The New Zealand Hacker Case: A Post Mortem

B. Endicott-Popovsky, D. Ryan, D. Frincke

A typical incident response pits technicians against networks that aren't prepared forensically. [1, 2] If practitioners do consider collecting network forensic data, they face a choice between expending extraordinary effort (time and money) collecting forensically sound data, or simply restoring the network as quickly as possible. In this context, the concept of organizational network forensic readiness has emerged.

The following is a discussion of selected computer crime cases, spanning a period of time of several year, that together demonstrate the need for a preventive and proactive response to malicious intrusion over a reactive one. It concludes with recommendations for how to "operationalize" organizational network forensic readiness.

I. INTRODUCTION

A typical incident response pits technicians against networks that aren't prepared forensically. [1, 2] If practitioners do consider collecting network forensic data, they face a choice between expending extraordinary effort (time and money) collecting forensically sound data, or simply restoring the network as quickly as possible. The latter means key evidentiary files most likely are altered in the process, limiting their forensic value. With limited interest in pursuing legal action, those administering networks most often make the expedient choice—responding to distraught users by restoring network function as soon as possible, ignoring the rigors of collecting and preserving forensically sound data. [3]

Recent legislation in the United States—Sarbanes-Oxley, the Health Information Portability and Privacy Act (HIPPA)—is changing this picture. In the interest of establishing evidence of having exercised reasonable care to protect data on their networks, legal counsel have begun urging organizations to invest in procedures and technology that will allow collection of forensically sound data defensible in a court of law. [4]

To understand the urgency for 're-thinking' incident response and the role of digital forensics, a discussion follows of two selected computer crimes that demonstrate the need for a preventive and proactive response to malicious intrusion over a reactive one. It concludes with recommendations for how to "operationalize" organizational network forensic readiness1.

II. THE CURRENT CONTEXT FOR CYBER SECURITY

A pattern of mutual escalation exists between malicious intruders and their victims. [5] (Figure 1) At an intuitive level, this could be described as a "Cyber Security Arms Race."

As cyber defenses improve, malicious intruders improve their skills in order to continue to wage successful attacks. As their skills improve, cyber defenses improve in order to repulse these more effective attacks, and so on, back and forth in a never-ending cycle. [5]

With both intruder and victim reacting in relation to one another, the Cyber Security Arms Race behaves like a system. [5]

---

1 Defined as 'maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response.' [2]
Like all systems, this system is held in place by many factors including the mindsets of both intruders and targets, which will be examined through an analysis of two cyber crimes. The crimes selected for analysis are part of the computer forensics educational curricula developed by one of the authors. [6]

### III. THE NEW ZEALAND HACKER CASE

A typical intrusion follows the steps in Figure 2. [7]

Attackers do reconnaissance in the first three steps:
- **Step 1** Footprinting (gathering open source information),
- **Step 2** Scanning (for services listening on networks)
- **Step 3** Enumerating (more intrusive probing).

This precedes
- **Step 4** Gaining Access (intruding).

Once inside, the intruders:
- **Step 5** Escalate Privileges to gain access and
- **Step 6** Pilfer sensitive information,
- **Step 7** Cover their tracks (altering logs, hiding tools),
- **Step 8** Create back doors (for future re-entry).

In the New Zealand Hacker Case, malicious intruders followed this general model. In 2002, it was referred to as "the largest security incident in New Zealand history." [9] Damages were estimated at $400,000. [10]

The case is used in the classroom as part of student discussions of "script-kiddie" behavior, [6] a term used by some to describe malicious intruders who use tools, written by others and readily available online, to accomplish intrusions.

The script kiddie is "someone looking for the easy kill. Their goal is to gain root the easiest way possible. They do this by focusing on a small number of exploits, and then searching the entire Internet for that exploit. Sooner or later they find someone vulnerable." [8]

The case involved activity observed in different locations, internationally. Theories about the numbers of perpetrators involved, their ages and motivation are based on media reports cited as the case develops.
A. Symptoms of the Attacks [11]

At one of the victim sites involved in this case, initial attacks were first reported on November 12, 1998. System administrators identified several unauthorized accounts and found related login records that gave evidence of intrusions. Systems logs showed the attacker executing a buffer overflow exploit. (Figure 3)

![Figure 3. Buffer Overflow Intrusion](image)

Reports began coming in from other system administrators at other sites that identified attacks from these intruders launched from compromised machines used as stepping stones. The attacks were traced back to the same originating ISP network. Over the next few days, pass through attacks were reported that crashed some Sun Solaris hosts running rpc.mountd.²

Sometime on or before November 15 someone using multiple stepping stones destroyed over 4,000 user websites, as well as 500 commercial web sites, hosted by a New Zealand Internet Service Provider on a server in the United States. [12, 13]

B. The Investigation

Through analysis of sniffer³ log files and undeleted command history files, system administrators were able to gather evidence that the intruders were using backdoors, installing sniffers, copying and accessing sniffer logs, and exploiting secondary systems. The intruders used a reconnaissance strategy of port scanning, looking for systems running the RPC port mapper, listening on tcp port 111. They were specifically seeking to identify hosts running the RPC mount daemon. Certain implementations of the RPC mount daemon were known to have a buffer overflow vulnerability. The intruders were using a published exploit to attack this service remotely, gaining administrative (or “root”) access to the host. [14]

Once gaining root access, they installed root kits⁴ and back doors for unfettered access in the future. Inside, they set up new accounts and installed network sniffers to capture logins and passwords. [15, 16] The compromised machines were used as stepping stones for attacks on other machines, often using a several-hop pattern before getting to the desired target⁵. [11]

C. Law Enforcement Outcome

There was evidence that several intruders were involved in the incidents described in this case. The individuals appeared to reside in several countries including New Zealand and the United States.

There were mixed media reports immediately after the incidents took place describing the individual in New Zealand, alternately, as underage, an ex-employee of the ISP, a college student, etc. [12, 13] Depending on the information source, his online moniker was given as either: "SharkDogg," or "spazrat," or "Acid Storm." [12, 13] It appears from this that accounts he used in these attacks were traded or shared or that an innocent party's identity was being used without their knowledge.

Later, there were media reports, that the intruder received a conviction and was sentenced to community service. [17] Although initially there were no laws in New Zealand at the time making cyber intrusion a crime, it is possible that authorities convicted him based on a related legal theory. [17]

² The exploit involved was written for Linux/x86 and not Solaris/SPARC (the result being segmentation faults on the SPARC processor) causing the systems to crash.
³ A program and/or device that monitors data on networks.
⁴ Automated tools for hiding intruders.
⁵ Attempting to disguise the actual origin of their attacks.
D. Victim Outcome

One target of these attacks documented the costs they incurred during the investigation. This included the effort involved with identifying and researching attacks on 18 different systems, analyzing and matching logs in order to trace the paths intruders took and restoration of the compromised systems. The I-CAMP model for documenting costs of incident response was used. According to their analysis, the investigator incurred costs of $27,794.54 + $4169.18 or approximately $1500/host examined. This included 417 hours of documented investigation time.

It should be noted that the primary purpose of this effort was not prosecution, but to identify as many involved systems as possible at the involved site and get them all taken off-line and out of intruders' hands at one time, rather than getting just a small percentage of them. Since sniffers were involved, any systems that were restored using the common “wipe and reinstall” method of dealing with intrusions would mean there would be continued bleed-over incidents from the sniffers that were still active, perhaps increasing the total number of compromised hosts and accounts and actually increasing the total damage suffered by the site (and other involved sites.)

E. Post Mortem

Given the 137,529 incidents reported by CERT in 2003, the last time such data was collected and reported by CERT, if each incident involved just one host at $1500 each, the total financial impact to those reporting problems would be $200,062,935.

Given that there were 417 hours of investigator time accumulated in documenting the case, or 23 hours per host, taking the same 137520 incidents (above) and again assuming each incident involved working with just one host, then 3,163,167 hours or 1581 people working full time for a year is implied.

IV. THE RUSSIAN HACKER CASE

Advancing to 1999-2000, United States v. Vasily Gorshkov is another well documented case that will allow analysis and insight into the challenges of pursuing accountability in intrusion cases. Like the previous case, this case has been used extensively in the classroom, as a demonstration of an intrusion by organized crime.

While the model for a typical intrusion follows the steps described in Figure 2, the Russian cyber criminals, Gorshkov and Ivanov, devised a completely unexpected scenario that didn't require an intrusion.

The Russian Hacker Case is one of the largest and most complex cases of criminal intrusion on public networks to have gone from forensic investigation through a successful prosecution. While perpetrated in 1999-2000 and prosecuted in 2001, the case continues to be a source of lessons learned for analysts exploring cyber crime and digital forensics.

A. Symptoms of the Attack

In 1999, seemingly unrelated complaints were reported to the FBI. These ranged from reported computer intrusions, computer outages, incidents of credit card fraud, and attempted extortion.

Several banks in different parts of the United States complained of web site defacement, intrusions, record theft and extortion. Numerous incidents of compromised systems were coming from the United States, Canada, the United Kingdom, Indonesia and Japan. In addition, e-Bay complained of "synthetic
auctions" and payment triggers, and PayPal experienced a rash of credit card payments from stolen cards. [21, 22]

The complaints of one particular ISP who reported a major intrusion, data theft and system outage, followed by an attempt at extortion, led to unlocking this series of crimes, tying them to a criminal enterprise in Chelyabinsk, Russia at tech.net.ru. [22]

![Chelyabinsk, Russia](image)

Figure 4. Home of tech.net.ru - Chelyabinsk, Russia [22]

After compromising the ISP's systems, the perpetrators identified themselves as 'computer security experts' from Russia and attempted to extort compensation from their victim, threatening to take them offline and do other damage if they didn't comply with their requests.

### B. Catching the Criminals

Working with the victim, a 'sting' operation was developed whereby the FBI set up an ersatz startup company, "Invita," and invited two of the malicious intruders to Seattle to "interview for jobs as security consultants." As part of their interview process, they were told they would be required to demonstrate their hacking prowess. [22]

When they arrived they were escorted to a business incubator that "housed the offices" of Invita. As the Russian intruders demonstrated their prowess using Invita equipment, previously installed keystroke loggers recorded log-ins, passwords and commands as they downloaded their tools from servers at tech.net.ru and repeated the steps that had gained them entry to the ISP. On the way back to the airport, both were arrested and incarcerated preparatory to trial. [23]

### C. The Investigation

In the meantime, the authorities performed "remote forensics" data retrieval on active servers at [http://www.tech.net.ru](http://www.tech.net.ru) & [http://www.freebsd.tech.net.ru](http://www.freebsd.tech.net.ru), downloading 2.3 Gb of data. [22, 23] Ultimately, forensic investigators discovered a wealth of information and tools, including root kits, scanners and sniffers, many exploits, 56,000 credit card numbers, bank records and entire bank databases, stolen transaction information from web hosting scams, network maps, login and password combinations and other assorted victim data. [21, 22, 23]

Incriminating Perl scripts were found that were designed to subscribe randomly to free email accounts (using random name generation, random country and domain binding) then populate an SQL database table with the results. Random generators for e-Bay and PayPal account creation were also found. The latter were randomly associated with names in stolen credit card databases. [21]

While the Russian gang had a variety of criminal projects underway, their major enterprise was a virtual business that fabricated both sides of online auctions, automating the process using the Perl scripts just described. Forensic analysts reconstructed the business model (Figure 5). [21, 22]
Summarizing the business process, the intruders' scripts would post non-existent products to sell on eBay. Different scripts would pay with stolen credit cards, which would cause payments to precipitate into PayPal accounts that another script created. Then a different set of scripts would create and generate email acknowledgements to the "buyer" and "seller," simulating the eBay process. [21, 22] By keeping credit card transactions below a threshold, they avoided triggering undue scrutiny. In less than 9 months, credit card companies were defrauded of over $25 million dollars. [23]

Since PayPal, at that time, was not making cash payments to international bank accounts, the criminals used the money accumulating in PayPal to buy goods through other online merchants, and then have them shipped to Russia where they were unloaded in the black market for cash through their network in Kazakhstan. [22, 23]

### D. Law Enforcement Outcome

On November 10, 2000, the two Russian cyber criminals, Vasiliiy Gorshkov and Aleksey Ivanov, were arrested in Seattle, Washington. They were tried and sentenced in two different jurisdictions in a joint prosecution involving the U.S. Attorneys Offices in New Jersey; Hartford, Connecticut; Seattle, Washington; and Los Angeles and Sacramento, California. Gorshkov, 26, was sentenced in Seattle on October 4, 2002 to three years in Federal prison. On July 24, 2003, Aleksey Ivanov, 23, was sentenced in Hartford to four years in Federal prison. [24]

### E. Victim Outcome

The costs to victims of the automated auction scam were estimated at $25 million. [21, 22, 23] The total level of effort required to prosecute these two cyber criminals is more difficult to estimate. Numerous members of the FBI and local law enforcement worked on this case over several years. The primary digital forensic expert worked on the case full time for approximately nine months, analyzing the logs and files downloaded from tech.net.ru, recreating the crime, building the courtroom case and serving as an expert witness in the courtroom. Fully burdened, a reasonable estimate for his time alone would be $100,000.

### F. Post Mortem

The Russian Hacker Case is by far more complicated than the average incident response. To extrapolate costs and hours spent on this case across the total of all incidents in any year would not make sense.

Nevertheless, it could be concluded that in this forensic investigation, like the previous one, time and money invested were significant with comparatively little in terms of results. The table below compares the cases to make this point.

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>New Zealand Hacker Case</th>
<th>Russian Hacker Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of attack</td>
<td>Typical intrusion scenario (Fig. 2)</td>
<td>Online automated auction scam</td>
</tr>
<tr>
<td>Intruders</td>
<td>Script kiddies</td>
<td>Criminal hackers</td>
</tr>
<tr>
<td>Damages</td>
<td>$400,000</td>
<td>$25 million</td>
</tr>
<tr>
<td>Investigator time</td>
<td>417 hours</td>
<td>9 months</td>
</tr>
<tr>
<td>Investigation costs</td>
<td>$27,800</td>
<td>$100,000 (partial)</td>
</tr>
<tr>
<td>Consequences</td>
<td>Community service</td>
<td>3 &amp; 4 years in Federal prison</td>
</tr>
<tr>
<td>Investigator</td>
<td>Sys admins learning forensics</td>
<td>expert recruited to work for the FBI</td>
</tr>
<tr>
<td>Network Forensic readiness</td>
<td>Reactive</td>
<td>Reactive.</td>
</tr>
</tbody>
</table>
In summary, digital forensic investigations in both cases were conducted in a reactive mode. Having examined the lengths to which network forensic investigators must go to develop evidence, the current ad hoc approaches would not be sufficiently scalable to address the significant numbers of intrusion cases needing forensic documentation that organizations may experience in the future. [18]

V. 'OPERATIONALIZING' NETWORK FORENSIC READINESS

In this context of high costs in money and time for investigating malicious online intruders, the concept of network "forensic readiness" has emerged. In 2001, practitioners such as @Stake [2] introduced the concept, defining the term as 'maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response.' [2]

In recent papers, researchers have begun to elaborate upon this definition by developing models that begin to 'operationalize' the concept of network forensic readiness. Yasinsac and Manzano have proposed six categories of policies that can enhance network forensics in enterprises [25] Wolfe-Wilson, J. and Wolfe, H.B recommend planned procedures be incorporated into existing incident response plans [26] and Carrier and Spafford describe a readiness phase that ensures support for forensically sound investigations. [27]


VI. RETHINKING COMPUTER SECURITY TO INCLUDE FORENSICS

As mentioned earlier, a network administrator's main focus is keeping the network up and running. Following an intrusion, usually not much consideration is given to preserving evidence or engaging law enforcement. These practices are seen as distracting to the restoration of service and not worth the effort, since legal redress of any kind is unlikely to be pursued, as has been discussed. [18]

The current state of network management strategies is captured in CERT's Survivability Model, which institutionalizes the hacker arms race. The model implies the inevitability of being attacked, accepting that cyber security strategies are primarily defensive in nature. A previous publication describes modifications to that model that include digital forensics and suggests that to find a way out of the escalation cycle of the arms race will require a different way of thinking. [5]

VII. DIRECTIONS FOR FUTURE WORK

Future work will continue to develop a framework and methodology for conceptualizing, designing and developing forensic ready organizational networks.

VIII. REFERENCES


[10] Endicott-Popovsky, B.E., Lectures and Assignments: CSSE591 Computer Forensics: Seattle University, Seattle, WA.


