NATIONAL CENTER FOR DIGITAL INTRUSION RESPONSE
NCSA • 1205 W. CLARK ST. • URBANA, IL 61801

Technical Report NCDIR-2008-01
www.ncdir.us

Whitepaper Version 1.1 (DRAFT)
Last modified: February 6, 2008

FBI Major Case 216: A Case Study

National Center for Digital Intrusion Response[1]

[1] NCSA, 1205 W. Clark St., Urbana, IL 61801

NCDIR is funded by the Federal Bureau of Investigation and is a collaboration between the FBI and the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

1 Overview

This case study describes FBI Major Case 216, which ultimately became a collaborative investigation between the FBI and site security professionals into a series of cyberattacks that took place from August 2003 to March 2005. Incident response specialists at the National Center for Supercomputing Applications (NCSA), located at the University of Illinois at Urbana-Champaign (UIUC), played a significant and crucial role in this investigation. The attacks encompassed over a thousand sites, including high-security military sites and federal research laboratories, university sites, private sector sites, and machines owned by individuals, both in the U.S. and in Europe. In one case, a large company (Cisco) reported the theft of source code, which was later published online. The case drew much concerned interest from the FBI and the Departments of Energy and Defense particularly because of the initial, very real possibility that the attacks were sponsored by a foreign state. However, most of the damage sustained came in the form of time spent investigating the intrusions; notifying sites and users; and cleaning up, repairing, and securing the compromised systems. Investigation participants, estimate the cumulative cost of the Stakkato intrusions to be in millions of dollars. At its peak, the investigation involved 50 federal agents.

Ultimately, the intrusions were traced back to a 19-year-old man in Uppsala, Sweden, nicknamed "Stakkato," who had begun the attacks when he was 16. Convicted of having gained unauthorized access to several Swedish university networks, "Stakkato" is still under investigation by the FBI for the Cisco code theft [1].

2 First signs

The National Center for Supercomputing Applications, a production supercomputing facility first funded in 1986 by the National Science Foundation, is heavily used by thousands of researchers all over the world in government, education, industry, and academia. Because NCSA's resources are open and accessible, rather than hidden behind firewalls (as in the case of many DoD, DoE, and industrial supercomputing facilities), protecting NCSA's systems from compromise is a priority. NCSA's Incident Response and Security Team (IRST), first organized in 1993, focuses on detecting and responding to attacks and intrusions and preventing system vulnerabilities.

NCSA first became aware of the attacker's presence on March 20, 2004, when he gained access to an NCSA machine, from which he began testing several others for vulnerabilities. Jim Barlow, who leads NCSA IRST, first discovered the attack on a Sunday evening as a result of an alert triggered automatically by a system that monitored services such as intrusion detection, network flow analysis, and log files. The alert was triggered by an atypical surge in the number of connections for this machine at this particular time of day.

Barlow first had to establish that some service was not being run legitimately on the machine that would account for the surge in activity, so he scanned the machine to find out which ports were open. He also began collecting the network flows to and from the machine to see if the traffic could explain the surge's cause. The scan alerted Barlow that there was a problem: open port 41705 was running a backdoor SSH client, which granted remote access to an unauthorized user. Had other hosts been similarly compromised? A scan of the entire network revealed that indeed, two other machines were running the same malware. In fact, one of these machines turned out to be a supercomputer that was also a node on the TeraGrid, a National Science Foundation (NSF)-funded project that provides distributed high-performance computing resources across multiple sites to scientific researchers. The world's largest, most comprehensive distributed computing infrastructure for open scientific research, the TeraGrid is used for extremely large-scale simulations in areas such as molecular dynamics, seismology, atmospheric science, and cosmology. Like the NCSA machine, the other nodes are also located at universities and national laboratories across the country.

Figure 1. Map of the nine partner sites of the NSF TeraGrid. Dedicated machines at each of these sites together form a powerful distributed supercomputer facility capable of extremely large-scale computations. Academic partners include NCSA (UIUC), San Diego Supercomputing Center (University of California at San Diego), Texas Advanced Computing Center (University of Texas at Austin), Pittsburgh Supercomputing Center (University of Pittsburgh), and supercomputing facilities at Caltech, Indiana University, and Purdue. Argonne National Laboratory (ANL) in the southwestern Chicago suburbs and Oak Ridge National Laboratory (ORNL).

At the time of the attacks in spring 2004, the TeraGrid's combined resources included 24 teraflops of computing power and 1 petabyte of data storage, connected by a high-speed network. As of late 2007 those numbers had grown to more than 750 teraflops and 30 petabytes, interconnected at 10-30 gigabits/second via a dedicated national network. [3]

2.1 Contacting other compromised sites

The TeraGrid's security group meets on a weekly basis to discuss policy and incidents encountered by member sites, which made it easy for NCSA IRST to communicate what they'd found. Early on, it became apparent that many TeraGrid sites had been compromised in much the same way: the attacker would install trojans that could then collect usernames and passwords from that site. Because many of the TeraGrid sites share the same user base, many users simply use the same usernames and passwords for multiple accounts, making it

easier for the attacker to move between TeraGrid sites. Users at several different sites reported receiving taunting messages from an intruder calling himself Stakkato. One user even reported that, having hacked into her machine, Stakkato had even erased her file directory and deleted a year and a half's worth of email after eavesdropping on an email exchange with a system administrator in which she called the intruder a "quaint hacker" [4].

It became clear to the investigators that the attacker had a number of specific vulnerabilities that he would attempt to exploit at a given site. As the investigation progressed, NCSA IRST compiled a list of all these vulnerabilities, as well as the directories where the attacker would typically install malware and store the rootkit he used to harvest usernames and passwords. Whenever he moved to a new site, NCSA IRST would contact that site's administrators and send them this information to alert them to the case and help them track the intruder.

3 Law enforcement is brought in

Often, when a system administrator discovers that a machine has been compromised, he will shut the machine down, investigate the incident, and clean up and secure the machine; the attacker will then depart for more vulnerable sites. However, in this case, the attacker was extremely persistent in breaking into TeraGrid machines through compromised accounts, causing NCSA investigators to wonder about his motivation. These sites were difficult to secure because they comprised a large number of endpoints at universities and research institutions that were not under the control of the TeraGrid organization. While the thousands of users at these sites could be notified that their accounts had been compromised or were at risk for compromise, they could not necessarily be required to change their passwords or modify their online behavior. It was at this point that the NCSA investigators realized they needed to notify the FBI.

When an intruder persistently threatens computing resources and institutional and user data, a university has an acknowledged interest in assisting with a federal investigation. However, because of privacy concerns, data crucial to the investigation cannot be provided unless search warrants and subpoenas are issued. First, the NCSA security team had to alert the UIUC legal department of their intent to engage with the FBI. The UIUC legal department then arranged a meeting between NCSA's security team, the campus security team, the campus police, and a local FBI agent. The NCSA security team described what had happened and what they knew of the extent of the compromises both at NCSA and at other sites who were also in the process of contacting their local FBI. The FBI Springfield Division opened a case, as did a number of other field divisions in whose territories the compromised sites were located.

Computer intrusion cases are especially time-critical; however, the collection of essential evidence can be problematic. Simply confiscating an entire compromised machine as evidence may render a crucial computing resource unavailable to the victim organization and its users for the duration of the investigation. In the case of the NCSA attacks, for example, one of the machines was a supercomputer used not only by NCSA and other UIUC

researchers but by researchers all over the country. One solution to the problem of collecting evidence from heavily-used computing resources is to create an image, or exact reproduction, of the hard disk. However, this too can be problematic: the volume of such hard disks is often measured in terabytes (thousands of gigabytes), and sifting through all of this data not only raises potential user privacy issues but can be needlessly overwhelming and time-consuming to investigators. Additionally, because university data retention policies often have short timeframes to safeguard user privacy, evidence of an intruder's activities recorded in network traffic logs often disappears with the periodic instution-mandated destruction of these logs.

For the next few weeks the NCSA security team continued to meet with the FBI and with University legal counsel to determine what data the FBI required for the investigation, a crucial and necessary prerequisite to serving subpoenas or search warrants for computer data. This involved determining which IP addresses had been affected, what kind of data they had already, and what items, specifically, they would need to request from other sites. In particular, asking for specific data items, rather than simply requesting all data and sifting through it, cut down substantially on the time and effort needed.

Establishing a productive working relationship between a case agent and an institution or organization victimized by cyberattacks is extremely important to the smooth and efficient collection of essential evidence, especially if this is the agent's first cyberinvestigation. While Craig Adams, the agent covering MC 216, had a background as a systems engineer which aided him considerably in the investigation, his working knowledge of cybersecurity issues and procedures at the time was not as extensive as that of a typical, active incident responder. The NCSA security team was able to provide guidance in determining which logs would be most relevant to the case.

4 Method of attack

Further investigation by the NCSA security team revealed that the intruder's plan of attack for infiltrating and compromising large computing sites was complex and well-organized. Initially, he used known exploits to infiltrate a small number of hosts onto which he then installed trojaned secure shell (trojan-ssh) clients. Users would log into other systems, inadvertently using the trojaned ssh clients which would then harvest their usernames, passwords, and the IP addresses of the machines they were logging into.

With these stolen credentials, the attacker then would gain access to the external systems and use a rootkit, a software package used to exploit vulnerabilities, to gain administrative privileges on those systems, where he would then repeat the process, installing trojan-ssh clients, collecting more usernames and passwords, gaining access to new machines, and thus gradually increasing his network of compromised systems.

As the attacker's "network" evolved, it also came to include machines that served as supporting infrastructure. The trojaned SSH clients would send harvested user data back to yet another compromised machine that served as a password collector, which stored the data for future use. All user data was addressed to a statically-configured hostname, which the

attacker managed anonymously through a public dynamic DNS site. Dynamic DNS permits a domain owner to map a static domain name to different machines, so whenever the attacker thought he had been discovered or was being monitored, he would simply move the password collector to a different machine, which he did several times over the course of the investigation.

The attacker also maintained a repository for his malware on another of the machines he had compromised early on which a web server was running. Unbeknownst to this machine's owner, the attacker accessed and downloaded these tools every time he gained access to a new host and used them to escalate his privileges on the new conquest. Finally, to make the task of tracking him difficult (or impossible), the attacker would log into compromised systems circuitously by way of a number of distributed intermediate systems.

Ironically, once discovered, the components of this relatively sophisticated support framework increasingly proved key to monitoring the attacker's movements and, ultimately, to his apprehension.

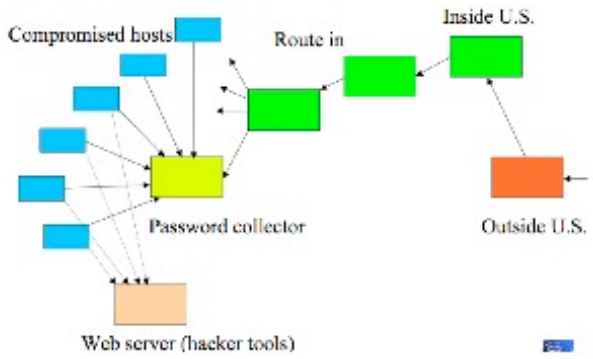

Figure 2. The attacker's U.S. network, his point of entry, and his supporting infrastructure.

5 Tracking the intruder

By May 2004, the holes that had allowed the intruder to install his backdoor software had been patched, and NCSA systems had been secured against him. The NCSA security team knew what kind of behavior to watch for, what kinds of exploits the intruder was using, and how he managed to compromise and obtain user accounts. Now that they had a good idea how the intruder was operating, they could try to monitor and track his movements from host to host, using a network of honeypots, while at the same time attempting to trace him back to his originating IP address.

5.1 Creating a honeypot

A honeypot is a kind of decoy system set up to lure and possibly trap intruders intent on breaking into a real information system. It is usually unprotected and may contain data or resources that appear to be valuable in some way. A honeypot may be a single machine or

an entire network that appears to be part of the intruder's target but is actually isolated and carefully monitored for unauthorized access.

Honeypots are deliberately exposed and vulnerable to attack and can often be compromised within a matter of minutes or even seconds. The challenge that the investigators faced was ensuring that the honeypot they constructed would attract this specific hacker. However, they were able to accomplish this by tailoring the site's vulnerabilities to the intruder's preferred method of attack: in this case, inserting a username, password, and honeypot IP address directly into the intruder's password collector to lure him to it, in the hope that he would install a trojan-ssh client on the decoy machine. The NCSA honeypot, for example, was made to look as if it were used, with a few logins a day, and a "user" logged in whose activities the attacker could monitor.

As the investigation came to encompass several DOE sites, the investigators began to develop a network of honeypots so that when the intruder stole a user's credentials, the first thing he would do after logging in was to check out the SSH known host spot to find out what machines the user typically logged into from that account and then try to use the same credentials to try to access the user's account on that machine. Anticipating this behavior, the investigators created several user accounts on multiple machines in the honeypot network which used the same usernames and passwords—an easy target for the intruder.

Stakkato did take the bait and hack into these accounts as anticipated. In many cases monitoring an intruder's behavior in a honeypot can be the key to catching him. However, in this case, the investigators were able to reverse engineer Stakkato's rootkit (Section 5.2.3.1) and trace him back to his point of origin before the honeypot surveillance yielded significant results.

5.2 Monitoring points of presence

To determine the location from which the attacker was operating, the investigators conducted a manual traceback. They began by posting inquiries on some security mailing lists about who or which sites were responsible for particular IP addresses, making it clear that they were only interested in looking at traffic and not at data. In this case, it helped that the intruder tended to use a path through the same machines for weeks at a time. The traceback was a highly collaborative activity, involving security engineers at NCSA and SDSC, FBI personnel, system administrators at ISPs and universities in Sweden, and many other individuals and organizations here in the U.S. and abroad.

To track the intruder and monitor his behavior, the investigators ultimately came to rely on four different points of presence: the site where the intruder stored and downloaded his software, the intruder's password collector, the machines the intruder moved through as he made his way into the United States, and ultimately, the intruder's own home machine.

5.2.1 Malware repository

The website from which the intruder downloaded his trojan SSH client and rootkit was a server maintained by a CS student in Maryland for his own purposes. Rather than simply advise the machine's owner to clean up his site and patch his vulnerabilities, the investigators contacted him, told him what was going on, and asked him if he could let them have his weblogs on a regular basis. The student readily agreed and ultimately gave root access to the investigators so they could simply log in and take whatever logs they needed, which they did, every day, morning and night.

5.2.2 Password collector

The investigators also began to monitor the intruder's password collector as it shifted from machine to machine. Whenever someone would log into a machine on which the intruder had installed a trojaned SSH client, the client, spoofing the genuine SSH client, would send the username, password, and IP address of the compromised machine back to the password collector. The password collector itself could easily be moved, thanks to a dynamic DNS hosting the intruder had embedded in the software, which permitted him simply to go to the dynamic DNS site and change the IP address, causing all the trojaned SSH clients to then transmit user information to the new machine. The investigators would contact the owners of the machines that were being used as password collectors and request their logfiles so they could find out what sites had been compromised with the trojaned SSH client.

Monitoring the sites that served as the intruder's password collectors allowed the investigators to notify the hacked sites and send them the usernames and passwords that had been compromised. However, it also provided some insight into the intruder's behavior and frame of mind. For example, he often chose as usernames the names of some of the investigators who were involved in tracking him down, such as the FBI agent who opened up the case in Chicago, or a system administrator in California whose site he'd attacked.

5.2.3 Login path

Investigators also began contacting system administrators for the machines that appeared to serve as the attacker's entry points into the U.S. As the investigators uncovered the intruder's trail, they found that his usual *modus operandi* was to move through a few machines in Europe first before making the jump to U.S.-based servers, from which he would then launch his attacks.

5.2.3.1 The Unsuckit tool

The Linux rootkit Stakkato used for all his attacks was called the Suckit (short for "Super User Control Kit") rootkit. Written by two Czech hackers in 2001, Suckit needed no kernel support, which enabled it to evade a common administrative security measure of disabling support for loadable kernel modules. Suckit used a spoofed packet to bypass firewall configurations, enabling a hacker to create and encrypt a remote-access, connect-back shell.

This rootkit was also hard to detect because it did not alter the target filesystem and could hide processes, files, and connections, fooling common Linux security tools such as `fuser`, `lsof, netstat, ps,` and `top`. [5]

An important breakthrough in the traceback conducted by the incident responders occurred in July 2004 when the owners of one of the machines in the attacker's regular network routes relocated to a new position at a small Massachusetts college named Simon's Rock. An interested site administrator there began to preserve tcpdumps of all the traffic on this machine and became involved in the investigation. As he examined the attacker's rootkit, he realized that it could be reverse engineered if he could just break the rootkit's encryption key, giving investigators clear text of all the attacker's activities. With the help of a DoE researcher, he was able to accomplish just that, creating a tool named—logically—Unsuckit.

The Unsuckit tool proved a powerful weapon against the intruder. Investigators were able to stream data from the tcpdumps of compromised machines through the tool, generating clear text of the attacker's every movement—every command he ran, all the directories and files he accessed on machines providing tcpdumps. However, after a couple weeks the Simon's Rock system administrator who developed the Unsuckit tool realized the attacker's traffic was decreasing, signaling that he possibly suspected discovery and was preparing to move on. The administrator knew he would have to act quickly, so, starting with connections away from the Simon's Rock site, he was able to trace a path back through all the machines the attacker was using or had connected through.

5.2.4 Originating machine

The Simon's Rock traceback ended in a machine with a dynamic DNS hostname, running both an IRC server and a web server, located in Sweden. It was the final piece of the puzzle: the intruder's own home machine. Because these services were open to the world, the machine's traffic could be monitored legally but covertly using web and IRC proxies. The IRC server yielded a list of nicknames (nicks), some of which the investigators recognized from elsewhere; with more digging, they were able to come up with information on the other IRC users, which included the suspect's girlfriend and several of his friends.

The suspect's webpage and other public directories on his machine also provided useful information: the handle Stakkato; photographs of himself and his classmates, four of whom had accounts on his machine; his likes (milk) and dislikes (white hats); and, tellingly, several phrases that appeared in the taunting emails he sent to site administrators and users whose accounts and machines he'd compromised.

Figure 3. Photos of the intruder known as Stakkato, found in public directories on his home web server. Upper left: Stakkato's drink of choice makes it probable that he is the author of the IRC profile on his machine that declares, "I like milk." Lower right: Stakkato's school picture. He is in the middle of the front row (arrow above his head, the word "ARE" on his shirt).

6 Apprehension

While FBI and NCSA investigators were monitoring and tracking Stakkato's movements in the U.S., in Sweden there was a parallel investigation into a very similar series of attacks at several universities, including one that compromised over 400 machines. As in the U.S. investigation, Swedish system administrators also began tracing the frequency of certain words and phrases from the password collector and other compromised machines back to the IRC channel on Stakkato's machine. After sifting through large numbers of IRC logs and identifying certain handles, Swedish investigators were able to match the nicknames of suspects to their actual owners.

Swedish law enforcement, however, was unable to engage as quickly and actively as the FBI did in Major Case 216, in large part because Swedish privacy laws are very strict and make wiretapping suspects far more difficult. On November 1, 2004, a new law took effect that justified wiretapping for the purposes of data intrusion cases. In the meantime, along with their American counterparts, the Swedish investigators continued to watch, wait, and gather evidence. Swedish law enforcement finally engaged with the FBI and NCSA investigators in

early January, and finally, on March 9, 2005, they apprehended Stakkato and seized his machines and data. The intrusions ceased immediately. [6]

7 Lessons learned

Large-scale cyberattack investigation requires a trusting, effective working relationship between law enforcement and IT. The most important lesson to come out of Major Case 216 was that cooperation and collaboration was essential among law enforcement, cybersecurity professionals, administrators of targeted sites, and targeted organizations themselves. Cybersecurity professionals and administrators at targeted sites were a driving force in the investigation because they had specific expertise in handling security issues at their sites, effective tools for log and data analysis, the ability to closely monitor the intruder's activities on their systems, and a more or less trusted network of contacts at other sites and institutions, which became vital as the scope of the investigation widened. In particular, NCSA incident responders played a major role in the investigation. The former Special Agent with whom NCSA IRST collaborated argues that assistance from an organization similar to NCSA continues to be necessary to the investigation of large-scale cyberattacks. He recommends that trusted security professionals at targeted sites should be engaged in the investigation process as early as possible.

Information needs to be a two-way street between investigators and site administrators. Site administrators have a strong interest in keeping their systems secure. While information must be provided in a judicious manner, ensuring that potential information sources such as site admins are clearly informed about both the nature and the severity of a series of attacks helps to ensure their participation in the investigation. Major turning points in MC 216, such as the ability to closely monitor the webserver that functioned as Stakkato's malware repository (Section 5.2.1) and the development of the Unsuckit tool (Section 5.2.3.1) were due to the assistance of willing, cooperative administrators in Maryland and Massachusetts who had been made aware of the scope of the attacks and the investigation.

Likewise, communication between investigators is also important. Agents may only be working on the portions of a cyberintrusion case specific to their locales, but they still need to clearly understand the case as a whole so that they can communicate effectively with potential information sources. Communications between field offices should contain clear, comprehensive summaries that include crucial information that can be communicated to potential information sources.

Agents working on investigations into cyberattacks need to be properly equipped with the appropriate hardware and software. Throughout the duration of 216, tools for parsing data were scant and equipment was often old and outdated, which frequently hindered collaboration with NCSA incident response specialists. Laptops with up-to-date, stable, secure operating systems and high-speed internet are basic necessities for working on computer-related cases. Analysis tools and the prerequisite knowledge for using them effectively are also crucial and can improve the effectiveness of working relationships with incident responders and site administrators.

There is a need for widespread, if basic understanding of computing and computer systems-related issues across the Bureau. This became a concern for communication both internally and externally. In 2004, agents submitting time-sensitive requests such as trap-and-trace found that supervisors were often unfamiliar with concepts and terminology in computer networking and security critical to the case. Additionally, agents who were unfamiliar with computing and cybersecurity-related issues were often less effective in communicating with and getting cooperation from administrators and machine owners who were potential information sources.

Documentation mechanisms across the Bureau need to reflect accurately how criminals employ digital technologies. For example, in 2004 agents found that the paperwork for submitting trap-and-trace requests was designed for phone surveillance requests and that there were no appropriate fields on these forms for IP or email addresses. To complete their requests, they would have to manually modify the form. Similarly, electronic communications containing leads concerning computer trespass cases often included IP addresses or URLs instead of the names or locations of subjects, and because these terms were less recognizeable, they were less likely to be indexed and correlated. As a result, many agents worked on similar intrusions in isolation, unaware for some weeks that they all could have been perpetrated by Stakkato.

8 Timeline of 216 Events

Following is a chronology of events that occurred before, during, and after the investigation of FBI Major Case 216.

August 2003	• First known related compromised box discovered with rootkit, tools installed in directory.
October 2003 – December 2003	• Attacks on machines at BNL, Caltech, Colorado. • At Caltech, hacker actually initiates talk sessions with users and taunts them (e.g., I own the machine, you can't kick me off, I'll be back…)
March 2004	• Attacks on machines at Berkeley, LBL, NCAR ANL, SDSC. • From one compromised machine at NCAR, an attack is launched on NCSA machines. • Attacks on TeraGrid machines.
April 2004	• A system administrator at Stanford begins to notice a pattern of attacks and puts up a Web site describing the vulnerabilities the hacker is exploiting and his tools of choice, with particular attention to abnormal TCP traffic on Port 53 [7]. • Intruder sends bragging email referencing Kevin Mitnick, with phrases such as "my kung fu is great." • The website of Tsutomu Shimomora at SDSC is hacked and content replaced with graphics, profanities, and messages along the lines of "you're not all that." Shimomura is famous as one of the investigators who helped track down and catch cybercriminal Kevin Mitnick in 1995. (By 2004, Shimomura was no longer working at SDSC and website was no longer active.) • At White Sands Missile Range in New Mexico, an attacker gains access to an internal, unclassified machine providing weather forecasts. • The DOE's Computer Incident Advisory Capability (CIAC) notifies the Forum of Incident Response and Security Teams (FIRST) about the attacks on the national labs. • AP and Washington Post cover March 2004 attacks, labeling them "TeraGrid attacks." [8]

May 2004	• Working with NCSA and SDSC, administrators at UMN and CMU detect intruder traffic on their servers. Although they are not yet able to decrypt his rootkits, the investigators are able to decrypt other tools and activities, leading to the discovery of a password collector at the University of Colorado (Boulder?). • Internet2 community is contacted about the attacks, but there is no response. • Part of Cisco's Internetworking Operating System (IOS) is illegally copied and posted on the Internet.
June 2004	• Investigators contact and start tracking malware web distribution site.
July 2004	• First traceback completed. • Owner of a compromised machine at CMU moves to Simon's Rock College, MA. A system administrator at Simon's Rock becomes involved and, with help from a DOE lab researcher, reverse engineers the hacker's rootkit, creating the Unsuckit tool.
August 2004	• The manual traceback is completed and is found to match the traceback performed by security professionals in July. This traceback provides a crucial part of the legal foundation for the case against the intruder. • Swedish contacts are traced back to same individual via Swedish IRC channels.
September 2004 – January 2005	• While the FBI builds their case, intruder's movements are monitored closely to prevent the attacks from escalating out of control. System administrators at sites where attacks occurred are notified and provided with information about detecting attacks and patching holes. • Joint FBI/incident response efforts to apprehend individual are increased.
January 2005 – March 2005	• Swedish law enforcement agency begins cooperation with investigation after realizing that it links up with a similar investigation in Sweden. [6] • The intruder, a recent high school graduate known online as Stakkato, is apprehended. • Once the apprehension is made, all activity at monitoring points stops.

9 References

[1] "FBI investigates Swedish hacker," *The Local: Sweden's News in English*, November 19, 2007. http://www.thelocal.se/9140/20071119/

[2] "Security at NCSA," NCSA Cybersecurity Directorate, Oct. 2007. http://security.ncsa.uiuc.edu/wiki/Security_at_NCSA

[3] "About the TeraGrid," NSF TeraGrid. http://www.teragrid.org/.

[4] J. Markoff and L. Bergman, "Internet Attack Called Broad and Long Lasting by Investigators," *New York Times*, May 10, 2005.

[5] sd and devik, "Linux on-the-fly kernel patching without LKM," *Phrack Magazine*, Dec. 2001. http://www.phrack.org/issues.html?issue=58&id=7#article

[6] L. Nixon, "The Stakkato intrusions: what happened and what have we learned?" *CCGrid06 Cluster Security Workshop*, Singapore, May 17, 2006. http://www.nsc.liu.se/~nixon/stakkato.pdf

[7] Stanford University ITSS Information Security Services, "Multiple UNIX compromises on campus," *Stanford University ITSS Security Alerts*, April 6, 2004. http://www.stanford.edu/group/security/securecomputing/alerts/multiple-unix-6apr2004.html

[8] B. Krebs, "Hackers Strike Advanced Computing Networks," *Washington Post*, April 13, 2004. http://www.washingtonpost.com/ac2/wp-dyn/A8995-2004Apr13