UFO UpDates Mailing List

The Story Of The UFO Superhackers

From: Stig Agermose@online.pol.dk (Stig Agermose)
Date: Tue, 7 Apr 1998 04:06:25 +0100
Fwd Date: Tue, 07 Apr 1998 01:51:31 -0400
Subject: The Story Of The UFO Superhackers

Thanks to the Sunday Times.

Stig

****

The schoolboy spy

Sunday Times - London

Sun, Mar 29 1998

The Americans called him their No 1 enemy, but he was only 16. Jonathan Ungoed-Thomas reveals one of the strangest stories of the cyber-age.

On the evening of April 15, 1994, six American special agents sat in a concrete basement at a secret air force base patiently waiting for an attack. Their unseen and unknown enemy had for weeks been rampaging across the Pentagon network of computers, cracking security codes and downloading secret files.

Defence officials feared the infiltrator was a foreign agent. They were monitoring his move ments in a desperate effort to trace him to his lair.

He had first been spotted by a systems manager at the Rome Laboratory at the Griffiss air base in New York state, the premier command and control research facility in the United States. He had breached the security system and was using assumed computer identities from the air base to attack other sites, including Nasa, Wright-Patterson air force base - which monitors UFO sightings - and Hanscom air force base in Massachusetts. He was also planting "sniffer files" to pick up every password used in the system.

This was a new type of warfare, a "cyber attack" at the heart of the most powerful military machine on earth. But the American military had been preparing for "cyber war" and it had a new breed of agent ready to fight back against the infiltrator. Computer specialists from the Air Force Office of Special Investigations (AFOSI) and the Air Force Information Warfare Centre in San Antonio, Texas, were dispatched to Rome Laboratory to catch the attacker.

By the end of the second week of their attempt to outwit him, their windowless basement room was a mess of food wrappers, sleeping bags and empty Coca-Cola cans. Sitting among the debris, the American cyber agents saw a silent alarm throb on one of the many terminals packed

into the 30ft by 30ft room. Datastream Cowboy, as he called himself, was online again.

They carefully tracked him on a computer screen as he used the access code of a high-ranking Pentagon employee to sign on. This gave him the power to delete files, copy secret information and even crash the system. As he sifted through battlefield simulation data, artificial intelligence files and reports on Gulf war weaponry, the agents worked frantically at their terminals, trying yet again to establish who he was and where he had come from. It was futile. Datastream Cowboy always bounced around the world before launching an attack and it was impossible even to establish in which country he was sitting.

Suddenly he left the Pentagon system. The agents rapidly checked the computer address of his new target and were chilled by the result: he was trying to get access to a nuclear facility somewhere in Korea.

The shocked agents saw a terrible crisis coming. The United States was embroiled in tense negotiations with North Korea about its suspected nuclear weapons programme. The Clinton administration was publicly split between a faction that wanted to punish the Stalinist regime in Pyongyang for attempting to develop a nuclear bomb and State Department diplomats who insisted on a gentler approach.

If the paranoid North Koreans detected a computer attack on their nuclear facility from an American air base - because Datastream Cowboy had assumed an American military identity by routeing his assault through the Griffiss computer - they would be bound to believe that the hawks had won and this was an act of war. Senior defence officials were hurriedly briefed as the agents attempted to establish the exact location in Korea of the computer that Datastream Cowboy was trying to crack.

After several tense hours, they had their answer. His target was in South Korea, not North. The security alert was over, but the damage meted out by Datastream Cowboy was not. In the space of a few weeks he had caused more harm than the KGB, in the view of the American military, and was the "No 1 threat to US security".

What made Datastream Cowboy so dangerous, in the view of the Americans, was that he was not alone; he was working with a more sophisticated hacker who used the "handle" of Kuji. The agents repeatedly watched Datastream Cowboy unsuccessfully attack a military site and retreat for an e-mail briefing from Kuji. He would then return and successfully hack into the site.

Both Datastream Cowboy and Kuji were untraceable. They were weaving a path through computer systems in South Africa, Mexico and Europe before launching their attacks. Over 26 days, Datastream Cowboy and Kuji broke into the Rome Laboratory more than 150 times. Kuji was also monitored attempting an assault on the computers at Nato headquarters near Brussels.

It was only three years after the final collapse of Soviet communism, but there was already a strong fear within the American government that the United States had become vulnerable to a new military threat: electronic and computer warfare.

Both America's superpower military arsenal and its huge civilian economy had become reliant on microchips and in the words of Jamie Gorelick, a deputy attorney-general: "Some day we will wake up to find that the electronic equivalent of Pearl Harbor has crippled our computer networks and caused more chaos than a well placed nuclear strike. We do not want to wait for that wake-up call."

What made the American military so vulnerable was that the Internet - the computer communications system that had been developed by Pentagon scientists as a tool for survival after nuclear war - was opening up in 1994 to anyone in the world who had access to a cheap and powerful personal computer.

The Internet automatically brought hackers to the very gates of the Pentagon's most secret files - and it could not be policed, as it had been deliberately set up without controls to ensure ease of access for nuclear survivors.

According to official American figures, the Pentagon's military computers are now suffering cyber attacks at the rate of 250,000 a year and it is retaliating with a $3.6 billion programme of computer protection to key systems.

THE attacks by Datastream Cowboy and Kuji were the opening shots in this barrage, and the Pentagon generals insisted that they had to be found and put out of action. It would have been relatively simple to shut them out of the Pentagon network, but they would survive to attack again - and their identities and the information they had already stolen would have remained unknown. The American cyber agents were ordered to continue chasing them through the electronic maze.

But how? They used a process called "fingering" in which they tried to detect every computer that Datastream Cowboy had used as stepping stones before attacking them. A computer on the Internet gives its own address in the first few bytes of any communication and the agents tried to trace Datastream Cowboy's path backwards. The process can often be hit and miss because of the vast amount of traffic on the Internet and the hacker's path was simply too long and circuitous to follow to its end. The agents almost gave up hope. Then old-fashioned police work was brought to bear. In the cyber age, where do hackers hang out? On the Internet, of course. They "chat" with each other through their screens.

The agents had informants who cruised the Internet and one of these made the breakthrough. He found that Datastream Cowboy hung out at Cyberspace, an Internet "service provider" based in Seattle. Moreover, he was a particularly chatty individual who was eager to engage other hackers in e-mail conversation. Naive, too. Before long, the informant had established that Datastream Cowboy lived in the United Kingdom. He even gave out his home telephone number.

Jubilant, a senior AFOSI agent contacted the computer crime unit in Scotland Yard for assistance. Datastream Cowboy's number was traced to a house in a cul-de-sac in Colindale, part of the anonymous north London suburbs. In cold war days it would have been a classic address for a spy's hideaway.

Telephone line checks revealed that the hacker was first dialling into Bogota, the Colombian capital, and then using a free phone line from there to hack his way into the sensitive military sites.

American agents flew to London and staked out the address with British police officers. Detectives were cautious, however, about making an immediate arrest because they wanted Datastream Cowboy to be online when they entered the house, so that he would be caught in the act.

At 8pm on May 12, 1994, four unmarked cars were parked outside the Colindale house. Inside one of them, a detective's mobile phone rang. An agent from the Rome Laboratory was on the other end: Datastream Cowboy was online. Officers made a second call to British Telecom in Milton Keynes and established that a free phone call was being made to South America.

Posing as a courier, one of the officers knocked on the door. As it was opened by a middle-aged man, eight policemen silently appeared and swept into the house. The officers quietly searched the downstairs and first floor. Then, creeping up the stairs to a loft- room, they saw a teenager hunched in his chair tapping frantically away on the keyboard of his Pounds 700 PC World computer. They had found Datastream Cowboy.

One of the detectives walked up silently behind the young suspect and gently removed his hands from the computer.

For 16-year-old Richard Pryce, a music student, it was the shock of his life. He looked at the policemen as they prepared to arrest him and collapsed on the floor in tears.

"They thought they were going to find a super-criminal and they just found me, a teenager playing around on his computer," says Pryce now. "My mother had noticed people sitting outside our house for a few days beforehand, but I didn't think much of it. I never thought I would get caught and it was very disturbing when I did.

"It had just been a game or a challenge from which I had got a real buzz. It was unbelievable because the computers were so easy to hack, like painting by numbers."

Pryce, who was then a pupil at The Purcell School in Harrow, Middlesex, was arrested at his home but released on police bail the same evening. Five stolen files, including a battle simulation program, were discovered on the hard disk of his computer. Another stolen file, which dealt with artificial intelligence and the American Air Order of Battle, was too large to fit on to his desktop computer. So he had placed it in his own storage space at an Internet service provider that

he used in New York, accessing it with a personal password.

During the subsequent police interviews, one pressing question remained unanswered: who was Kuji? Pryce claimed he had only talked with his hacking mentor on the Internet and did not know where he lived. American investigators regarded Kuji as a far more sophisticated hacker than Datastream. He would only stay on a telephone for a short time, not long enough to be traced successfully. "Kuji assisted and mentored Datastream and in return received from Datastream stolen information...Nobody knows what Kuji did with this information or why it was being collected," agents reported.

Mark Morris, who was then a detective sergeant with Scotland Yard's computer crime unit, was one of the investigating officers on the case. "It was awesome that Pryce, who was just one teenager with a computer, could cause so much havoc, but the greater worry in the US was about Kuji," says Morris. "The fear was that he could be a spy working for a hostile foreign power. The job was then to find him."

Pryce did give detectives one telephone number, but it was a red herring: a school library in Surrey. During the next two years of compiling evidence in Britain and America in the case against Pryce, British detectives and American agents failed to turn up any evidence that might lead to Kuji.

Their break finally came in June 1996 when the computer crime unit decided to sift once again through the mass of information on the hard disk of Pryce's computer.

Morris took on the job. "I was at home with my laptop and went through every bit of that hard disk, which was a huge task." It took him three weeks. If all the files had been printed out they would have filled 40 filing cabinets.

At last he found what he wanted. "At the bottom of a file in the DOS directory I saw the name Kuji. Next to the name was a telephone number. Pryce might not have even known it was on his system because he downloaded so much information."

For American agents hoping to catch a superspy, Kuji's telephone number was a grave disappointment. He was based in Cardiff. A team of officers drove up to his address, a terraced house, and finally discovered Kuji's identity. He was 21-year-old Mathew Bevan, a soft- spoken computer worker with a fascination for science fiction. His bedroom wall was covered with posters from The X Files and one of his consuming interests was the Roswell incident, the alleged crash of a UFO near Roswell, New Mexico, in July 1947. He was arrested on June 21, 1996, at the offices of Admiral Insurance where he worked.

"I would never have been caught if it wasn't for Pryce and even then they took two years to find me," Bevan says now. "And the only reason Pryce got caught was that he gave his number to a secret service informant."

Bevan, the son of a police officer, said he had not even been alarmed when Datastream Cowboy disappeared from the Internet. "Everyone was joking with me on the e-mail that he must have been arrested, but I didn't believe it. It wasn't until a year later that a friend phoned me and said: 'Have you seen the papers? They think you're a spy'."

However, Bevan became confident that he had escaped detection and was stunned when he was arrested. "I was told to go and check the managing director's computer. I went in and there were seven or eight of them in suits and I was arrested." He was charged the next day with two counts of conspiracy under the Criminal Law Act 1997. He was later charged with three offences under the Computer Misuse Act 1990.

Pryce had been charged in June 1995, about 13 months after his arrest, with 12 offences under Section 1 of the Computer Misuse Act 1990. He was also charged with conspiracy three days before Bevan's arrest.

At the culmination of one of the biggest ever international computer crime investigations and after a massive security scare in the United States, law enforcers were left with a meagre and faintly embarrassing prize: two young hackers who in their spare time, from the comfort of their bedrooms, had penetrated what should have been the most secure defence network in the world. To rub salt into the wounds, their credentials were hardly impressive. Pryce had scraped a D grade in computer studies at A-level and Bevan had dropped out of an HND course in computer science.

Pryce's father, Nick, who restores musical instruments, said: "They said Richard was a No 1 security threat and I think that was just rubbish. They had overreacted and when they found out it was just a teenager, they still wanted to try to make an example of him. I never knew what he was doing at the time; I just thought he was in his bedroom playing on his computer. When I found out, I never thought he had done anything particularly wrong and neither did our friends. He just showed how bad security was on those computers."

But how did two rather ordinary young men manage to penetrate the Pentagon computer system and spark such a massive security alert? Both were bright and articulate, but there was nothing in their backgrounds to suggest a computer wizardry that would outwit the American military. Their success was based on a mixture of persistence and good luck, which was abetted by crude security mistakes in the Pentagon computer system.

Pryce had had a musical upbringing with his two sisters, Sally and Katie, and had a passion for playing the double bass. He was bought his computer when he was 15 to help him in his studies. He would spend his spare time linked up to a bulletin board on the Internet, where computer users traded information and chatted. It was here tha he got his first introduction to hacking.

"I used to get software off the bulletin boards and from one of them I got a 'bluebox', which could recreate the various frequencies to get free phonecalls," he said. "I would phone South America and this software would make noises which would make the operator think I had hung up. I could then make calls anywhere in the world for free."

Now 20 and in his third year at the Royal College of Music in London, Pryce said: "I would get on to the Internet and there would be hackers' forums where I learnt the techniques and picked up the software I needed. You also get text files explaining what you can do to different types of computer.

"It was just a game, a challenge. I was amazed at how good I got at it. It escalated very quickly from being able to hack a low- profile computer like a university to being able to hack a military system. The name Datastream Cowboy just came to me in a flash of inspiration."

The attack on Rome Laboratory, his greatest success, relied on a ferret called Carmen. Pryce easily gained low-level security access to the Rome computer using a default guest password. Once inside the system, he retrieved the password file and downloaded it on to his computer. He then set up a program to bombard the password file with 50,000 words a second. "I just left the computer running overnight until it cracked it," he explained.

If all the air force officers with access to the computer had followed orders and used passwords with a mixture of numerals and letters, his attack would have been foiled; but luck was on his side.

Morris, who has since left Scotland Yard's computer crime unit and now works in London for Computer Forensic Investigations, a private company, revealed: "He managed to crack the file because a lieutenant in the USAF had used the password Carmen. It was the name of his pet ferret. Once Pryce had got that, he was free to roam the system. There was information there that was deemed classified and highly confidential and he was able to see it."

Once he was in the system, Pryce kept getting access to higher levels in his aim to become a "root user", which gives the hacker total control of the computer with the power to shut out other users and command the entire system.

"I was interested in Rome Labs because I knew they developed stuff for the military. I just wanted to find out what they were doing. I read that UFO material was being kept at Wright Patterson base and I thought it would also be a laugh to get in there. I also hacked into a Nasa site," he said.

"Rome Labs was my main project. I got the programming code for an artificial intelligence project. I downloaded files so I could view them at leisure at home.

"I know there was a big fuss when I tried to hack into a computer in Korea, but there was nothing sinister about it. I just fancied having a go at a different sort of computer and I happened to be on the Rome Laboratory computer. I just tapped in the address for the Korean research computer, but I didn't hack into it. It never went further

than that." During an intensive three months of hacking, Pryce sent e-mails at least twice a week to the fellow hacker he knew as Kuji, without knowing his real name was Mathew Bevan.

Bevan, who is now 23, was more of a loner than Pryce and would spend up to 30 hours without a break on his computer. He claims the fraternity of hackers gave him the friendship that he had failed to find during his childhood. "I was bullied at school and I found my little community and interaction through my computer," he said. "The hackers would all egg each other on. There wasn't anything malicious about it. If there was, I could have downed as many computer systems as I wanted. I was just really looking for anything about UFOs. It was like war games; I just couldn't believe what we could get into. I wasn't tutoring Pryce, but the Americans made out I was because they thought I was some kind of east European masterspy."

Pryce agrees: "We embarrassed them by showing how lax their security was and that's why they made out we had been a huge security threat. I'm now amazed by what I did, but I wasn't surprised at the time. It was just my hobby. Some people watched television for six hours a day, I hacked computers."

The first time Pryce and Bevan met in person was in July 1996 when they appeared at Bow Street magistrates court jointly charged with conspiracy and offences under the Computer Misuse Act. "He was at the back of the court when I went in and his mother said: 'You'd better say hello', which he did. We didn't even have a chat," said Bevan.

Conspiracy charges against both Pryce and Bevan were later dropped, but in March last year Pryce was fined Pounds 1,200 after admitting 12 offences under the Computer Misuse Act. His lawyers said in mitigation that there had been some exaggeration when the Senate armed services committee had been told in 1996 that the Datastream Cowboy had caused more harm than the KGB and was the "No 1 threat to US security". The remaining charges against Bevan were dropped in November after the Crown Prosecution Service decided it was not in the public interest to pursue the case.

Nevertheless, the case of Datastream Cowboy and Kuji remains one of the most notorious in American cyber history. The two young men are living this down in different ways. Pryce's computer was confiscated, to his initial dismay. "After I had my computer taken away it was quite difficult because I had been doing it every night for a year," he said. "If they hadn't caught me, I would have carried on." Now he thinks hacking was a waste of time and insists he will never do it again. He does not even own a computer any more.

Bevan, however, has put his notoriety to good use: he is now employed testing the computer security of private companies.

Targeting the pentagon

United States defence computers have for years been one of the most coveted targets for hacking addicts inspired by the film War Games, which showed a boy cracking an American defence network and nearly starting the third world war.

One of the pioneers of this craze was Kevin Mitnick, who repeatedly hacked into Pentagon computers in the mid-1980s. He was jailed in 1989 but continued his exploits on his release and was arrested again after a two-year hunt by the FBI. The number of cyber attacks on the Pentagon is estimated by Washington officials as 250,000 annually, but the incidents the public hears about are only the few where hackers get caught. In 1996 six Danes who hacked into Pentagon computers were given sentences of up to three months. The same year, special agents tracked down three teenage hackers in Croatia who had also succeeded in penetrating Pentagon computers.

They were never identified or charged, however, as there is no law against computer hacking in Croatia. Last month there was a spectacular example of the hackers' work when American defence officials revealed that the Pentagon computer network had been subjected to a relentless two-month attack. CIA agents were reportedly anxious that the hackers might be the agents of Saddam Hussein.

FBI agents blamed a secret convention of hackers believed to be held in New York. A few days ago, the real culprit gave himself up. Ehud Tenenbaum, an Israeli teenager who dubbed himself The Analyser, had

worked with two young hackers in California. Under house arrest in Tel Aviv, he said the attacks were not malicious. He had concentrated on American government sites because he hated organisations. "Chaos, I think it is a nice idea," he said.

[Next Message | Previous Message | This Day's Messages]
[This Month's Index | UFO UpDates Main Index | MUFON Ontario]

UFO UpDates - Toronto - updates@globalserve.net
Operated by Errol Bruce-Knapp - ++ 416-696-0304

A Hand-Operated E-Mail Subscription Service for the Study of UFO Related Phenomena.
To subscribe please send your first and last name to updates@globalserve.net
Message submissions should be sent to the same address.

[UFO Topics | People | Ufomind What's New | Ufomind Top Level]

To find this message again in the future...
Link it to the appropriate Ufologist or UFO Topic page.