Uncovering the mystery of Shadowhawk.

Print

Title Annotation: *hacker who committed computer crimes*
Author: *Cook, William J.*
Date: *May 1, 1990*
Words: *4688*
Publication: *Security Management*
ISSN: *0145-9406*

ON JANUARY 23, 1989, JUDGE PAUL PLUNKETT OF THE US DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS FOUND AN 18YEAR-OLD COMPUTER HACKER GUILTY OF COMMITTING FIVE ACTS OF juvenile delinquency, as charged in a federal information under 18 USC 5032, for violations of the Computer Fraud and Abuse Act of 1986, 18 USC 1030(a)(6) and 1030(a)(4). The hacker was acquitted on one count of destroying computer data under 18 USC 1030(a)(5).

On February 14, 1989, the hacker was sentenced to nine months in prison, to be followed by two and a half years' probation, and was ordered to pay restitution totaling $ 1 0,000. On February 28, 1989, he started serving his prison term in a prison in South Dakota. If the hacker had been 18 when he committed these crimes, he would have faced a possible 13-year prison sentence and fines totaling $800,000.

Facts developed during a one-week trial established that between July and September 1987, the hacker, under the code name Shadowhawk, used a modem on his home computer to gain unauthorized remote access to AT&T computers in Illinois, New Jersey, North Carolina, and Georgia and stole copies of copyrighted AT&T source code worth over $1,120,000.

The lifeblood of AT&T'S effort to maintain its competitive position in the international telecommunications industry is its R&D community, known generally as Bell Labs. Bell Labs is made up of 27 different R&D laboratories in nine states and employs 28,000 people.

Bell Labs' budget of nearly $3 billion per year reflects AT&T'S commitment to basic and applied research in artificial intelligence; computer hardware and software development; data acquisition through telemetry; energy extraction, conversion, and combustion; information systems planning, design, and development; manufacturing systems-, material process control; microelectronics; military systems; photonics; robotics; surface technology; switching and transmission systems and component engineering; and systems testing and evaluation.

The scientists and engineers at Bell Labs benefit from significant input from other lab members at the various Bell Lab sites in developing their research. To meet this need, electronic mail and files on projects are exchanged daily on AT&T'S extensive internal computer network. Major hubs in this national computer communication network are referred to as "gateway" computers.

AT&T is protective about its R&D efforts. Its guidelines for safeguarding proprietary information are clear and state in part:

It is the policy of AT&T to protect proprietary information assets and to share them with others only when it is in the interest of AT&T to do so and where such disclosure is not otherwise legally prohibited.

Proprietary information of AT&T is only made available to authorized employees of AT&T on a need-to-know basis and in compliance with applicable laws and regulations.

AT&T and Bell Labs are popular hacker targets because of the highly sophisticated computer software engineering at their locations. In 1986 and 1987, vulnerabilities in the security of AT&T'S Unix-based computer network were discovered by computer hackers and published on computer bulletin boards, known as hacker bulletin boards or pirate bulletin boards. As a result, in early 1987, AT&T was hit with an unusually high number of successful remote access computer break-ins from the hacker community.

Prompt action by AT&T corporate security and California state authorities in the spring of 1987 closed down a group of southern California youths responsible for a large percentage of the attacks. By June 1987 the principal remaining hacker attacking AT&T computers was identified as "Shadowhawk."

Periodic monitoring of pirate bulletin boards in Texas and Chicago by Hank Kluepfel and others with AT&T corporate security first led to the discovery of the Shadowhawk attacks against Bell Labs in mid-1987.

On May 10, 1987, a hacker identified as Shadowhawk placed detailed information on how to attack AT&T Unix computers successfully on a computer bulletin board service (BBS) known as Phreak Klass-2600, in Lubbock, TX. In his message, he bragged he was a pretty experienced" hacker against the UNIX system and told his readers about a trapdoor password (.SH) he had installed on the AT&T network to gain system administrator privileges on UNIX computers (count one).2

On May 11, 1987, Shadowhawk placed an additional message on the Texas bulletin board that bragged he had obtained AT&T Unix source code and a list of UNIX computers on the AT&T network. He then asked other bulletin board readers to join him in installing Trojan horses and abusing the AT&T network.

On June 8, 1987, Shadowhawk published the entry codes to 27 computers owned and operated by AT&T, Massachusetts Computer Corp., and Rockwell International's computer division on the RIPCO BBS in Chicago (count two).

On June 28, 1987, Shadowhawk published the names, telephone numbers, log-in accounts, and passwords to seven additional AT&T computers on the RIPCO BBS in Chicago. In his messages, Shadowhawk described how to attack AT&T computers by impersonating other AT&T computers and explained how AT&T files could be transferred between computers and off the AT&T network (count three).

As a result of the series of attacks on AT&T computers at Bell Labs in Naperville, IL, in early 1987, many of the systems administrators there began to monitor traffic closely on their computers. On July 8, 1987, this vigilance paid off when a systems administrator observed and copied an unusual telephone number that was calling for files from his computer "C1."

The administrator kicked the intruder off his computer and reported the captured number to AT&T Corporate Information Security, where Kluepfel and his assistant Jerry Dalton quickly made the correlation between the intruder's telephone number and the BBS messages of Shadowhawk. Dalton traced the intruder's telephone number to a residence on the north side of Chicago and requested Illinois Bell to install a dial number recorder (DNR), which is also known as a pen register, on the telephone line to protect AT&T, Illinois Bell, and their subscribers.' Ten days later, on July 18, 1987, the first of a series of remote access break-ins to AT&T computers originating from the residence was recorded on the DNR.

ON JULY 18, 1987, A NATO MAINtenance and Supply Agency computer owned by the US Missile Command and located at an AT&T managed facility in Burlington, NC, was broken into by remote access, and copies of UNIX computer source codes worth $18,000 were copied and stolen. Shadowhawk gained unauthorized remote access to the NATO computer directly from his home computer by using a log-in account and password that identified him as a UUCP administrative user. (UUCP is the AT&T program that permits the transfer of files from one computer to another.)

Once on the NATO computer, Shadowhawk manipulated the system to obtain systems manager privileges, known as root or super user. As super user he then changed the systems (transfer) file and told the NATO computer to recognize the modem located at this home telephone number as a valid account to receive transfer files. He then told the NATO computer to create a large archive file and fill it with AT&T proprietary source code programs4 and transfer the archive file to his computer in Chicago. When the transfer was completed, he eliminated his tracks from the NATO computer and left the system.

Through this access, Shadowhawk obtained AT&T'S EMACS Full Screen Editor software program valued at $10,000, AT&T'S ESH command interpreter software program valued at $3,000, and AT&T'S basic computer language interpreter for UNIX valued at $5,000.

The documentary evidence supporting this scenario came principally from the DNR installed on Shadowhawk's phone, which showed that his computer was connected directly to the NATO computer at the time of the theft. Log records on the NATO computer showed that no authorized user was on the computer at the time of the theft. When the search warrant was executed in September 1987, the agents found the contents of this transfer file on Shadowhawk's computer.

On July 23, 1987, Shadowhawk also stole a copy of AT&T'S state-of-the-art Artificial Intelligence C5 Expert Systems software program from a highly secured computer in the R&D section of Bell Labs in New Jersey. This software was worth $1 million.

In this attack, Shadowhawk first gained unauthorized remote access by masquerading his computer as a Bell Labs Illinois gateway computer when he logged on to an unrestricted dial-up modem attached to a Bell Labs Illinois computer, C2. He then used this compromised Bell Labs Illinois computer to enter the Bell Labs computer network and contact the Bell Labs New Jersey artificial intelligence Al) computer, containing the C5 Artificial Intelligence software.

Shadowhawk then manipulated the systems files on the Al computer to become super user and directed the New Jersey Al computer to copy and transfer the Al program to the C2 computer at Bell Labs Illinois. Once the first step of the file transfer was completed, Shadowhawk told the Bell Labs Illinois computer C2 to download the software program to his home computer, which was still masquerading as the Bell Lab Illinois gateway computer. He finally erased his file tracks from C2 and left the network.

This scenario was documented by the July 23, 1987, DNR records that showed a call was made from Shadowhawk's computer to the AT&T computer in Naperville, C2, at the same time the file containing the C5 program was downloaded from the Al computer at Bell Labs New Jersey through the C2 computer at Bell Labs Illinois. An exact copy of the C5 Artificial Intelligence Source Code was subsequently found on his computer during the execution of a federal search warrant at his home on September 4, 1987.

A review of his computer during the search also disclosed that the dial-up password to his computer was gateway. During conversations with the agents, Shadowhawk admitted that he had sometimes masqueraded as the gateway computer when he was on the AT&T network.

The Al program theft from a Bell Labs computer in New Jersey through a Bell Labs computer in Illinois brought Bell Labs Security Specialist John Hickey and Bell Labs Consultant Doug Price onto the investigation team. Their immediate investigation disclosed an unrestricted dial-up modem in one part of the laboratory that had been discovered by the intruder and was being used as his entrance to the network.

FOR A FEDERAL OFFENSE TO OCCUR under 18 USC 1030, a computer intrusion must involve a "federal interest computer." The clearest example of this is an attack on a US government-owned computer. However, the federal interest computer involved in each of the Shadowhawk charges involved the defendant's use of several computers, at least one of which was out of state. This miniature, interstate computer network is awkwardly defined as a federal interest computer.

Several of Shadowhawk's significant attacks on the Bell Labs computer network were never charged because the use of his computer in Chicago to obtain files from Bell Labs' campus in Naperville, IL, did not cross state lines.

Therefore, no federal interest computer was involved as required by federal law.

Noninterstate (nonfederal interest) intrusions by Shadowhawk included his July 27, 1987, theft of 40 to 50 Unix source code files, including one file worth $5,000; his July 31 theft of 327 highly sophisticated computer-aided, computer-design programs known as COSMOS; and his August 3 theft of the source code for the AT&T 5ESS switching system valued between $28,000 and $40,000. During each of these intrusions Shadowhawk disguised his computer as a gateway computer on the AT&T internal network.

The July 27 theft mentioned earlier was of particular interest because it involved the temporary storage of a file stolen from Bell Labs computer C3 on a separate computer, C2, in a different building at Bell Labs. The evidence reflected that on July 25 Shadowhawk called C3 at Bell Labs Naperville for 10 hours and transmitted a large file of Unix source code to C2. Two days later Shadowhawk reentered the Bell Labs network and transmiitted the file from C2 to his home computer, which was masquerading as the AT&T gateway computer at Bell Labs.

Shadowhawk was interested in more than Unix source codes. On August 25, 1987, he gained remote unauthorized access to Bell Labs Illinois C7 computer for seven continuous hours to obtain the latest updates on UNIX system vulnerabilities. These files were found at Shadowhawk's house at the time of the search.

BETWEEN AUGUST 28 AND SEPTEMBER 2, 1987, Shadowhawk successfully attacked an AT&T computer at Robbins Air Force Base (AFB) in Georgia. The Robbins computer was diagnosing the operation of the base's AUTOVON and PUBLIX telephone switching systems and contained a highly sophisticated AT&T proprietary source code.

Shadowhawk gained remote access to the Robbins AFB computer through an open password on the line printer (LP) account. He examined the computer files and then created a large archive file, which he filled with AT&T proprietary source code software, plus the AT&T diagnostic research on the Robbins AFB system. He then changed his identity from LP to C7 (a development computer at Indian Hills), gained super user status on the Robbins AFB computer, and transferred the large file from Robbins AFB to his home computer. He retained the AT&T source code program but destroyed 10 hours of AT&T diagnostic files reflecting the operation of the Robbins AFB communication system.

The DNR on Shadowhawk's home computer documented his connection to the Robbins AFB computer during this time. Moreover, some of the contents of the large file from Robbins AFB were found on his home computer at the time of the search. Shadowhawk later admitted to the agents that he was trying to get on the defense data network, but he said he didn't think he was on an Air Force base computer.

The 10 hours of destroyed diagnostic data on the operation of the AFB communication system mentioned earlier created a special problem. If the lost files reflected no weaknesses or shortcomings in the ALJTOVAN system, then the value of the lost files would be only the lost time of the AT&T systems expert on the project, approximately $1,250.

On the other hand, if the lost files reflected a weakness in the overall network operating under stress, then the value of the loss would be too great to estimate. The weakness would not surface until the Robbins AFB communication system was put under stress.

Shadowhawk was acquitted of this charge because the trial court felt the records destruction was taking place without his knowledge and as a byproduct of this theft of data.

EVIDENCE DEVELOPED BY THE US Secret Service in Chicago established that Shadowhawk's method of operation was based less on genius and more on using passwords, user Ids, and hacking techniques learned from hacker bulletin boards. Typically, he gained access through common people errors, such as easily guessed passwords, default passwords left on the computer, or unrestricted dial-up modems.

Once he was on a computer he used techniques published on bulletin boards to become super user and immediately installed trapdoors and Trojan horses that would allow him to reenter in the event he was discovered by a systems administrator and kicked off the system.

One such Trojan horse worked on an AT&T-designed, time-triggered, audit-security program that scanned its computers periodically, checking the validity of passwords on file. Invalid passwords and passwords that were not recognized were removed from the system.

Shadowhawk changed this periodic program to modify the access permissions of the password file to be open, not closed, after the scan, thereby ensuring that even if his password were deleted by the scan he could get right back in through the reopened password file door. He passed this tip on to others through the bulletin boards and described his system for installing these time-triggered trapdoors on bulletin boards.

After securing his position on the computer, Shadowhawk methodically checked the electronic mail traffic in the computer's memory for any passwords or user Ids left behind. Passwords and user Ids were also searched out in the computer's system files. He then turned his attention to the source code files on the computer to see if the computer contained any programs of interest. If interesting files were found, they were copied and placed in an archive file for transfer. When Shadowhawk left the AT&T computers, he generally tried to remove all evidence that he had logged on to the files, making it difficult to trace his attack.

The trial evidence showed - and the defendant admitted on cross-examination-that part of his activities involved the theft of valuable telephone services from the Allnet and Sprint telephone systems by fraudulently using calling card numbers. No specific dollar value for this theft was determined by Allnet or Sprint.

Shadowhawk later explained to the Secret Service and FBI that he obtained calling card numbers from the various bulletin boards he used. He also noted that while he could have hacked out other card numbers himself, he used the numbers from the BBS because they would be so heavily used it would be impossible for the authorities to pursue or prosecute any one thief.

The charges brought against Shadowhawk under 18 USC 1030 required the government to establish that the defendant specifically intended to violate the law. Such intent is established by direct evidence, such as the defendant's admissions, and by circumstantial evidence.

Some of the strongest evidence that Shadowhawk was aware of the illegal nature of his actions came from the warning screens AT&T placed on the entry ports to its data network (see the accompanying box). These screens were followed up by clear warning screens at the beginning of much of the source code downloaded by Shadowhawk. The screens indicated that the information was fully owned and protected by AT&T Bell Laboratories.

These warning screens were located in the records seized from the defendant and were printed out and offered as evidence. They clearly established that the defendant was well aware he was illegally attacking a protected system and protected data files. Further substantial evidence of intent came from the other records seized in the search and from Shadowhawk's prior arrest history.

DURING THE EXECUTION OF A search warrant against his residence on September 4, 1987, federal agents and agents of AT&T recovered 52 stolen AT&T software programs stored on Shadowhawk's home computer, plus software programs stolen from MIT. Federal agents also recovered software programs from his computer that were specifically designed to attack computer networks and install Trojan horses. Handwritten logbooks also disclosed 22 other computers at AT&T and other institutions that Shadowhawk had installed trapdoors on.

Shadowhawk arrived home while the search was underway. Initially, he denied that he had used the name Shadowhawk when he was questioned by the Secret Service and FBI. But he admitted he had broken into AT&T computers and stolen AT&T copyrighted Unix source code.

Shadowhawk acknowledged that he knew he was acting illegally when he copied and stole the materials, and he also admitted that he had been attacking AT&T computers since about September 1986. He noted that his ability to steal the AT&T software had been limited until his parents bought him an AT&T PC 3B I computer with a UNIX operating system in May 1987. He eventually admitted that he had used the name Shadowhawk when he authored messages on computer bulletin boards that provided other hackers with the passwords log-ins and locations of numerous AT&T computers and the procedure for successfully attacking the computers.

Shadowhawk's bulletin board messages also detailed how hackers could successfully

* enter AT&T computers undetected,

* change the password and system files on the computer,

* steal information from the computer through the use of electronic mail features,

* create trapdoors and Trojan horses on the computer to make subsequent reentry easier, and

* erase tracks on the computer that would disclose that the computer had been attacked and then leave the AT&T computer.

Shadowhawk's statements to the federal agents were incriminating but, in retrospect, clearly less than candid. He admitted he was Shadowhawk at least three times but only after it was clear the agents knew he had used that name on the bulletin board messages.

He said he did not know he was attacking a NATO computer in North Carolina, but the trial evidence established that Shadowhawk placed the call directly to the North Carolina computer from his home telephone. He denied taking artificial intelligence source code, but the trial evidence showed he had established an elaborate remote access path to steal the artificial intelligence program worth $1 million from Bell Labs in July 1987. He still had it on his computer in September 1987.

Shadowhawk said he never took an AT&T program known as Cosmos, but the computer logs established he had deliberately searched out the computer-aided design program known as COSMOS. He told the agents he never put any Trojan horses on the computers he entered, but the testimony of AT&T'S George Otto established Shadowhawk had left Trojan horses on the AT&T Bell Labs R&D computer in New Jersey when he took the Al program.

During cross-examination, Shadowhawk admitted that on August 1, 1986, he was arrested and charged by the Chicago police with unlawful use of a computer. On that occasion he had gained unauthorized remote access to the computers of Keller Graduate School of Management in Chicago and erased some of the school's access codes. Shadowhawk then published his procedures for attacking the Keller computer on a local BBS in Chicago.

Illinois Bell provided the police with information that led to a consent search of his house and the discovery of computer printouts that linked Shadowhawk to the business school break-in. He admitted committing the crime and was released to his parents. He was advised by the Chicago police department that his BBS message was used by another hacker to shut down Keller's computers and caused substantial damage to the system.

AT TRIAL SHADOWHAWK'S ATTORney contended that Shadowhawk had not violated 18 USC 1030 because none of the computers he had attacked was specifically owned by the federal government. The government responded that 18 USC 1030 defined a federal interest computer as a government computer or one of two or more computers used in committing the offense, not all of which are in the same state. This set the parameters.

The government then noted that Shadowhawk had attacked the AT&T computers in North Carolina, New Jersey, and Georgia with his computer in Chicago and the assistance of a compromised AT&T computer at Bell Labs in Naperville. The government argued and the Court agreed that by linking computers to create this temporary network Shadowhawk had met the definition of a federal interest computer as defined in 18 USC 1030.

In dismissing the defendant's claim, the trial court noted that the federal interest computer language was Congress's way of establishing the interstate nexus frequently required in federal statutes.

Shadowhawk's attorney also contended that the government had not established that Shadowhawk had acted with intent to defraud, that he had only copied AT&T files, and that the original files were left unaltered on the AT&T computers. The attorney also argued that Shadowhawk had not sold copies of the files to anyone else and therefore had not made a profit from the files he had stolen from AT&T.

The court, however, again concurred with the government that intent to defraud included either a loss to the victim or the taking of something valuable by the defendant. The evidence established that the market value AT&T attached to the various pieces of source code involved was well in excess of $1 million, with the value of the artificial intelligence program alone being $1 million.'

The evidence also established that the stolen programs clearly had value to Shadowhawk, who admitted that by using the stolen programs he had saved a substantial amount of money that he would have had to spend if he purchased the software on the open market. Under the facts presented, the court determined that Shadowhawk had clearly acted with intent to defraud.,,

At sentencing, the government called for substantial incarceration based on the following factors:

9 The quality of stolen software (52 separate programs) and the value of the stolen data ($1,120,000) were substantial.

* The AT&T costs ($174,841) associated with the break-ins were also substantial.

* The degree of preparation and planning used by the defendant showed that he had executed well-planned attacks calculated to maximize the amount of data he could steal and minimize his chances of being caught. The government argued that but for the actions of the AT&T investigators and federal agents, the defendant would still be stealing computer data by remote access.

* Shadowhawk's attacks were not isolated activities. Rather, as he admitted

* cross-examination, since 1985 he had been hacking and stealing computer data from computers in schools and businesses.

* The defendant's attacks against the Keller business school and the disclosure that his bulletin board information about the attack had been used by someone else to shut down the business school's computers were very aggravating.

As the defendant acknowledged during cross-examination, the Keller incident put him on notice that his bulletin board messages could be used to damage computers and the businesses that use them. He also admitted he promised his parents he would stop hacking. But he further admitted that shortly after the Keller incident and his promises to the police and his parents he began breaking into AT&T computers and publishing information about his attacks on computer bulletin boards.

The government argued that while the defendant was young, he nevertheless had established a pattern of continuing criminal activity and that probation, which was essentially the tactic used by the Chicago police after his juvenile arrest, had been completely ineffective. It was also argued that Shadowhawk had learned to manipulate the system to use his juvenile status as a way to avoid punishment.

The government also argued that the development of computers as an integral part of the American government, scientific, and business communities had also generated groups of technologically sophisticated thieves. It was further noted that these high-tech street gangs could destroy individuals and institutions from any location in the world as shown by the hacker harassment of Newsweek reporter Richard Sandza, who published articles critical of hackers.

The argument was also made that many computer crimes were never reported. Numerous reasons were cited for this phenomenon. Embarrassment and fear of potential bad publicity were cited by some victims. Other victims indicated that the amount of time involved working with investigators and prosecutors was seldom cost-effective, especially in view of the low probability that the defendant would receive a prison sentence or be ordered to make restitution.

Victims also had little faith in the criminal justice system's ability to prosecute complex computer crimes or cases involving juvenile offenders. Both the juvenile and his victim had been schooled by the movie War Games to believe that the juvenile is beyond the reach of the law.

The government's position was that companies and individuals had to understand that computer-supported crime had to be reported if prosecutors and the courts were ever going to protect their right to the tangible and intangible property they develop and store on computers.

The government finally argued that a clear message had to be sent to the public at large and the computer community in particular that unauthorized attacks on computers and the theft of computerized information would not be tolerated by the courts.

The court sentenced the defendant to nine months in prison plus two and a half years' probation and ordered him to pay $10,000 in restitution to AT&T out of his own pocket. Shadowhawk began serving his sentence in a prison in South Dakota on February 27, 1989.