberSmuggling Center in Fairfax, Va., the investigation, dubbed Operation Blue Orchid, was just another case cleared.

Last May, Moscow police requested the assistance of the U. S. Customs attaché to investigate individuals running a Web site, hosted at www.geocities.com, that distributed pornographic videos of children.

The Customs attaché contacted the center, which conducted an undercover purchase of a video, resulting in the arrests and closure of the site.

Battling child pornography on the Net is just one of the center's jobs.

Envisioned in 1997 and dedicated in 2000, the CyberSmuggling Center fights crime via the Internet, including money laundering, drug trafficking, intellectual property theft and illegal arms trading.

"We have not found any new crimes as a result of the Internet," center director Kevin Delli-Colli said. Criminals "are just finding new ways to commit old crimes."

Customs first came across computers being used for child pornography in 1989 by monitoring online bulletin boards. But the advent of the Web intensified the problem.

The CyberSmuggling Center was Customs' answer to keep pace, and child pornography remains the center's main focus.

It has partnered with the National Center for Missing and Exploited Children in Alexandria, Va., which operates a toll-free hotline through which people can pass on information about child porn on the Internet. The tips are made available daily to law enforcement agencies, specifically Customs, the FBI and the Postal Service.

Cyber skill set

The CyberSmuggling Center has an annual budget of \$4 million and 37 employees, including agents and criminal investigators, some with training in computer forensics.

"Any time you have an Internet-related crime, you have computers at both ends, and you need people who can examine that for evidential purposes," Delli-Colli said.

Besides the director, there are three assistant directors who head the Child Exploitation, Computer Forensic and Cyber-crimes units.

The Computer Forensic Unit examines computers used in other crimes and trains field agents. It also works with the Bureau of Alcohol, Tobacco and Firearms, IRS and Secret Service to standardize forensic software, methods and training techniques.

Tech cramming

The training, called the Computer Investigative Specialist

Program, involves two weeks of studying major PC operating systems and hardware components through a Computer Technology Industry Association certification program. Examiners also take two and a half weeks of advanced computer evidence recovery training, targeting network OSes.

The agents use souped-up PCs they've dubbed forensic media analysis desktops to conduct laboratory-like examinations in the office. The PCs are customized for the center.

"To go out and buy a computer that just has our needs and our forensic tools is somewhat different from a standard commercial box," said James Thomas, a Customs senior special agent. "We want swappability of hard drives and components. We'll take this drive out and put another one in. We use different operating systems."

To build these systems, Customs hired Skytech Inc. of Alexandria, Va. The 800-MHz Pentium III PCs can support as many as seven hard drives and run Microsoft Windows 98, Windows 2000 or Linux, Skytech president Cat Crosby said.

"They are made in such a way that the agents can hook up any hardware device to the desktop PCs," she said.

The computers are designed to extract data from any media: hard drives, floppy disks, tapes, magneto-optical disks, CD-ROMs, CD-RWs, DVDs, flash disks, and Zip and Jaz drives. The PCs also are equipped with specialized software for field exams of suspects' computers.



"We have not found any new crimes as a result of the Internet," center director Kevin Delli-Colli said. Criminals "are just finding new ways to commit old crimes."

Forensic tools for the preservation, recovery and analysis of digital evidence include Safe-Back from New Technologies Inc. of Gresham, Ore.; EnCase from Guidance Software of Pasadena, Calif.; and Norton Utilities from Symantec Corporation.

Agents will soon be able to access a dedicated server via a virtual private network. The server will host a Web site that lets agents communicate, get technical support and download upgrades to their field software.

Because the Internet is boundless, agents sometimes find themselves working outside of

their jurisdictions.

“On the Internet, you don’t know where your criminal is,” Delli-Colli said. “It could be someone across the street or [across] the country.”

Usually, law enforcement agencies assign agents to a case depending on the jurisdiction or area in which the case falls, he said. But often, cooperation from other countries becomes critical.

According to Thomas, laws in the United States have not caught up with technology. “All laws refer back to documentary evidence,” he said. “Some of

them do not apply to the digital evidence.”

Once assigned to a case, the agents find the computer that was used in the crime and make forensic images of the machine’s guts.

“Forensics image is the bit-by-bit transfer of the machine, and then with the image we try and find the information that is relative to the offense,” Thomas said.

The trouble is that some judicial districts have not agreed on whether original evidence or its exact image is the best evidence, he said.

“According to Thomas, laws in the United States have not caught up with technology. “All laws refer back to documentary evidence,” he said. “Some of them do not apply to the digital evidence.”

Viruses-now they are Political

*Reprinted from Government Computer News, April 30, 2001
by William Jackson—Cyber Eye Columnist
Submitted by Special Agent Stan Newell, DCIS New Jersey Resident Agency*

If anyone is wondering when information warfare will rear its ugly head, it’s already happened.

Infowar hasn’t come in the form of a cyber-Pearl Harbor, shutting down power grids and networks as doomsayers have predicted. It’s been more subtle. Infowar is arriving as propaganda aimed at American hearts and minds rather than at the nation’s critical infrastructure. So far, the attacks have been crude, low-cost Web site defacements, denial-of-service attacks and computer viruses.

The most recent was the Injustice worm, which carried a text payload that exhorted recipients to “help us to stop the bloodshed” by Israeli security forces against Palestinians. The worm directed a recipient’s browser to pro-Palestinian Web sites and mailed itself to the first 50 ad-

resses in the recipient’s Microsoft Outlook address books, as well as to 25 Israeli addresses.

I doubt that it generated much sympathy for the Palestinian cause, but the creators seem to have had some consideration for their targets. The worm updated a value in the Windows registry to ensure that each recipient got only one copy of the infected e-mail. For the Israeli addresses targeted with every copy, however, wide distribution would have equaled a denial-of-service attack.

By their very nature, worms and viruses are not good vehicles for favorable propaganda. They inspire only anger, frustration and an immediate effort to stop their spread.

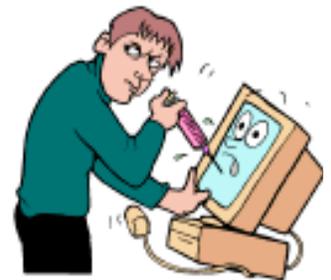
Such random violence accomplishes little, but that hasn’t stopped terrorists from using

bombs and bullets.

The usual rules apply in stopping politically motivated computer terrorism: Keep antivirus engines updated, and don’t open unexpected attachments. Of course, such precautions are no more likely to be universally adopted in the future than they have been in the past.

The best bet to stop new viruses and worms probably is software that monitors the behavior of the attachments floating about in systems. When a piece of code misbehaves, the software blocks it.

You might be far from trouble spots on the other side of the globe. But you could become a victim of the next flare-up in the Middle East, Europe, Asia or Latin America if you don’t take precautions now.



*A publication of the DCIS
Northeast Field Office*

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: lives@dodig.osd.mil

We're on the Web!

www.dodig.osd.mil/dcis/dcismain.html



The Defense Criminal Investigative Service

"Protecting America's War Fighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.

10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency

Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency

525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency

Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency

One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty

1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency

441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099