SCANNERS

SHORTWAVE

THE URBAN DX'ER

Vol.10 No1
January, 2005
NYDXA@yahoo.com

Established 1984

BIG BROTHER'S INTENTIONAL JAMMING!

During last years Republican convention in NYC, many people reported that their cell phones and other wireless devices were inoperative in and in the vicinity of Madison Square Garden. A frequent contributor to our group, working within MSG confirmed that some sort of intentional "wide band" nose was intentionally being generated presumably to prevent the use of cellular devices for "illegal or terrorist" purposes. An anonymous source passed on this memo that confirms the use of such technology.

"*ADVISORY MESSAGE: Here is some additional information regarding Electronic Counter Measures "ECM" that appear to have been used at both conventions and again last week at the Presidential Inauguration.*

During the 55th Presidential Inauguration it was clearly evident to us that the USSS deliberately placed into service RF Jamming Technologies that caused severe interference to our wireless microphones, wireless ifb's and 2-way radio systems.

Additionally, "Public Switched Wireless Networks" such as AT&T, Verizon, Nextel, Skytel Sky Paging, Cingular, T-Mobile, Blackberry and other forms of wireless communications normally available to the public at large were rendered "in-operable" from approximately 1030 Hrs on Thursday, 1/20/2005 until late in the afternoon as the festivities had concluded in front of The White House at Lafayette Park.

The end user would see a full signal strength indication on a cellular telephone but was unable to place or receive any calls during the "ECM" operations. Occasionally some users were able to place calls successfully but the general experience was that you were out of luck when using a wireless device.
The jamming signal appears as a very "wideband carrier" operating at extremely high power levels and sounds similar in nature to high power radar normally used by the military. During our operations in Boston we were told that the normal rf output power of the jammer was at levels which exceed 5KW. This form of security is surely to become a standard operating procedure for the US Secret Service and other US Government Security Agencies during high profile events and is clearly a technology which will have destructive impact on the various forms of wireless normally used by the networks. I hope that you may find the attached information useful."

NEW JERSEY DEMONSTRATES CAPACITY FOR ENHANCED INTER-AGENCY COMMUNICATIONS

<Editor's Note:> During the January 19th net, I mentioned some radio activity on the 800 mhz ITAC channels. The activity included an inter-agency drill in which various NY / NJ municipalities checked in. Here's the story what it was all about!

Last week, New Jersey officials demonstrated technological solutions they are using to enable personnel from different emergency agencies and first responder disciplines to communicate with each other using their existing radio equipment, Attorney General Peter C. Harvey announced.

At a press conference at Jersey City's Emergency Operations Center on Summit Avenue, Attorney General Harvey, State Police Lt. Col. Lori Hennon-Bell and federal, state and municipal officials, observed first responders from federal, state, local and other agencies demonstrate "interoperable" radio communication. Led by Raymond Hayling II, the state's Chief Public Safety Communications Officer, 12 different agencies were connected by tuning to assigned frequencies in their own band that are then connected through a central dispatching center. The 12 agencies represented federal, county, state and municipal governments and each operated on different radio frequencies among the 800 MHz, UHF and VHF spectrums. Prior to today's public demonstration, the system was tested with more than 40 agencies, including New York City OEM, FBI, NY/NJ Port Authority and other New Jersey public safety agencies.

"One of the many lessons of 9/11 was that first

responders -- primarily at the command level -- must be able to talk to each other. As the World Trade Center towers began to fall, an event witnessed from this very location, we know that police and firefighter commanders had numerous and debilitating problems communicating by radio with their own units and, most of all, with each other," said Attorney General Harvey, who also chairs New Jersey's Domestic Security Preparedness Task Force, the state's cabinet-level body that sets homeland security policy and oversees its implementation. "This is a great step forward for New Jersey."

"I am pleased that New Jersey is on the cutting edge in providing enhanced inter-agency communications," said Col. Rick Fuentes, superintendent of the New Jersey State Police. "As director of the State Office of Emergency Management, I know how vital it is that commanders from different first-responder agencies, whether law enforcement, firefighters, emergency medical services technicians or others, be able to communicate with each other. Effective inter-agency communication is critical to effective response to -- and management of -- emergencies. It is also critical to ensuring responders' safety."

Harvey said that the technology demonstrated today had already provided successful interoperable communications in the Northeastern New Jersey Urban Area Security Initiative (UASI) region this past summer during the Republican National Convention and during the period from August through November that the Homeland Security Alert System was elevated to orange status for the financial sector in Northern New Jersey based on threats against the Prudential building in Newark.

The inter-agency radio system had been developed as a priority of New Jersey's UASI, which includes the cities of Jersey City and Newark, as well as Bergen, Essex, Hudson, Morris, Passaic and Union counties. The UASI region has dedicated approximately $1 million in federal homeland security funds from the Department of Homeland Security (DHS) to facilitate enhanced inter-agency communications to this point.

Agencies that participated in last week's demonstration were: the United States Coast Guard; FBI; the New Jersey State Police (Troop B); NY/NJ Port Authority; the University of Medicine and Dentistry of New Jersey's REMCS Unit; Hudson County Prosecutor's Office; NJ Department of Transportation; Essex County Sheriff's Department; Passaic County Sheriff's Department; Jersey City Police Department; Jersey City Fire Department; Jersey City Emergency Medical Services; Newark Police Department; Paramus Police Department; Newark Fire Department; Nutley Fire Department/HazMat Unit.

Hayling said that New Jersey's current technological solution relies on existing frequencies being "patched" together on existing equipment through a central dispatch point. He said that a northern New Jersey law enforcement agency has been designated as the UASI region's "dispatch center" when inter-agency communications are required. Furthermore, Hayling noted that New Jersey's technological solution differs from those based on "interconnect switches," in which numerous radio systems are patched together through a separate piece of technology. Interconnect switches result in a "party line" connection, he said, in which many individuals and agencies may be indiscriminately linked. New Jersey's solution, on the other hand, results in a targeted "private line," helping to ensure that only the first responders key to any particular emergency are able to communicate. Hayling said that improvements to the system are ongoing.

In addition to the UASI region, two other regions of the state -- designated by the Domestic Security Preparedness Task Force -- are already using Task Force distributed planning grants to implement similar enhanced inter-agency communications systems. These are the Delaware River Region (Burlington, Camden, Cumberland, Gloucester and Salem counties) and the Central Region (Somerset, Middlesex, Mercer and Monmouth counties). Hayling said that the remaining Task Force designated regions (the Northwest Region -- Hunterdon, Sussex and Warren counties and the Shore Region -- Atlantic, Cape May and Ocean counties) would be coming online in the next few years.

In the long term, Attorney General Harvey said, the state ultimately expects to upgrade to a system that uses standardized radio equipment and frequencies. This will cost approximately $150 million to $200 million, he said.

According to Hayling, the system demonstrated allowed Jersey City to meet the standards of RapidCom 9/30, a Department of Homeland

Security initiative announced by President Bush in July 2004. RapidCom 9/30 required the demonstration of incident-level, interoperable emergency communications by September 30, 2004. It was designed to enable first responders in 10 cities identified by DHS as "high-threat urban areas" to communicate with each other in the event of a large emergency incident such as a terrorist attack.

GUESS WHAT T-MOBILE DOESN'T WANT YOU TO KNOW?
http://www.securityfocus.com/news/10271
http://www.wired.com/news/technology/0,1282,66265,00.html
Last week a story quietly broke with a few news services. Strangely, the major networks hardly mentioned it.

A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year, which he used to monitor U.S. Secret Service e-mail, obtain customers' passwords and Social Security numbers, and download candid photos taken by Sidekick users, including Hollywood celebrities. Though the exact numbers vary, it's now known that the hacker could access information on any of T-Mobile's 16.3 million customers. The information included many customers' Social Security numbers and dates of birth, according to government filings in the case. He <the hacker> could also obtain voicemail PINs, and the passwords providing customers with Web access to their T-Mobile e-mail accounts. He did not have access to credit card numbers.

What's interesting is, "*T-Mobile, which apparently knew of the intrusions by July of last year, has not issued any public warning. Under California's anti-identity theft law "SB1386," the company is obliged to notify any California customers of a security breach in which their personally identifiable information is "reasonably believed to have been" compromised. That notification must be made in "the most expedient time possible and without unreasonable delay," but may be postponed if a law enforcement agency determines that the disclosure would compromise an investigation".*

Because the details of this story are some extensive, I've attached PDF versions of the story as posted on two web sites.

WINTER WEATHER TRAFFIC CAMS
We're now well into winter weather and unexpected traffic snafu's are bound to happen. The NNJ Scan list recently published a list of cameras accessible over the Internet. These can be both informative and entertaining.
http://www.state.nj.us/transportation/traffic/cameras/rt37/rt37_13.2.shtm
http://www.state.nj.us/transportation/traffic/cameras/
http://www.nj.com/traffic/
http://www.state.nj.us/turnpike/nj-conditions-cams.htm
http://www.nycroads.com/roads/expwy_NJ/
http://www.metrocommute.com/video/newyork/indexnj.html
http://www.fortlee.com/htm/trafficams.htm
http://www.novartisinfo.com/common/skycam_both.htm

The last one is Route 10 east and west, in East Hanover, NJ at Ridgedale Road.

NOTABLE NYC UPDATES
Though some of these frequencies are beyond the reach of conventional scanners, it's still interesting to see how the wireless infrastructure continues to expand. The FCC's web site recently carried these updates for NYC's government communications.

5855 Mhz - INTELLIGENT TRANSPORTATION SERVICE
4940-4990 Mhz - WiFi for citywide access

MW - MICROWAVE PUBLIC SAFETY POOL
WNTL543 City of New York
23375 Mhz - 80-02 KEW GARDENS RD QUEENS (QUEENS) NY

WNTL544 City of New York
22175 Mhz - 125-01 QUEENS BLVD KEW GARDENS (QUEENS) NY

WNTN466 City of New York
21925 Mhz - BROOKLYN V A HOSPITAL 800 POLY PL BROOKLYN (KINGS) NY

WNTT788 City of New York
2462.188 Mhz (Mobile)
868.825 Mhz - unknown use

DOITT Trunked System Tranmsitter Locations for possible Phone Patch/FailSoft:
856.4375 Mhz - 1901 1ST AVE (METROPOLITAN HOSPITAL)
857.4375 Mhz - 3424 KOSSUTH AVE (NORTH CENTRAL BRONX HOSPITAL)

858.4375 Mhz - 82-68 164 ST (QUEENS GENERAL HOSPITAL)
859.4375 Mhz - 451 CLARKSON AVE (KINGS COUNTY HOSPITAL)

Low Power Repeater at 655 W 34 ST (JAVITTS CENTER)
857.2125 Mhz
858.2125 Mhz
859.2125 Mhz

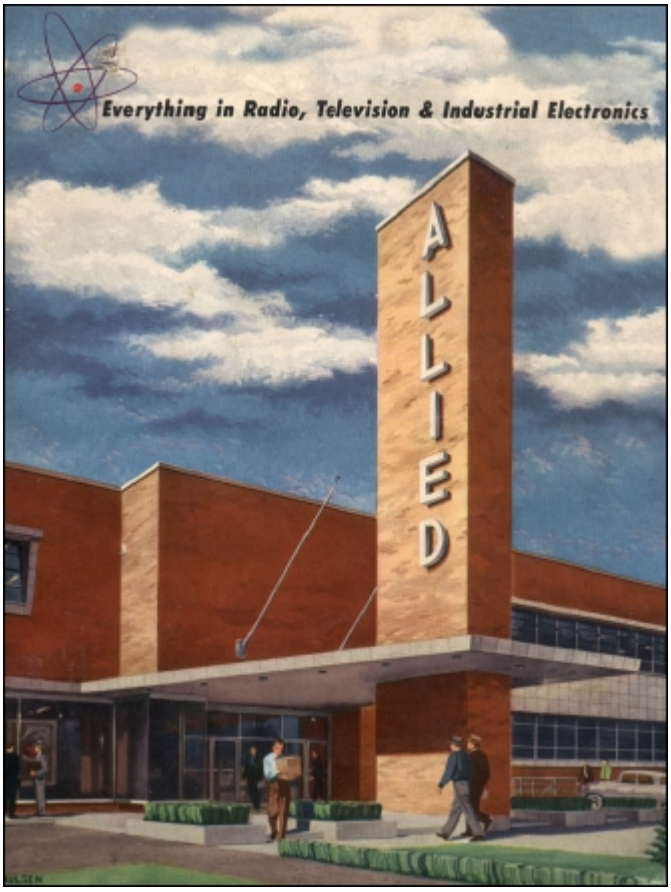
FDNY REPEATERS for STARFIRE II DATA SYSTEM
856.2125 Mhz
856.7375 Mhz
857.7375 Mhz
858.7375 Mhz
859.7375 Mhz

These frequencies will be used at locations in (RICHMOND) NY, BRONX HOSP, SEAVIEW HOSPITAL (RICHMOND) NY, QUEENS, COLUMBIA PRESBYTERIAN HOSP, CREEDMORE PSYCHIATRIC CTR, CARLYLE HOTEL NY, FRANK DE PAULO JHS, MUNICIPAL BLDG NEW YORK, NY and the Merril Lynch building in NYC.

LOOKING BACK
Newcomers to the radio hobby may not recognize the name Allied Radio or Knight Kit. For those of us who have been tinkering with radios back to the days when they had those strange glowing glass tubes instead of IC's, you probably learned how to solder building a Knight Kit.

Allied Radio (now known as Allied Electronics) is a company with a long eight decade history. It was founded in Chicago, IL. in 1928. Its purpose was to distribute radio parts for Columbia Radio Corp. By 1932, Allied was selling electronic parts by catalog. Storefront sales operations were established with the goal of selling to amateur radio operators and electronics experimenters. During WWII, Allied devoted itself to the war effort by handling government contracts and high-priority industrial needs. This was Allied's first real experience in industrial electronics. After the war, Allied continued to sell to the consumer and industrial markets. Sometime around 1962, Allied Electronics was created as a subsidiary of Allied Radio. In 1971, Allied was acquired by Tandy (now Radio Shack Corp.) and moved its headquarters to Fort Worth, Texas. Around 1981, Spartan Manufacturing acquired the company. In 1997, Avnet took over ownership. In 1999, Allied Electronics was acquired by Electrocomponents plc of the United Kingdom. Allied Electronics continues to sell electronic components by catalog and Internet ordering. Allied Radio produced a line of kits under the Knight label.

Thos of us here on the East coast probably never visited Allied Radio. Here's a few photo I found.of what Allied looked like in its heyday.



http://www.knightkit.com/covers.html
http://www.knightkit.com/allied.html

If you were a fan of Lafayette Radio, you might also enjoy these web sites!
http://www.cbgazette.com/laf3.html
http://www.daveswebshop.com/lafayetteradio.shtml

READER MAILBAG
"I've been meaning to tell you that you do a wonderful net every Wednesday night 9 pm(started listening like a month ago) and have a great website (very informative) I came across. Unfortunately I cant make that repeater its too far away for me. I would like to be added to the

newsletter if its possible. I also had a question; I came across the frequency, **143.280** its a Westchester Coast Guard aux radio or something first i though it was ham but its not but they use ham terms. I was wondering
if i can like get info about it if its ok.
I would like to speak to you on the air sometime i pretty much use the N2ROW/R in Brooklyn linked system 441.1 +5, 136.5 PL – "Ralph"

In response to your question Ralph, "*As for the 143.280 frequency, I am gathering some info on it to post on the website. It is indeed a Coast Guard Auxiliary repeater that has counterparts in other areas using different PL tones. Many stations that you hear on them are ham radio operators who joined their local USCGA flotilla. – Charlie, N2NOV*"

DEP

NYC DEP <Dept of Environmental Protection> Police Aviation unit which has been mentioned on the net before. Several mentions on various scanner groups have discussed that DEP & DOITT are working on some sort of new radio system for the DEP Police to replace the 37.50 mhz now in use. This channel is shared with the watershed engineers. It's quite possible that the new license mentioned below will replace 37.50. You may want to monitor 151.235 to see what pops up. My guess is that it will be in the Apco 25 format.

Air Beat Magazine had an interesting article on this operation. The article is attached in PDF and the link to view the site directly is at
http://www.alea.org/public/airbeat/back_issues/nov_dec_2004/diverse_missions.htm

WQBR907
City of New York
[applicant is the city of New York. system will be used to coordinate the official business of the licensee.]
ctrl pt 1 - NYC DEP BWS/DWQC SUTTON PARK OFFICE VALHALLA NY

1 - ROXBURY DRIVE YONKERS (WESTCHESTER) NY
151.235 131' FB 35e
20K0F1E Digitized Voice (possible encryption)
2 - 121 LOZZI DRIVE MT. PLEASANT (WESTCHESTER) NY
151.235 180' FB 35e
20K0F1E Digitized Voice (possible encryption)
3 - 96 LILY POND LANE KATONAH (WESTCHESTER) NY
151.235 49' FB 35e
20K0F1E Digitized Voice (possible encryption)
4 - 24 KMRA around site 2
151.235 MO 100x35e
20K0F1E Digitized Voice (possible encryption)

WFM ACTIVITY

For those of you who happen to have radios that can tune wideband FM in the old (40-MHz) band here's something of interest.

An experimental station WB3XXE has been licensed under STA for the next six months or so to broadcast from the Armstrong tower in Alpine, N.J. with 250 W on 44.1 MHz in wideband FM. The Philly-based engineer who built it (and unfortunately whose name I did not catch) has been operating the station intermittently with classical music from CD using a home-brew Phasotron transmitter into a modified 6-m dipole antenna mounted on the middle arm of the Armstrong tower. The station has an Optimod 8100A for processing. The owners of the site are planning a public commemoration of Armstrong's life and work for some time later this summer.

The station was operational during the SBE15 meeting held in Armstrong's former office last Thursday evening. According to the operator, it was being copied in Philadelphia, as well as on a restored Stromberg-Carlson console set in Armstrong's former laboratory. Plans are to move the station to 42.8 MHz at some point before the public event.

FREE PRO-83 SOFTWARE

There is a freeware program to load frequencies and search ranges for the Pro-83. The program is called Load83 and is available through the Yahoo Groups in the Pro-83 group. You must become a member to download. The program has been tested; it works great and it's very simple to use – best of all it's free! This program uses the same programming cable as the Pro-92.

WHAT'S CONFIDENTIAL – WHAT'S NOT

With the heightened security that's entered our daily lives, from time to time we receive well intended warnings, suggesting that some of the information we offer might be construed as "confidential." In the February 2005 issue of Monitoring Times, Bob Grove responds to this topic. Monitoring Times is read worldwide and many who subscribe are in fact with the three letter government agencies. His response summarizes the situation very well. While the information we

include may not be one click away on Google, all of it is public. Finding such information is a matter of knowing where o look and what terms to search on. If any information contained in any issue can be proven "confidential" we'll gladly remove the information from the newsletter archives.

Milcom Accountability

Soon after publication of our December issue, we received this courteous letter of concern regarding an item in the Milcom column on National Guard HF ALE addresses

Morning Mr. Van Horn,
I would like to inform you that the information you're disclosing (Monitoring Times) about the NG HF Radio Net is considered FOUO [For Official Use Only – ed.] and should not be released without approval from NGB. This net is stood up in support of Homeland Security in case the unthinkable happens. By disclosing this info, you make our net unreliable during a crisis situation. I can't tell or make you do anything, but I hope you can understand the consequences of your actions. This is not a call to beat anyone up; this is a call for support.
God Bless (name withheld by MT)

<Bob's response>
"The Monitoring Times staff appreciates such expressions of concern, and we do hear from supervisory officers on occasion. We are encouraged to know that such officers are vigilant in their efforts to protect our country's security. In this case, the National Guard band plan has been in public domain for decades, and there is no possibility of classifying what is already in wide, public circulation. New listings, however, can be classified, although transmissions in the clear will still remain vulnerable to discovery and identification. The details in our article were contributed by casual monitors of the spectrum, not by official sources, and point out the one gaping fallacy in an effort to curb the proliferation of such information: A radio system is only as secure as its operators make it. The old military adage, "Loose lips sink ships," is as valid as ever. But if we felt that there was any danger in the publication of such information, it would not have appeared in print; MT is an informational, not a sensational, magazine. Because of its authority and accuracy, its subscribers include many levels of federal/military intelligence. Grove Enterprises (publisher of Monitoring Times) is continuously sought by these agencies for equipment recommendations. Historically, government radio communications in the clear have had no expectation of privacy; that is the reason that radio systems that handle sensitive and tactical communications are equipped with encryption and scrambling capability. The lack of their use does not impose any restrictions on someone who happens to overhear that unguarded transmission. It is the responsibility of the sender to provide measures to protect its security. Complete system disruption by deliberate interference is virtually impossible due to propagation characteristics, and government radio-direction-finding equipment sits ready to locate such miscreants. We thank our concerned reader for contacting us, and hope that this response is reassuring. – Bob Grove, Publisher"

HAPPY ANIVERSARY!

This issue of The Urban DX'er marks the beginning of it's 10th year complimenting our weekly net. For those of you who are new to our group, you might find its origin interesting.

The original Urban DX'er was first published back in April 1984 by Charles Hargrove, N2NOV and continued for only eight issues. There was a diverse collection of articles and columns. In some issues the club's founder, Greg Baker, wrote a column called "Beyond the Ether". The newsletter (magazine) was typed on an old Smith-Corona portable typewriter and the pages pasted onto landscaped 8.5" x 11" paper. It was then folded in half and spine-stapled so that it was a mini-magazine.

For example, Issue #2 (May 1984) had the following in it's Table of Contents:
London Calls Close to Home.....Pg 2 - "London Calling" Ad in NY Times a First!
Chasing the FM Pirates of NYC...Pg 5 - The Great WHOT Hunt
BBC's Special Programming.....Pg 9 - Programming Notes
The Perverted Vee (Antennas)....Pg10 - Antennas Using PVC and Wires
Bonnie Coot Joins NYDXA.....Pg13 - Regular Monthly Column
Peking Also Has SW Pirates.....Pg15 - NY Times Article
May Frequency Changes.....Pg16 - DW, Sri Lanka, Australia, Liberia,
Algeria, Columbia

Issues were offered for $.50 or 3 IRCs for a sample

and $5.00/year. With no subscribers outside of our local membership, publication ceased due to unnecessary expense since they were all sharing this info at monthly meetings anyway. They had a DX Hotline on Charlie's answering machine where everyone shared what was heard on the Shortwave bands. Info left on the incoming tape was summarized on the outgoing tape for all to hear and make use of. Early members of the group include Bill Bergadano (KA2EMZ), Ken Newman (K2JLK), Sig Hoffman, Dr. Mike Schuster and others. They tried to have the club affiliated with ANARC (Association of North American Radio Clubs) but
were told that they were only interested in "specialty" clubs and not a general purpose radio group. As the years have gone by, the NYDXA has been an organization that "specializes" in the needs and interests of listeners in the urban setting of metropolitan NYC and it's surrounding counties.

While writing some stories for Monitoring Times I heard about a weekly scanner net held on a repeater in Bayonne, NJ. I'm not quite sure how, but before too long I was helping Charlie run the net.
About this time we had a group of very dedicated jammers who got enjoyment disrupting the net. Little did they know that we were a bit more persistent and a bit more resourceful! It didn't take long before many people got frustrated and started leaving the net. Charlie and I got the idea to create a newsletter, as a temporary means of keeping everyone updated.

For about 6 months the newsletter was distributed by US mail. That got expensive and we realized that we had to come up with a better way. About this time I was introduced to a new piece of software,
Adobe's Acrobat! Acrobat and my newly acquired dial up Internet account gave birth the present Urban DX'er. During its first two years the net moved to a few different repeaters, hoping the jamming wouldn't follow. It did but we refused to give up. Eventually, a few of the people who participated had enough and let's just say that things started happening!

The "temporary" newsletter now in it's 10th year, is currently distributed via e-mail to many scanner / SWL enthusiasts. As far as I know, it's probably the longest running free newsletter of its kind. Its success is due to the informative contributions we receive and to the weekly participation. The thanks and credits go out to all who have participated over the 10 years!

Urban DX'er would like to thank all those who contributed to this month's issue!
Charlie - N2NOV, Dave, KE2SL, Bob, N1MLZ, "Joe S.", KC2GIK, "anonymous" and N2HWY

SECURITYFOCUS NEWS

Hacker penetrates T-Mobile systems

By ***Kevin Poulsen***, SecurityFocus Jan 11 2005 7:43PM

A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year, which he used to monitor U.S. Secret Service e-mail, obtain customers' passwords and Social Security numbers, and download candid photos taken by Sidekick users, including Hollywood celebrities, SecurityFocus has learned.

Twenty-one year-old Nicolas Jacobsen was quietly charged with the intrusions last October, after a Secret Service informant helped investigators link him to sensitive agency documents that were circulating in underground IRC chat rooms. The informant also produced evidence that Jacobsen was behind an offer to provide T-Mobile customers' personal information to identity thieves through an Internet bulletin board, according to court records.

Jacobsen could access information on any of the Bellevue, Washington-based company's 16.3 million customers, including many customers' Social Security numbers and dates of birth, according to government filings in the case. He could also obtain voicemail PINs, and the passwords providing customers with Web access to their T-Mobile e-mail accounts. He did not have access to credit card numbers.

The case arose as part of the Secret Service's "Operation Firewall" crackdown on Internet fraud rings last October, in which 19 men were indicted for trafficking in stolen identity information and documents, and stolen credit and debit card numbers. But Jacobsen was not charged with the others. Instead he faces two felony counts of computer intrusion and unauthorized impairment of a protected computer in a separate, unheralded federal case in Los Angeles, currently set for a February 14th status conference.

On July 28th the

The government is handling the case well away from the spotlight. The

informant gave his handlers proof that their own sensitive documents were circulating in the underground marketplace they'd been striving to destroy.

U.S. Secret Service, which played the dual role of investigator and victim in the drama, said Tuesday it couldn't comment on Jacobsen because the agency doesn't discuss ongoing cases-- a claim that's perhaps undermined by the 19 other Operation Firewall defendants discussed in a Secret Service press release last fall. Jacobsen's prosecutor, assistant U.S. attorney Wesley Hsu, also declined to comment. "I can't talk about it," Hsu said simply. Jacobsen's lawyer didn't return a phone call.

Jan

T-Mobile, which apparently knew of the intrusions by July of last year, has not issued any public warning. Under California's anti-identity theft law "SB1386," the company is obliged to notify any California customers of a security breach in which their personally identifiable information is "reasonably believed to have been" compromised. That notification must be made in "the most expedient time possible and without unreasonable delay," but may be postponed if a law enforcement agency determines that the disclosure would compromise an investigation.

Company spokesman Peter Dobrow said Tuesday that nobody at T-Mobile was available to comment on the matter.

Cat and Mouse Game

According to court records the massive T-Mobile breach first came to the government's attention in March 2004, when a hacker using the online moniker "Ethics" posted a provocative offer on muzzfuzz.com, one of the crime-facilitating online marketplaces being monitored by the Secret Service as part of Operation Firewall.

"[A]m offering reverse lookup of information for a t-mobile cell phone, by phone number at the very least, you get name, ssn, and DOB at the upper end of the information returned, you get web username/password, voicemail password, secret question/answer, sim#, IMEA#, and more," Ethics wrote.

The Secret Service contacted T-Mobile, according to an affidavit filed by cyber crime agent Matthew Ferrante, and by late July the company had confirmed that the offer was genuine: a hacker had indeed breached their customer database,

At the same time, agents received disturbing news from a prized snitch embedded in the identity theft and credit card fraud underground. Unnamed in court documents, the informant was an administrator and moderator on the Shadowcrew site who'd been secretly cooperating with the government since August 2003 in exchange for leniency. By all accounts he was a key government asset in Operation Firewall.

On July 28th the informant gave his handlers proof that their own sensitive documents were circulating in the underground marketplace they'd been striving to destroy. He'd obtained a log of an IRC chat session in which a hacker named "Myth" copy-and-pasted excerpts of an internal Secret Service memorandum report, and a Mutual Legal Assistance Treaty from the Russian Federation. Both documents are described in the Secret Service affidavit as "highly sensitive information pertaining to ongoing USSS criminal cases."

At the agency's urging, the informant made contact with Myth, and learned that the documents represented just a few droplets in a full-blown Secret Service data spill. The hacker knew about Secret Service subpoenas relating to government computer crime investigations, and even knew the agency

was monitoring his own ICQ chat account.

Myth refused to identify the source of his informational largesse, but agreed to arrange an introduction. The next day Myth, the snitch, and a third person using the nickname "Anonyman" met on an IRC channel. Over the following days, the snitch gained the hacker's trust, and the hacker confirmed that he and Ethics were one and the same. Ethics began sharing Secret Service documents and e-mails with the informant, who passed them back to the agency.

Honeypot Proxy

By August 5th the agents already had a good idea what was going on, when Ethics made a fateful mistake. The hacker asked the Secret Service informant for a proxy server -- a host that would pass through Web connections, making them harder to trace. The informant was happy to oblige. The proxy he provided, of course, was a Secret Service machine specially configured for monitoring, and agents watched as the hacker surfed to "My T-Mobile," and entered a username and password belonging to Peter Cavicchia, a Secret Service cyber crime agent in New York.

Cavicchia was the agent who last year spearheaded the investigation of Jason Smathers, a former AOL employee accused of stealing 92 million customer e-mail addresses from the company to sell to a spammer. The agent was also an adopter of mobile technology, and he did a lot of work through his T-Mobile Sidekick -- an all-in-one cellphone, camera, digital organizer and e-mail terminal. The Sidekick uses T-Mobile servers for e-mail and file storage, and the stolen documents had all been lifted from Cavicchia's T-Mobile account, according to the affidavit. (Cavicchia didn't respond to an e-mail query from SecurityFocus Tuesday.)

By that time the Secret Service already had a line on Ethic's true identity. Agents had the hacker's ICQ number, which he'd used to chat with the informant. A Web search on the number turned up a 2001 resume for the then-teenaged Jacobsen, who'd been looking for a job in computer security. The e-mail address was listed as ethics@netzero.net.

The trick with the proxy honeypot provided more proof of the hacker's identity: the server's logs showed that Ethics had connected from an IP address belonging to the Residence Inn Hotel in Buffalo, New York. When the Secret Service checked the Shadowcrew logs through a backdoor set up for their use -- presumably by the informant -- they found that Ethics had logged in from the same address. A phone call to the hotel confirmed that Nicolas Jacobsen was a guest.

Snapshots Compromised

Eight days later, on October 27th, law enforcement agencies dropped the hammer on Operation Firewall, and descended on fraud and computer crime suspects across eight states and six foreign countries, arresting 28 of them. Jacobsen, then living in an apartment in Santa Ana in Southern California, was taken into custody by the Secret Service. He was later released on bail with computer use restrictions.

Jacobsen lost his job at Pfastship Logistics, an Irvine, California company where he worked as a network administrator, and he now lives in Oregon.

The hacker's access to the T-Mobile gave him more than just Secret Service documents. A friend of Jacobsen's says that prior to his arrest, Jacobsen provided him with digital photos that he claimed celebrities had snapped with their cell phone cameras. "He basically just said there was flaw in the way the cell phone servers were set up," says William Genovese, a 27-year-old hacker facing unrelated charges for allegedly selling a copy of Microsoft's leaked source code for $20.00. Genovese provided

SecurityFocus with an address on his website featuring what appears to be grainy candid shots of Demi Moore, Ashton Kutcher, Nicole Richie, and Paris Hilton.

The swiped images are not mentioned in court records, but a source close to the defense confirmed Genovese's account, and says Jacobsen amused himself and others by obtaining the passwords of Sidekick-toting celebrities from the hacked database, then entering their T-Mobile accounts and downloading photos they'd taken with the wireless communicator's built-in camera.

The same source also offers an explanation for the secrecy surrounding the case: the Secret Service, the source says, has offered to put the hacker to work, pleading him out to a single felony, then enlisting him to catch other computer criminals in the same manner in which he himself was caught. The source says that Jacobsen, facing the prospect of prison time, is favorably considering the offer.

<tips@securityfocus.com>

Discussion

Hacker penetrates T-Mobile systems elttyL
Hacker penetrates T-Mobile systems Anonymous
  Hacker penetrates T-Mobile systems FahQ
  Hacker penetrates T-Mobile systems Anonymous
Hacker penetrates T-Mobile systems Anonymous
  Hacker penetrates T-Mobile systems Anonymous
Hacker penetrates T-Mobile systems Kevin Wandtke <kwandtke@hotmail.com>
  Hacker penetrates T-Mobile systems Anonymous
Catch me if you can (again) Pau Garcia i Quiles
Peter Cavicchia should be reprimanded Anonymous
  Peter Cavicchia should be reprimanded Anonymous
    Peter Cavicchia should be reprimanded Anony-mouse
  Peter Cavicchia should be reprimanded Anonymous
  Peter Cavicchia should be reprimanded Anonymous
    Peter Cavicchia should be reprimanded Anonymous
      Peter Cavicchia should be reprimanded David Beaty
        Peter Cavicchia should be reprimanded FrankenPC
  Peter Cavicchia should be reprimanded Anonymous
Hacker penetrates T-Mobile systems Anonymous
  Hacker penetrates T-Mobile systems Anonymous
  Hacker penetrates T-Mobile systems Anonymous
Hacker penetrates T-Mobile systems Anonymous
  Hacker penetrates T-Mobile systems Anonymous
    Hacker penetrates T-Mobile systems Anonymous
Hacker penetrates T-Mobile systems siberian
Hacker penetrates T-Mobile systems TMobile customer
  Hacker penetrates T-Mobile systems Anonymous
    Hacker penetrates T-Mobile systems Anonymous
    Hacker penetrates T-Mobile systems Anony-mouse
Hacker penetrates T-Mobile systems Anonymous
Hacker penetrates T-Mobile systems nr
Hacker penetrates T-Mobile systems Anonymous
Hacker penetrates T-Mobile systems tiger
  Hacker penetrates T-Mobile systems SEbastion
  Hacker penetrates T-Mobile systems Armand

Hacker 'Gets More' From T-Mobile

Associated Press

08:52 AM Jan. 13, 2005 PT

WASHINGTON -- A hacker broke into a wireless carrier's network over at least seven months and read e-mails and personal computer files of hundreds of customers, including the Secret Service agent investigating the intruder, the government said Wednesday.

The hacker obtained an internal Secret Service memorandum and part of a mutual-assistance legal treaty from Russia. The documents contained "highly sensitive information pertaining to ongoing ... criminal cases," according to court records.

The break-in targeted the network for Bellevue, Washington-based T-Mobile USA, which has 16.3 million customers in the United States. It was discovered during a broad Secret Service investigation, "Operation Firewall," which targeted underground hacker organizations known as Shadowcrew, Carderplanet and Darkprofits.

Nicolas Lee Jacobsen, 21, of Santa Ana, California, a computer engineer, has been charged with the break-in in U.S. District Court in Los Angeles. Investigators said they traced the hacker's online activities to a hotel near Buffalo, New York, where Jacobsen was staying.

Jacobsen, who was arrested in October in California, has been released on a $25,000 bond posted by his uncle, who was ordered to keep his own personal computer locked up so Jacobsen couldn't use it.

The hacker was able to view the names and Social Security numbers of 400 customers, all of whom were notified in writing about the break-in, T-Mobile said. It said customer credit card numbers and other financial information never were revealed.

"Safeguarding T-Mobile customer information is a top priority for the company," said a spokesman, Peter Dobrow. He said T-Mobile discovered the break-in late in 2003 and "immediately took steps that prevented any further access to this system."

Court records said the hacker had access to T-Mobile customer information from at least March through October last year.

An online offer in March 2004, traced to Jacobsen, claimed hackers could look up the name, Social Security number, birth date and passwords for voicemails and e-mails for T-Mobile customers, court records said.

The Secret Service said its agent, Peter Cavicchia, should not have been using his personal handheld computer for government work. Cavicchia, a respected investigator who has specialized in tracking hackers, was a T-Mobile customer who coincidentally was investigating the T-Mobile break-in, according to court documents and a Secret Service spokesman, Jonathan Cherry.

Cavicchia, who won the Secret Service's medal of valor for his actions in the Sept. 11, 2001, terror attacks, resigned to work in the private sector. He told The Associated Press he was not asked to leave and said he was cleared during an internal investigation into whether he had improperly revealed sensitive information or violated agency rules.

The case against Jacobsen was first reported by the Web site Security Focus, which is owned by Symantec Corp.

Cherry, the Secret Service spokesman, said the agency's own e-mail servers were not affected by the T-Mobile break-in. "The account was a personal account of a Secret Service agent that was for a time compromised," Cherry said.

Cavicchia's T-Mobile handheld computer contained "very limited investigative material" that was obtained by the hacker, Cherry said, adding that no government investigations were compromised. Cherry said Secret Service policies prohibit agents from keeping work-related files on personal computers.

Cavicchia said Secret Service supervisors frequently e-mailed documents and other files to his wireless computer to review while he was traveling. "The only way for me to review documents while I was on the road was for them to send them to that address, which they knew wasn't an agency address," Cavicchia said.

John Frazzini, a former Secret Service agent, praised Cavicchia, who worked on some of the government's most sensational hacker cases. "His record is one of the most impressive that I have seen in the area of cybercrime investigations," Frazzini said.

Airborne Law Enforcement Association

ALEA Home
Members Only
Upcoming Events
Searchable Databases
Safety First Program
Air Beat Magazine
Police Aviation News
Images
Affiliate Information
Links
Site Search
Contact ALEA
ALEA Membership
ALEA Merchandise

Air Beat Magazine

Journal of the Airborne Law Enforcement Association

Diverse Missions
New York City's
Department of Environmental Protection Police
Aviation Unit
By Lt. Robert Wisker

New York City's water supply system provides approximately 1.3 billion gallons of safe drinking water daily to over eight million residents of New York City, to one million people living north of the City and to millions of commuters and tourists who visit the city every day. In all, the system has 1,972 square miles of watershed, almost 300 miles of aqueduct, 19 reservoirs, three controlled lakes and hundreds of ancillary structures supplying water to nearly half of the state's population. Much of the land owned by New York City is open to the public for fishing, boating, hiking and hunting, and to date, over 77,000 land-use permits have been issued to those who use and enjoy it, most of them responsibly.

The job of protecting this massive infrastructure of dams, reservoirs and aqueducts from criminal and environmental threats, in addition to protecting the employees who work on them and the public who live near and use them, falls on the New York City Department of Environmental Protection (DEP) Police Division. Complicating matters is the enormously different terrain encountered from the urban streets of New York City stretching to the farthest reaches of the watershed 125 miles northwest of the City into the deep forests of the Catskill Mountains.

The 210 members of the DEP Environmental Police perform their jobs on foot patrol, motorcycles, cars,

***Website Updated:* 01/28/2005**

Click here to see what's new!

ALEA's Initial Draft of Recommended Industry Standards

2005 Annual Pre-Conference Professional Courses

ALEA "Safety First" Program Overview

Updated Law Enforcement

4x4, ATV, patrol boats and, for the past five years, by air. For years, the suggestion of adding aviation as an intricate part of patrol work was debated, but inevitably the cost and complexity of running an aviation unit ended the conversation. Alternatives were looked at, such as interagency or intra-municipal agreements for aerial patrol, but these proved ineffective and were cumbersome for agencies that would be expected to make multiple patrols each week in regions not normally patrolled by them, taking time away from their primary area of responsibility. The more the unit looked, the more it became clear that to properly patrol the New York City water system from the air, a dedicated aviation unit as part of the DEP Environmental Police would be needed.

Unfortunately, none of the aviation unit members had extensive flying experience. But they have a strong belief in what could be accomplished. Finally, in 1999, after years of persistence (and a changed administration) someone listened and the Environmental Police began a trial program utilizing a part-time leased helicopter to patrol the aqueducts and remote regions not readily accessible by foot or vehicle. The department had decided that a helicopter was the most practical and versatile airship for our application, so the contract was awarded for a Bell 206-B, which happened to be formally owned by an upstate New York sheriff department. The DEP provided the TFO and the contractor provided a pilot and equipment, which included a Wulfsburg radio, SX5 and FLIR. This was pretty basic equipment for a patrol ship, but enough to give the DEP a chance to prove the benefits of aerial assets.

Once aerial work began, the unit started patrols of remote areas, and was able to do it in a fraction of the time with an immediate increase in incidents detected, demonstrating the effectiveness of aviation as a “force multiplier.” Patrols continued with the helicopter detecting dump sites, trespass offenses, encroachment and wild land fires, and assisting ground crews with searches and enforcement actions.

In September of the first year of operation, Hurricane Floyd gave a glancing blow to the New York metropolitan region. The aircrew over the course of the following two days videotaped each of the affected areas, finding washouts and numerous fields of floating debris ranging from tires and trees to barrels and cows.

The FLIR was extensively used to scan for hydrocarbons (gas and oil) that were spilled as a result of flood waters carrying away the fuel oil and gasoline tanks found on many upstate New York farms. The aircrew was also credited with expediting the ground crews’ work in locating and removing the debris in the effected areas. These first initial aerial

flights, although performed only two or three times a week, began to show just what could be accomplished, and how in some cases, having aviation assets can actually be cost effective.

DEP began learning valuable lessons and sought advice from other aviation units like the New York City Police Aviation Unit and the New York State Police Aviation Unit for safe operational practices. At this point, the unit was still a part-time operation with few scheduled patrols each week and no advantage of immediate response time to incidents. But that was about to change.

September 11 was a day that forever changed the way many of us do things. For the DEP Aviation Unit, it was the day we became a full-time aviation unit, call sign “Air-6.” That day and the days that followed found ours and other aviation units not knowing what was going to happen next. Aircrews from throughout the region were doing double duty, spending long hours to do whatever was needed. Air-6 was given its assignment to protect the water system coming into New York City. The departmental manpower situation, like all other departments, did not change however. Officers were assigned to extended tours of duty at strategic posts and resources were stretched.

The Aviation Unit took over the patrolling of remote and vital locations and was extensively used as an aerial platform, allowing for better manpower resource management by responding to incidents and advising our control center of the situations, thus allowing the dispatch of only those units needed.

Scheduled maintenance on the aircraft was performed during the evening hours or when weather was predicted to keep the aircraft down. The unit was fortunate in that very little unscheduled maintenance was necessary because the aircraft was well maintained to begin with.

In April 2004, DEP replaced the 206-B with a full time lease of a 206-L-1 from the same company, Heliworks of Pensacola, Florida. Heliworks had done a great job and won the competitive bid of the second contract. Again, this contract included pilots, but now they were to be CFIs working with DEP to help formulate and train for an in-house aviation unit. Because of the new contract, pilots will not be cut loose as mission rated until achieving a minimum hourly standard and passing a check ride.

Chief Pilot Geb Wolf, who is retired from the New York State Police, initially began pilot training for the unit. Wolf is a very accomplished pilot and he established an on-the-job training program for pilots and crew members, giving guidance on safe operational practices. The unit also has CFI Andy Perry, who comes from the civilian side and helps carry out the

training and safety programs.

The full-time leased Long Ranger, which was totally refurbished and modified by Stephen Simpson and his crew at Heliworks, including installation of a C-30 engine, was delivered with wire strike protection, pop-out floats, SX-5, Garmin 430, Technasonic TFM-550 radio and an Avalex AMS-7000 digital mapping system with AVR-8000 recording system integrated with a FLIR 2000. This modified L-1 gives us plenty of lift, pulling only 80 percent torque with equipment, two passengers, crew and a full load of fuel on liftoff. Maximum performance takeoffs in tighter areas are no problem.

A few of the installed components were chosen specifically for their low weight and high performance level. In particular, crewmembers were very impressed with the Technasonic TFM-550 FM Transceiver. This lightweight three-band radio weighs in at seven pounds installed and gives the operator 200 individual channels on each of the Lo, VHF and UHF bands. Complete with group scan capabilities, program-on-the-fly, selectable 1-10 watt power output, priority channeling, individual band volume control and cross band repeater capability between VHF and UHF, this radio is a high quality signal unit that is easy to operate and affordable.

Next, the unit chose the Avalex AMS-7000 Digital Mapping System with AVR-8000 recorder and Avalex 8.4 inch flat screen. This system provides street mapping, topographical mapping, VFR and IFR aeronautical maps and nautical charts. Optional map features include aerial photos and custom user maps. DEP has found the system to be just about pinpoint accurate in all mapping and tracking modes and, with a rate of five scans per second, provides almost instantaneous aircraft positioning.

The flat screen gives high quality images both on mapping and FLIR screens with excellent viewing on sunny days, but you still may want to install a custom screen shade, which helps immensely. The aircraft also has an optional Avalex mounting arm that folds the screen out of the way when not in use, whenever that might be. The 8.4-inch screen is easier for viewing. Operated by touch screen or keyboard in a Windows setup, this system is easy to operate.

The unit chose a KNEE-KEY kneeboard/keyboard system, which reduces cockpit clutter as opposed to a tray mounted or external keyboard. Capable of split-screen viewing for both mapping and FLIR viewing, the system writes to a mission data recorder or DVD+R disc that can be viewed on the Avalex screen or removed for play on a DVD player. Another useful feature is the built-in HSI, which displays on the Avalex screen and can take traffic data input. The Avalex Digital Mapping System is one of the most

useful tools the unit has acquired.

Commanded by Lieutenant Robert Wisker and his Executive Officer, Sergeant John Sweeney, DEP is located at Stewart International Airport, which is at about the center of the unit's patrol area. Rifton Aviation, the unit's FBO, has a full modern hangar with 24-hour line service, an office and many accommodations.

The unit currently averages around 850 hours a year flight time, which may not seem like much to some units, but for DEP, with a full-time lease aircraft, that adds up in operational costs. The unit has demonstrated to those in the city's government that purchasing and operating our own aircraft is clearly more cost efficient. In fact, the unit is currently in the process of completing bid specifications for the purchase of a new single engine helicopter that will finally be their very own. The bid specs are currently going through the internal process, and hopefully, will be out by early to mid-2005.

Author's Note: I don't know of any aviation unit that just started up and had all their experience and expertise delivered to them in a box.The DEP has a few notables we would like to thank for helping begin operations. ALEA's officers, members and their vast collection of information: it gave our aviation unit ideas and practical teachings, particularly through Air Beat articles. We also thank Deputy Inspector Gallucci and Lieutenant Randy Berry of NYPD Aviation at Floyd Bennet Field and Major Ken Rogers of the New York State Police Aviation Unit who have been a great help to us, all of whom offered us technical advice from their highly experienced staff and fielded any questions we have asked; these great units are tops in our book. We have come a long way in the past five years and have learned quite a bit. We've worked hard and have made some errors, but learned from them and continue to try to improve, always with safety as the first item on our checklist.

P.O. Box 3683 Tulsa, OK 74101-3683
Ph (918) 599-0705
Fax (918) 583-2353
Webmaster