# ZERO DAY

A NOVEL

MARK RUSSINOVICH

FOREWORD

Mark Russinovich is recognized by many as the world's leading expert on the Windows operating system. His tools are used worldwide by corporations and government agencies not only to keep their IT systems running, but to perform advanced forensics.

In this book, Mark has woven a compelling tale about an imminent threat to every person, household, corporation, and government that relies on technology and the systems that we depend on. While what Mark wrote is fiction, the risks that he writes about eerily mirror many situations that we see today. Clearly, we are more and more dependent than ever on Internet-connected computer systems: it is the way we communicate, do our banking, pay our taxes, book our travel, and buy merchandise. We take for granted that these systems will always be there and are set to protect our privacy and are secure. The strength of the Internet and Internet technologies is that we are so connected. However, this strength is also a weakness—these systems are vulnerable to attack from anywhere by anyone, and with little capital investment. The Internet also facilitates maintaining anonymity, on which many of us depend, but often creates a fertile ground for bad actors. As Mark's story unfolds, we see the hacker creating superviruses hiding behind many layers of virtual disguises, which make fixing the problem even more complicated and dangerous.

For too many years, we have heard cyber-security experts saying that we need to have more security, we need to use antivirus, we need to use anti-spyware, back up our systems, use firewalls, and be vigilant about what documents we open, links we click on, and programs we execute. These and other technologies help protect a system or small network, but do not necessarily protect the overall environment that weaves through the very fabric of the Internet, touching all of us. Mark has created a unique work that is not only entertaining but a call to action as well. This is a great read and a forward-looking picture of what we need to avoid.

I hope stories such as *Zero Day* remain just that—great reads that will hopefully never come true.

PROFESSOR HOWARD A. SCHMIDT

PRESIDENT AND CEO, INFORMATION SECURITY FORUM LTD.

WHITE HOUSE CYBER SECURITY COORDINATOR

# 000 ZERO DAY

Mark
Russinovich

FOREWORD BY
HOWARD A. SCHMIDT

**MEMORANDUM**


*NS rated 10*


**DATE:**


April 14


**FROM:**


John S. Springman


Deputy NSA, The White House


**TO:**


Roger Witherspoon


Executive Assistant Director, DHS


**RE:**


Interim Report

Following the catastrophic events late last year, Congress and the President directed the creation of a confidential Committee of Inquiry. Attached is the Interim Report of the Committee. It strikes me as a bit purple in places and speculative in others, but I accept that this is an accurate and fair rendering of the events last year. The IR has been disseminated to all involved agencies. Should there be areas you wish expanded, be certain to convey that desire to me within 10 days. Should you desire redaction of any portion, I am instructed to advise that such a request must be made in writing within the same time period, and state with specificity those sections to be deleted accompanied by a satisfactory explanation of the justification.

It is clear to me now that you were perfectly correct in your initial impression as stated at our enabling meeting. The events that led to such a cataclysmic chain of events, events I wish to add from which we are still attempting to recover, began in New York City, but only by a few minutes. They might just as easily have started over the Atlantic.

**MAJORITY OF COMPUTERS LACK SECURITY, REPORT**

By Isidro Lama

*Internet News Service*

August 10

**A report released Wednesday found that more than 80% of computers lack essential security software.**

The overwhelming majority of PCs in homes have been found to lack essential security protections, according to a report by a leading cyber-security firm. Most home computers lack either a firewall, anti-spyware protection or current antivirus software.

"Curiously, most consumers falsely believe they are protected," said a spokesperson for the Internet Security Association. "The reality is quite the opposite."

Despite modest improvements in home security since the first survey four years ago, much remains to be done. "At a time when the public turns increasingly to computers to handle finances and to house personal information, it is leaving itself exposed to exploitation," the spokesperson added.

The situation is no better with military and government computers, according to the report. "We are significantly exposed to a cyber-attack," the report concludes, "the consequences of which could exceed our imagination."

**MANHATTAN, NYC**

**SATURDAY, AUGUST 11**

**12:01 A.M.**

"Shhh!"

When the whisper came out of the darkness, the man stopped. A vast panel of glass covered the wall before him, displaying uptown Manhattan in a scene that might have been sold as a poster. Ambient light and the soft glow from a dozen computer monitors was all that spared the room total darkness. The logo of Fischerman, Platt & Cohen floated on each monitor.

In the hallway, the steps faded. A moment later her fingers touched his arm, pressing lightly against the soft skin on the inside of his wrist, her flesh much warmer than his. The thought of her so excited aroused him even more.

She tugged and he followed. "Over here," she whispered. He tried to make her out in the darkness but all he could see was her form, shapeless as a burka. They stopped and she came into his arms, on him even before he realized she'd moved. Her scent was floral, her mouth wet and also warm, tasting of peppermint and her last cigarette.

After a long moment she pulled back. He heard the whisper of clothing across nylon, the slight sound of her skirt dropping to the carpet. He sensed, more than saw, her form stretch on the couch. He unbuckled his trousers and let them drop around his ankles. He remembered his suit jacket; as he removed it, her hand touched his erection through his undershorts. She tugged them lower, then encircled him with her fingers.

Her grip guided him, and as he entered her, a single computer screen sprang to life behind the groaning couple. Turning blue, it read:

Rebooting …

After a few seconds, the screen flickered and read:

NO OPERATING SYSTEM FOUND.

The screen turned black.

**BRITISH AIRWAYS FLIGHT 188**

**NORTH ATLANTIC, 843 MILES OFF NEWFOUNDLAND**

**FRIDAY, AUGUST 11**

**12:01 A.M.**

The flight attendants were clearing breakfast in the passenger compartments as Captain Robert McIntyre scanned the dials of the PFD, the primary flight display, once again. Beside him, copilot Sean Jones sat facing dead forward in that semihypnotic posture so common to commercial pilots on extended flights.

The sound of the twin engines well behind the pilots was distant. Outside, air slipped past the airplane with a comforting hiss. The Boeing 787 Dreamliner, with 289 passengers, all but flew itself. Once the airplane reached a cruising altitude of thirty-seven-thousand feet, the pilots had little to do but monitor the instrumentation and be available should something go wrong.

The airplane could take off, fly itself, and land without human assistance. It was state-of-the-art, fly-by-wire technology, which meant the airplane had the latest in computers. The manual controls, such as the throttle and yoke, were not physically connected to anything, though they were programmed to give the feel that they were. Instead, they emitted electronic signals that moved the parts of the plane needed for control.

Computers had even designed the plane itself. So convincing was the computer construct that the airplane was approved for commercial use and had gone straight to production without a prototype. McIntyre commented from time to time that the 787 was the most beautiful and well-behaved airplane he'd ever flown. "Any plans in New York?" he asked his copilot.

Jones sat motionless for several long seconds. "Excuse me," he said finally. "Did you say something?"

"Want some coffee? I think you were off somewhere."

Jones yawned. "No, I'm all right. I get so bored, you know?"

McIntyre glanced at his wristwatch. They were still more than an hour out of New York City. "Better watch it. You'll be on record in another half hour."

The cockpit voice recorder functioned on a half-hour loop, constantly recording thirty minutes at a time, again and again. Pilots had long learned to be utterly frank only when they were not within half an hour of approach or for the first half hour after takeoff. These were the times anything unusual occurred, if at all. Once in the air, the airplane was all but unstoppable.

"I know, but thanks. 'Plans,' you asked? Nothing much. How about you?"

"Just a walk in the park, I think. I'm too old for the rest."

"Right. Tell it to your wife." Jones glanced back outside. "What's the altitude?"

"Let's see, right at thirty-seven thousand … Jesus, we're at forty-two thousand feet." McIntyre scanned the dials again as if searching for an error. The airplane had climbed so gently neither of the men had noticed. "Do you see anything on the PFD?"

"No. Looks good. We're on auto, right?" They'd been on autopilot since London. This wasn't supposed to happen. The plane had just come out of a complete servicing. All of the computer software had been reinstalled, with the latest updates. Everything should have been functioning perfectly. Instead, they were on an all but undetectable gentle incline.

"Right," McIntyre said. "I'm resetting auto.… Now." Nothing changed. After a moment he said, "Altitude is 42,400 and climbing. What do you think, Sean?"

Jones pursed his lips. "I think we've got a glitch. Shall we go manual?"

Pilots were under enormous pressure from the company never to go manual except at takeoff and on approach for landing. The computer not only flew the airplane in between but did a far superior job, increasing fuel efficiency by as much as 5 percent, a great money saver. If the pilots went manual, the flight data recorder, which kept a record of everything from preflight to postflight, would record it, and they'd have to file a report justifying their action.

"Airspeed's dropping," Jones said evenly. The autopilot was not only failing to keep the airplane at the proper altitude, but it hadn't increased power to the engines to compensate for the steady climb.

"Altitude is 42,900 and climbing," McIntyre said.

The door opened behind them and the senior flight attendant, Nancy Westmore, entered. "Are we climbing, boys? It feels odd back there."

The pilots ignored her. "Airspeed is 378 and dropping," meaning 378 kilometers per hour, well below the standard cruising speed of 945. "Altitude is 43,300 and climbing," Jones said.

"Have a seat, luv," McIntyre said. "And strap in. We're going manual." Westmore, a pretty blonde, blanched, then dropped into the jump seat and buckled up. The two had carried on an affair for the last three years.

"Bobby," Jones said, "PFD says we are approaching overspeed limit." The computer was reporting they had exceeded their normal flight speed and were approaching a critical limit.

McIntyre looked at the controls in amazement. "That's impossible! Airspeed is 197 and falling." The yoke-shaker program engaged and the stick began to rattle in front of him. In traditional airplanes, the yoke shook at stall. In the 787, the computer simulated the effect for the pilots.

At that moment the stall warning came on. "We're nearly at stall! It can't be both. Going manual … now."

A soothing woman's voice spoke. "Warning. You are about to stall. Warning. You are about to stall. Warning…"

But when the autopilot disengaged, nothing happened.

"Are you nosing down?" Jones asked, looking over, seeing for himself that McIntyre had pushed the yoke forward.

"No response," McIntyre said. "Nothing. Jesus!"

"Airspeed 156, stall. Altitude 43,750, still climbing. Holy shit!"

Then the mighty 787, cruising at over forty-three thousand feet, stalled. All 427,000 pounds of the airplane ceased to fly as the plane nosed up a final moment, then simply fell toward the blue ocean eight miles below. All three experienced a sensation of near weightlessness as the plane plunged toward the earth. Westmore closed her eyes and locked her mouth shut, vowing not to make a sound.

Behind them came a roar of passengers screaming.

As it stalled, the airplane lost its flight characteristics, which depended on forward motion through the air for control. The plane fell as an object, not as an aircraft. Without comment McIntyre pulled the yoke well back, fighting to maintain some control and keep the craft upright. Without air control, the plane could easily roll onto its back. If it did, they were lost.

Under his breath Jones said, "Hail Mary, full of grace, the Lord is with thee…" He scanned the PFD. "Airspeed 280, altitude twenty-nine thousand."

"Jesus," McIntyre said. "I've got nothing." The yoke was not giving him any feel. The plane was moving through space absent any control. "Engaging auto!"

Through the closed door came more screams. Neither pilot heard them.

Jones reached over and engaged the autopilot. Both men were trained that in an emergency, the autopilot had a superior solution to any they could come up with. They'd been shown example after example of pilots wrestling with airplanes until they crashed, doing the wrong thing over and over, when the autopilot would effortlessly have saved the craft.

"Patience. Give it time," McIntyre said as if to himself.

Another long moment passed. Nothing happened. The airplane wobbled to the right, corrected itself as it was designed to do, then wobbled to the left.

"Airspeed 495, increasing; altitude twenty-seven thousand, falling," Jones said. He resumed the Hail Mary.

"Mother of God," McIntyre muttered, "hear me. Disengaging auto. Setting throttle to idle!"

The airplane was now in a significant dive, and the crew could feel the buildup of airspeed as it rushed toward the sea. The sound from the passengers was now a steady desperate drone. The plane was well nosed forward. The horizon, which should have lay directly in front of them, was instead high above.

"Airspeed 770, altitude twenty-two thousand!" Jones's voice had risen an octave.

"Shit!" McIntyre said. "God damn you!" he shouted, cursing the airplane. "Reboot," he commanded. "Reboot the fucking computer! Hurry up."

Jones tore his eyes from the PFD. "Rebooting." They were under strict orders never to reboot in flight. This was a ground-service procedure. Jones fumbled for the switch. "Got it! Not responding, Bobby. It's not responding! It's locked!"

"Kill the power." McIntyre's face shone from sweat. "Hurry. We haven't much longer!"

Jones looked to his right, ran his hand and fingers down the display, found the master switch, and flipped it off. The PFD went black.

"Wait!" McIntyre snapped. "Give it a second. Okay. Now!"

Jones flipped the switch. "On!" There was a pause. The dials before them sprang to life.

From behind them came a steady roar of terror punctuated by loud noises, as luggage from the overhead compartments and laptops flew about, striking anything in their own flight path.

"Engaging auto!" McIntyre said. Nothing.

"It's still rebooting," Jones said. They couldn't know for certain either their airspeed or altitude, making reliable decisions impossible. "I estimate fifteen thousand with airspeed in excess of 836." They were nearly at standard cruising airspeed. "We're falling fast."

The nose was now well down as the 787 plummeted toward the earth. The air slipping across the exterior controls of the airplane had restored flight control, but the yoke still denied it to the pilots.

The sensation of falling was palpable. Behind the men now came a high-pitched howl neither could place. It was neither mechanical nor human. McIntyre glanced back, expecting the worst, and realized it was Westmore. He hadn't thought it possible for a human voice to make such a sound. "Quiet, luv," he said, trying to calm the terrified woman. "Please!" He turned to the front. "Disengaging auto!" In front of him, filling the entire windshield, was the blue expanse of ocean.

"It's rebooted now!" Jones shouted.

Without warning, the plane suddenly responded to the yoke.

"Oh, shit," Jones said, as the captain began to try to raise the nose of the plane. The dials were giving information now. "Airspeed 915, altitude eight thousand! Easy, Bobby, easy. Don't overdo it." If they managed to pull the aircraft out of the dive, the danger was that it would rocket uncontrollably into the sky, a situation nearly as deadly as the dive itself.

McIntyre pulled on the yoke steadily. His face was masked in sweat. His breath came out in short, labored puffs. The plane was pulling up in response to his command, but the horizon was still much too high, the space before them nothing but ocean.

"Airspeed 1034, altitude four thousand! Oh, God!"

McIntyre pulled back more forcibly on the yoke. They felt the g-forces as he compelled the airplane out of the dive.

"Airspeed 1107, altitude three thousand!"

"Come on, you bastard, come on." McIntyre pulled the yoke well back, all but certain one of the wings was going to come off.

"Oh shit, oh shit, oh shit!" Jones said. The g-forces pressed them heavily into their seats.

"Get up, get up, motherfucker." Behind the men, Westmore screamed again.

"Airspeed 1122! Altitude twenty-three hundred!" Jones said in a high-pitched voice, almost in falsetto.

"Climb, you bastard, climb!"

Suddenly the g-forces vanished as if an invisible hand had been lifted from them.

"We're climbing!" Jones said with a laugh. "We're climbing! Airspeed 1103, altitude twenty-six hundred!"

Flight 188 rocketed into the sky like a ballistic missile.

**MANHATTAN, NYC**

**FISCHERMAN, PLATT & COHEN**

**MONDAY, AUGUST 14**

**9:07 A.M.**

"Coffee? A Danish?" she asked with an inviting smile.

"No, thank you. I'm fine," Jeff Aiken said, considering closing his eyes until summoned for the meeting.

"Mr. Greene will with be with you any moment."

Jeff, still in a fog from his hasty trip, didn't take the time to admire what he sensed was an inviting view. The receptionist was not yet thirty, stylishly dressed, trim, obviously fit, but wearing the latest hairstyle, which made her look as if she'd just crawled out of bed and sprayed it in place.

Jeff had received the urgent call Saturday night—Sunday morning, actually—right after falling into a deep sleep, still dressed, splayed atop his bed at the Holiday Inn in Omaha, Nebraska. He'd just finished an exhausting all-night-all-day stint at National Interbank Charge Card Services. Their security system had been so porous that financial crackers, as criminally minded hackers were known, had systematically downloaded the personal accounts of more than 4 million "valued" customers. News accounts reported that the data looting had gone on for two weeks before being discovered. Jeff had tracked the information loss back more than three months and guessed it had been going on even longer.

Once he'd agreed to fly to Manhattan and negotiated a substantial fee for his time, it had taken all day Sunday to finish the security checks he'd installed on the new NICCS system. He doubted it would save the company from the ire of its violated cardholders, or federal regulators. If the company had spent a thousandth of his fee on routine security earlier, none of this would have happened. He never ceased to be amazed at the mind-set of supposedly modern executives. They still conducted business as if this were the twentieth century.

He'd arrived at the Omaha airport just in time to catch a red-eye to New York City. This would be his first trip there since the death of his fiancée, Cynthia, at the World Trade Center on 9/11, and he was almost overwhelmed by a range of unwelcome emotions. For an instant it was as if he were reliving the horror all over again. By the time he'd taken a taxi downtown, checked in and showered, he'd pushed his terrible memories aside and caught exactly ninety minutes sleep before shaving and dressing to arrive for this 9:00 a.m. meeting with Joshua Greene, managing partner of Fischerman, Platt & Cohen.

"Mr. Aiken?"

Jeff opened his eyes and realized he'd fallen asleep. He glanced at his watch: 9:23. "Yes?"

"Mr. Greene and Ms. Tabor will see you now. Are you sure you don't want some coffee?"

"Thank you. You were right. I'll take a coffee after all. Black." He smiled sheepishly. "Better make it a large."

The receptionist laughed, flashing brilliant white teeth. She showed him through the double door into the managing partner's office. "I'll get that coffee right now," she said.

The reception area had been designed in a 1920s art deco style that Jeff believed was inspired by the original interior design, given the age of the building and the exterior motif. The impression was reinforced as he entered the conference room. Dressed in brown penny loafers and wrinkled tan chinos, a dark blue travel blazer with a matching light blue polo shirt, he was accustomed to looking out of place in most corporate offices. After all, he reasoned, they hired him for what he knew and could do, not for his wardrobe. With short sandy brown hair and dark eyes, he was six feet tall and thirty-six years of age and had mostly kept his athletic build despite his work. Even catalog clothing fit him well, a girlfriend had once commented.

The pair sat at an expanse of glassy mahogany. The lawyer, Greene, was well dressed, to put it mildly, reminding Jeff of Gene Hackman in *The Firm*. That had been the mob's law firm, and Hackman had been the bad guy. The other was their IT person; she was almost, but not quite, a fellow traveler with Jeff, though her clothes had a Gap and Banana Republic look.

The well-suited man stood and introduced himself as Joshua Greene. "This is Sue Tabor, our IT manager. I thought it would save time if she sat in."

"We spoke late Saturday," Sue said as she rose to shake hands.

"Yes, I recall. Barely."

They waited as the receptionist returned with a large black coffee and a Danish Jeff had not requested. Greene waved her off before she could ask if anyone else wanted anything.

Sue was slender, of partial Asian heritage, late twenties, with jet-black hair stylishly cut in a bob. Her slender lips were a crimson slash, and she wore more makeup than he was used to seeing in offices.

Beneath her shirt he detected modest breasts, but her figure struck him as all angles. Her grip was firm, but there was no denying a certain shine in her eye as she met his gaze.

Greene was perhaps sixty years old and had the look of a man who spent his share of time in the gym. Broad-shouldered, he had graying hair and wore glasses with scarcely any rim, the lenses reflecting as if made of crystal. If someone told that Jeff Greene had once played football, it would have come as no surprise. While Sue was clearly West Coast in her accent, Greene came from somewhere in the Midwest. Jeff had heard a lot of that Johnny Carson talk in Omaha.

"I don't want to waste your time, Aiken," the lawyer said, "but I'd like to give you a brief summary before I hand you over to Sue. Saturday morning one of our associates came in earlier than usual and found himself the first in the office. When he attempted to use his computer, he could not. He checked with other computers and discovered that *none* of them were working. Sue was summoned and … I'll let her handle that part."

Greene cleared his throat. "I just want you to understand how critical this is. We billed more than ninety million dollars last year. We're not a large firm, obviously, but we are highly respected in our field. According to Sue, we cannot access our computer system. This includes our litigation records, both current as well as archived, e-mail, and our billing records. She also suspects that everything may be lost, or lost in part. She tells me that until we identify the source of the problem, we cannot even access our backup records to determine if they've been contaminated."

Greene gave Jeff a withering look that suggested he was at fault for the situation. "In short, we are dead in the water. Our cash flow has been stopped; our attorneys are unable to adequately work on existing cases. Once clients start figuring this out, those in a position to will defect, the others will sue. We need everything back, as soon as possible. The situation is critical."

Sue spoke, eyeing Jeff steadily. "The server is unbootable. I couldn't access the system at all."

That was odd, Jeff thought. In most cases, an infected computer would still boot, even if it didn't properly operate thereafter. "What are you able to do as an office?" Jeff asked.

"The attorneys are working on e-mail through our Internet provider's backup system," she said. "Many had current files in their laptops and are using those. I've not touched our backups since I have no idea what I'm dealing with here."

"How do you handle those?" Jeff asked.

"We have nightly backups of each computer to an in-house master server. Once a week, we make backup tapes that are stored in a fireproof safe. Once a *month,* we make a second set of backup tapes, and those are stored in another safe, off-site."

"Good. We'll have something to work with. How much can you tell me about what happened?"

"Sorry to say, almost nothing. The system simply isn't accessible. Not to me, at least." Sue grimaced.

Greene spoke. "Working without computers is a real problem for us. The younger attorneys simply don't know how to do without them; they've always had access to the various legal databases and resources. I had no idea we'd become so dependent on them." He glanced at Sue, then back to Jeff. "And obviously, being denied access to our work product is a serious problem—one that will prove very costly if you fail to fix this in a timely manner. Serious enough to put us out of business, in fact.

"But my most immediate concern is the prospect of losing our recent billing records. The longer we are down, the worse this is going to get. The system was automated. Now our attorneys are using pen and paper. We need to have our automated program up and running, and we need those billing records. They are vital. As is the case with any company, our income stream is essential."

Jeff took a long pull of coffee. It was hot and bitter. "Have you considered that your staff may have the virus in their laptops, since they were connecting to their office computers?"

Sue nodded. "I thought of that. Over the weekend I warned them not to boot, but I was too late. Some had already turned on their computers, but they had no problems. I've been running virus scans and system checks on their computers and found nothing other than the usual. Fortunately, so far whatever struck us is limited to our main system. Or seems to be." She smiled wanly.

"Do you have any idea what it is?" Jeff asked.

"None, but that's not really my area. Our firewall is excellent and up-to-date. We run antivirus software and keep it current. When I say 'up-to-date,' I mean daily. I have an assistant whose first job every morning is updating everything, seeing to the patches and running system security scans. He does that before he does anything else, and he comes to work ahead of most of the associates. So you can appreciate that I'm mystified how this could happen, because it should not have."

"That sounds good. And you're right: your measures should have been enough." Faced with the fresh challenge, Jeff felt himself growing suddenly alert and energized. This was very different from the work he'd just been doing, and any solution was going to be demanding, exactly the kind of problem in which he could lose himself.

Greene interrupted Jeff's thoughts. "I've got a meeting with the other partners and need to give them something. How long, Aiken? How long will this take, and how much of our information can we get back?"

"I can't say, in all honesty. Not at this point. I'll let you know as soon as I can make an assessment."

"All right," Greene said grimly. "I'm told you're the best. I need you to prove it."

**DETROIT, MICHIGAN**


**MONDAY, AUGUST 14**


**9:21 A.M.**


Buddy Morgan, balding, fifty-three years old, overweight, returned from his coffee break four minutes early. A twenty-three-year veteran of the United Auto Workers, he had the right to select his own shift; that's why he was working now. The supervisor, a longtime drinking companion, didn't give him any grief while the new robots did what they were programmed to do.

Not like the old days, not at all. Buddy had served his time on an air gun, the last eight years of it driving three nuts home to partially mount the right front wheel of the Ford Taurus. God, how he'd hated those never-ending days.

But that was behind him. Now he had seniority. As he told his wife, June, he was nothing more than a grease monkey. The robots did all the work. His job was to make sure they stayed online.

It was a helluva system, he had to admit. His domain was fourteen of the robots, "turkeys" as he called them. Each consisted of a massive arm mounted on a squat pedestal. At the working end of the arm was the "head," complete with a "beak." This was the part that did the welding, fast, accurate, untiring. The whole "gaggle"—he was unaware that the proper word was *rafter*—was run by the master computer. He monitored a dummy terminal at his workstation, but had no control of the system. That was work for the college boys.

Buddy spent most of his shift at his station, glancing at the monitor, then up at the slow-moving assembly line, then at his turkeys, nodding and twisting in their odd dance. The area around the workstation was filled with the smell of electronic welding and a not unpleasant sweet aroma of fine oil that came from the robots. His nearest coworker was a hundred feet away, and that was just fine with Buddy. Most UAW brothers were a pain in the ass.

Buddy's job was simple enough. He walked behind the turkeys and checked the moving parts for signs of a problem. This rarely happened. Japanese-designed, the things were built in Korea and could really take it, he often said. On a regular schedule, he pulled one off-line for examination. Not pulled, exactly; he pressed a large blue plastic button that caused the robot to retreat from the assembly line five feet. There he lubricated certain points, in all just six; then he wiped the entire machine down,

though that really wasn't his job, but he liked his turkeys looking good; then he pressed the blue button again, and the docile thing slid back in place.

The amazing part was that the other turkeys knew one of them was missing—something to do with the programming—and they simply assumed the job of the one he took off-line. Amazing. Really amazing. If you didn't get laid off, this automation thing was a wonder.

At first he'd been surprised such high-tech turkeys required manual oiling at all. He'd figured they'd designed that into them. His trainers explained that they had originally been self-oiling, but factory managers, in an excess of cost-mindedness, had put the robots on the floor without adequate supervision. There had been some real problems. They might be twenty-first-century marvels, but a certain number of turkeys required the presence of a human. The solution had been to design them so they had to be serviced regularly.

But for the most part, his fourteen turkeys worked untended and to perfection. They were completely silent, as far as he could tell. The only sound came when they zapped the frame of the SUV moving along its two rails, like a subway car crawling along.

Today, however, Number Eight was giving him fits. He'd pulled it off-line three times already, and his boss, Eddie, told him to quit messing with it. Take it off-line for good and let the techs fix it. The other turkeys could take up the slack for a few hours.

That struck Buddy as pretty sloppy. He would never have told anyone, not even June, but he loved sitting at his station, that monitor frozen in place telling him everything was as it should be, the turkeys, nodding and straightening, twisting this way and that, as they welded the frame of Ford's new SUV, the first of the really big hybrids. He just loved it.

But Eddie had a point. Sometimes even a turkey acted up. They could work forever, but not without some maintenance. Buddy reached Number Eight and lowered his hand to press the button. Unseen behind him, the dummy monitor at his workstation flickered. The screen reset.

Along the line, the turkeys stopped in place. Then, like soldiers in close-order drill, they pulled themselves back as if standing to attention. Buddy stopped what he was doing and gawked. He'd never seen anything like this. The assembly line was still moving, but the turkeys weren't zapping the frames. He stepped forward to take a better look.

At that moment, all fourteen turkeys spun in place in a violent, dizzying circle. Number Eight struck Buddy with its beak, sending him flying onto the assembly line, landing with a loud grunt, sprawling across the tracks.

Stunned, he couldn't move for several vital seconds. Just as he grasped where he was, the frame of a new Monument SUV moved across his neck.

**MANHATTAN, NYC**

**IT CENTER**

**FISCHERMAN, PLATT & COHEN**

**MONDAY, AUGUST 14**

**9:32 A.M.**

After Greene left the conference room, Sue Tabor led Jeff to the IT room, moving with a catlike grace. "Don't let his manner bother you," she said. "Josh is a good guy—for a lawyer, I mean—but his neck's on the line over this. If we don't recover enough data to save his hide, he'll be forced into retirement and I may be out of a job."

"I doubt that it was your fault," Jeff reassured her. "I'm seeing more and more of this sort of thing. Malware is more easily finding ways into once secure computer systems. Viruses of all kinds are simply getting more sophisticated."

Sue sighed. "I warned him last year not to go all electronic. He didn't listen. We had a small accounting department then, run by a blue-haired lady who was the firm's first hire forty years ago. Though everything was on computers, she insisted on running billing-record hard copies every night. Greene thought the size of her department was a needless expense, and so was all that paper. She was retired, her department was reduced to two, and no more hard copies. I warned him."

"There's nothing worse than being right when your boss is wrong."

Sue looked at Jeff sideways, with a sly smile, and that shine in her eyes. "Sounds like you've been there."

Jeff closed his eyes for a moment and drew a deep breath before turning back to Sue. "It shows, huh? What did you see when you tried to boot? Exactly."

"Like I told you Saturday night, I couldn't get into the system and decided immediately not to waste any more time trying. I'm really just a systems manager." Sue shrugged apologetically. "My primary job is to keep everything running smoothly and make certain there are no hiccups. Security is part of it, of course, but it's limited to updated antivirus software, patching, and a firewall. Our primary problems have been viruses associates bring in from home on their laptops, or employees opening attachments from spam. Nothing I couldn't handle until now. To my knowledge, nothing ever made it into the servers."

"Have you contacted the firm's bank?" She shook her head. "You need to," Jeff advised. "You should shut down Internet access to your account until this is solved. It's possible that's what this was all about. We can't know how much information they extracted before the system froze."

"I'm on it," she said, her cell phone already out. Near the ladies' room he watched her speak intensely; then put the phone away and go through the door. As he waited, Jeff geared himself up for what he had to do. A few minutes later Sue returned, makeup freshly applied, her lips repainted that bright crimson. "Thanks," she said. "I should have thought of that on my own. They're taking care of it right now."

"There's more." Jeff was never comfortable with this aspect of his job. He hated being the bearer of bad news. "I'm sorry to say that you're going to have to unplug all the servers and every computer from the network. We have to assume they're infected, even though you've detected nothing—which would mean that at this point they're serving as a breeding ground, propagating the worm. That means your lawyers will lose their e-mail."

Sue moaned. "Let me show you to your workstation, then I'll take care of it."

The IT Center was located in an undesirable area of the building. Windowless, with monitors, computers, and cables running helter-skelter, a dry static sensation in the still air, it was a copy of hundreds of other such offices Jeff had seen. Sue introduced him to her assistant, Harold, a short, nerdy young man wearing a Yankees baseball cap with the brim backward. He was playing a video game on what looked like a personal laptop. As they entered, he hurriedly put it away.

"What are you playing?" Jeff asked. His secret vice was action video games.

"Uh, *Mega Destructor III.*"

Jeff nodded approvingly. "I've got *MD IV* in beta. I'll burn you a copy."

The young man grinned.

Sue shook her head. "Boys."

Jeff grinned. "What can I say?"

Standing with one hand on her hip, Sue explained the system, gesturing with her free hand. "Every lawyer has a desktop PC and a laptop. This is the server room with four blade servers. We use

one as our Web server, another as a backup domain controller, and so on. The primary one, with our litigation records and accounting, is the one that's down. We run a standard networking program, Active Directory, and are connected to the office PCs." What she described appeared identical to other systems on which Jeff had worked. In theory that should make this job a bit easier than it initially sounded, he thought. But in reality? Jeff was too experienced ever to expect a free ride.

"All right. I'll get started," he said, looking for a place to set up. "Which one should I use?" Sue pointed as he reached down and opened his work bag, extracting a black CD case filled with a wide range of disks, which he referred to as his Swiss army knife. As he began, Sue left to inform everyone they were now off-line for the duration, at least at the office. Harold moved a chair over so he could watch what Jeff was doing.

"It's good to get some action," Harold said with a smile. "I'm pretty bored playing games."

"Glad to have you. I'm going to need your help if we're to get this fixed." Jeff's CD included the standard diagnostic and recovery tools used by everyone in his profession, but he'd added a collection of utilities he'd picked up over time. This was the disk that would allow him to boot and provide a minimal environment from which he could work, since the computer was no longer making one available.

As he slid the disk into the server's optical drive, his first thought was that whatever had occurred here was caused by any one of the thousands of new variants of existing viruses that appeared routinely, as many as fifty a month. He hoped that it was a new version of an existing virus, set loose by some student hacker looking for bragging rights. Something like that could have crept under Sue's radar. Even in that eventuality it could still be a difficult job, but one he could manage. There'd likely be full, or nearly full, recovery because the data the company needed would still be somewhere in the server.

But once his own operating system was running, the first thing Jeff noted was that he couldn't detect *any* data on the hard disk. It was as if the disk had never had an operating system installed. Even the standard *C:* drive icon was missing. He'd never seen this before and he experienced a sudden chill. *How can this be?* he thought. This wasn't going to be routine after all, he realized, feeling both exhilarated and apprehensive.

Sitting down at her computer beside him, Sue frowned and said, "Call me Miss Unpopular. They act as if I put the damn virus in myself." She looked at his screen. "Getting anything?"

Jeff told her what he'd done and seen so far.

"I need me one of those nifty boot CDs you've got."

Jeff smiled, suddenly looking twelve years old. "You'll have to kill me to get it." The CD was the result of thousands of hours of hard work, and in many cases it was what made his success on a job possible. He'd once joked he planned to be buried with it. "What will you work on?" he asked her.

Sue pursed her lips. "I'm going to spin my wheels, probably—analyzing the firewall and proxy server logs, if that makes sense to you." Jeff nodded. That area had to be covered, and it would save time if she did it. "Maybe I'll stumble onto something useful. This is *not* my field at all."

"You might get lucky," Jeff encouraged her. As Sue set to work, he ran a salvaging tool that could make guesses and ignore what would otherwise look like errors. With this he had more success, since it was able to provide him a view of files and folders previously not visible.

Now able to scan through what was left of the disk's data, Jeff searched for the files that contained the core configuration of the system. What he found instead were bits and pieces of the original operating system and temporary copies of portions of program data. Though he was disappointed, he was still able to reconstruct a portion of the file system and registry with its database, which stored settings and various options for the computer's operating system. *At least it's a start,* he thought.

Next he skimmed through the corrupted registry entries. It was a bit like scanning the television guide to see what was on, rather than watching an evening of programs. He found that part of the data was overwritten, a standard means of destruction. Random symbols had been written over the existing data, making it difficult, sometimes impossible, to recover the original data. Peculiarly, though, only a portion of the original data had been overwritten. If that had been the purpose of the virus, Jeff thought, the job was incomplete.

Several explanations were possible. The most obvious was the presence of a destructive virus that had its overwriting operation aborted by a bug in the virus itself. The virus might have triggered behavior that resulted in the operating system's becoming corrupted, which had then stopped the virus and the overwriting dead in its tracks. Not very sophisticated, if that was what had happened.

A truly effective virus would never kill the driver or operating system that served as its host. That would be like a disease killing someone before it could infect anyone else. The most effective viruses were those that existed on computers with the operators never knowing any better. Before the operating system was destroyed, such a worm would be seeking to replicate and spread itself, though slowly, so as to escape detection. But in this case some part of it had nuked the system, in effect committing suicide.

Now Jeff scanned the corrupted registry file settings. Malware commonly created entries so that the operating system activated them each time the computer was turned on, or whenever a user logged in. He examined every entry that looked even remotely suspicious. When he located a reference to a program or piece of code he didn't recognize, he found the code's file and examined it further, looking to see if the file provided the product it was associated with and the company that wrote it, since malware typically lacked such information.

Then he performed Web searches to find information about the file's purpose, to see if anybody had previously flagged it as malware. Tedious and time-consuming, this formed the heart of what he did each day at work when on jobs like this. That initial flash of excitement he'd experienced waned as

exhaustion began to overtake him again. Working while exhausted was typical, though. In these situations, time counted for everything. Yet so far, nothing.

Two hours later, Jeff finally got a break when he came upon a reference to a device driver that appeared suspicious. Device drivers were programs that allowed other programs to interact with a bit of hardware, such as a printer, and were attractive to malware authors because they could be leveraged to create spyware, viruses, and adware that hid from standard security protections. Most home PCs had some form of these types of malware without the owner even knowing it.

All device drivers had information that included the path to the file on the disk that contained the driver's code, so Jeff was able to locate the driver image in question without any trouble. One, ipsecnat.sys, had a name that looked similar to that of a legitimate and standard driver, but he didn't recognize it. When he examined it, the file's version information reported itself as being from Microsoft, but a Web search turned up no hits on a driver by that name. *Score one for my team,* he thought.

Reinvigorated, Jeff loaded the driver into a code analyzer that allowed him to see a human-readable version of the instructions that the computer executed. Analyzing malware at this level was a big part of his job, so he could run through the instructions in his head the same way the computer would. This way he was able to understand its overall purpose.

He read:

.text:00000000007B35D8 xor [rcx + 30h], rdx

.text:00000000007B35DC xor [rcx + 38h], rdx

.text:00000000007B35E0 xor [rcx + 40h], rdx

.text:00000000007B35E4 xor [rcx + 48h], rdx

.text:00000000007B35E8 xor [rcx], edx

.text:00000000007B35EA mov rax, rdx

.text:00000000007B35ED mov rdx, rcx

```
.text:00000000007B35F0 mov ecx, [rdx + 4Ch]


.text:00000000007B35F3 loc_7B35F3:


.text:00000000007B35F3 xor [rdx + rcx*8 + 48h], rax


.text:00000000007B35F8 ror rax, cl


.text:00000000007B35FB loop loc_7B35F3


.text:00000000007B35FD mov eax, [rdx + 190h]


.text:00000000007B3603 add rax, rdx


.text:00000000007B3606 jmp rax
```

When he finished, Jeff was thoroughly alert. The code was obviously encrypted. Viruses often encrypted themselves to make it time-consuming, or even impossible, for virus scanners to unravel the core code. The malware decrypted itself into memory when launched, which could take up to several seconds because of the levels and complexity of the encryption scheme employed. That was why a slowly booting computer was often a sign of infection.

The next three hours flew by as Jeff tried to match the encryption algorithm used by the hacker against those commonly employed by malware authors. Finally, he decided that he was looking at something new. This part of his work was like a puzzle to him, one in which he pitted his own creativity and determination against that of the hacker. In its own way it was not so different from the most difficult computer games he played except that real stakes were involved here. Knowing that kept Jeff's excitement tamped down, though he couldn't resist a mental pat on the back before continuing.

As a precaution, he set up what was essentially a "virtual" computer that allowed him to examine the virus in operation, but at a much slower pace. The virtual computer behaved exactly like a real one and, to the user, looked like the screen of a real computer displayed in a window on their desktop. But the virtual computer gave Jeff great control over the process since he was able to control execution of the malware, starting and stopping it as needed. In this way, he hoped to be able to unravel the code.

Next he dropped the code onto the disk as an unencrypted copy of the driver. Completely consumed, he lost all touch with day and night. Even Sue didn't exist as a person. She vanished from his world, though she sat next to him. He was neither thirsty nor hungry. He felt no discomfort in his body.

It often seemed to him, during a job like this, that he'd been born for this work, such was his capacity to shut out everything else. For him a computer problem was like solving a brain teaser, and he loved games. He also hated being defeated. The real world could be chaotic and violent and frequently felt, at least to him, to be out of his control. But with work he could understand a computer, even the viruses that attacked them. Success here was clearly defined: when he was finished, the computer either worked or it didn't.

Right now his only world was the one on the screens before him.

**DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.**

**DIVISION OF COUNTER CYBERTERRORISM**

**MONDAY, AUGUST 14**

**9:51 A.M.**

"I don't get the connection," George Carlton said as he leaned back in his chair, eyeing with cautious pleasure the woman seated before him.

Dr. Daryl Haugen, dressed casually in jeans and a snug blouse, paused before responding. Slender and just over average height, with a fair complexion and blond, shoulder-length hair, she was stunningly attractive. The way Carlton eyed her while pretending he was not was a reaction she'd grown accustomed to as a teenager. A computer science graduate of MIT and thirty-five years old that July, she'd worked hard to be taken for what she was, much more than a pretty bauble on a man's arm. Men such as Carlton, who acted as though they took her seriously when all they really were interested in was her butt, rubbed her the wrong way. But what she had to get across to him was too important for her to waste time getting angry over his juvenile chauvinism.

"We've come up with eight incidents so far," she said, leaning forward to emphasize her point. "The most deadly was at a hospital in New York City. The computer glitch there appears to have caused four deaths from misapplied medications. There are similar reports out of several hospitals in other boroughs."

"What about these other incidents?" Carlton leafed through the papers as if searching for something specific, then stopped in apparent frustration. "I've read your report. Frankly, I don't see a connection between any of them, and I certainly don't see a national security issue. As you know, during my tenure here we've made significant strides in combating computer viruses, especially when they target government or military computers."

Daryl sighed to herself. *Not that again,* she thought. "I can't be certain, but it looks like more than one virus. It's odd, striking like this in so many seemingly unrelated places, and being so deadly." She wrinkled her brow. "The viruses were also in systems that should have excluded them. We need to understand quickly why they didn't. We have no idea how many of them are out there, or how they

spread. If they're commonly on the Internet—and this assumes we're dealing with more than one and not a single virus with different manifestations—they're going to cause a lot of trouble, not just in home and business computers but in government and military ones as well."

"Well, that's good," Carlton said.

"Excuse me?"

"I mean that they are going after computers in which my department has a direct concern," he said hastily. "Not that the viruses are good as such."

Daryl bit her tongue. She needed this fool's help.

"I'm saying that's the kind of thing we are so effective at interdicting," Carlton added, dragging his eyes away from her chest. He'd first met Daryl when she'd worked at the National Security Agency in 2000. She'd been assigned to liaison with his Cyberterrorism–Computer Forensics Department at the CIA. She'd been unexpectedly forthcoming, even providing some source data they'd lacked, which proved quite accurate. But the best part of the arrangement had been her drop-dead looks. He'd suggested drinks more than once, but got nowhere. Neither had anyone else in the department.

He'd been more than pleased when he learned that she'd left NSA and was now assistant deputy executive director CISU (Computer Infrastructure Security Unit)/DHS and head of a team at US-CERT (Computer Emergency Readiness Team), which technically reported to him at DHS, where he was now chief of counter cyberterrorism. US-CERT was expected to operate independently, alerting him only when they came upon an issue of national security. This was the first time she'd ever asked to work in the field. He doubted he even had the authority to refuse, but he was damned if he was going to acknowledge any limits to his power.

"Aren't the hospitals cooperating?" he asked, squaring his shoulders to look more forceful.

"Sure," Daryl confirmed. "But I don't know what they're holding back, thinking it's not important. The virus or viruses will have left tracks. I can't trust others to find them. That's not what they do. They just want to get their systems functioning. We need to educate ourselves quickly. The protections at one of these infected hospitals were much better than those of, say, nuclear power plants." She met his eye to see if she was making her point. "We need to know, George. We can't sit on this."

For a moment Carlton wondered what she knew, and if that was meant to be a veiled threat. "Well, of course you should go. Thanks for keeping me in the loop. Keep me posted."

He watched her retreating figure with more than a little regret and sighed. These computer types were always getting worked up over nothing. The few attractive women among them were the worst.

**KELLOGG, IOWA**

**SKUNK RIVER NUCLEAR GENERATING STATION**

**MONDAY, AUGUST 14**

**11:43 A.M.**

Barnett Favor scanned the computer screens with a practiced eye, then leaned back in his chair. He'd begun his shift at six that morning and had just finished lunch. On most days he "assumed the position," as he jokingly called it—closed his eyes and took a catnap. Either of the other two men on the shift, or the computers themselves, would alert him if he was needed. Favor crossed his hands comfortably on his stomach and closed his eyes.

The Skunk River Nuclear Generating Station was a General Electric boiling-water reactor, located on the Skunk River some forty miles east of Des Moines. It provided nearly half of the electricity of the city, while the rest of its output was distributed throughout the eastern rural stretch of the state and into western Illinois. One of the last nuclear power plants completed in the United States, it had undergone an extensive overhaul in 2005 and was now entirely modern.

In the years since the disaster at Three Mile Island, when multiple human errors had caused a partial core meltdown, enhanced reliance had been placed on computers to handle the complex decision-making necessary if something went wrong. As a result, Favor and his team had almost nothing to do with the plant operation.

Since the overhaul the station had run without incident, not that there had been many in the previous two decades of its operation. Favor had been with the company since high school and was just two years from retirement. He'd cut his teeth on an old coal-fired generating plant, discontinued when the Skunk River Nuclear Generating Plant had come on line. In the early days the operation of the two hadn't been all that different. Water was still heated and turned into steam, which ran turbines, which produced electricity. The only real difference was how that water was heated.

After several minutes Favor shifted in his seat, then accepted that he wasn't going to nod off. Instead, he decided to get himself a Coke. If he couldn't take a nap, he'd take in a bit of caffeine.

The control room of the plant looked like something out of *Star Trek*. A long, curved wall contained a wide range of gauges and dials. At waist level was a shelf the workers used for a desk. Immediately in front of them was a bank of computer screens that told the story. The men used three chairs on wheels to scoot across the floor and along the wall as they monitored the conditions of the plant. In reality, they had little to do.

Just as Favor stepped from the soft-drink machine, every computer screen in the room blinked, twice. "What was that?" he said.

Orin Whistle, who'd worked there nearly as long, looked up from the paperback he'd been reading, a blank expression on his face. "What happened?"

Josh Arnold stood up in place as if he might suddenly need to run. "Something's going on, Barney."

At that moment Favor could feel the change. The plant was tens of thousands of moving parts, each performing its specific function. The mix produced a familiar vibration and comforting background hum that changed only when one of the two reactors was taken off-line for maintenance. Otherwise, nothing ever changed.

"The turbines are speeding up," Whistle said as if to himself. "I'm resetting the control." He looked at the gauges, the amber lights playing across his face. "No change."

"Heat's up, Barney," Arnold said, touching the temperature gauge in front of him as if to confirm what his eyes told him. "I don't see why, though."

The twin nuclear piles were set to run at their standard temperature, allowing the water coursing through them to be superheated to produce the steam that created electricity. A second stream of water ran through the system like coolant from the radiator of an automobile, intended to maintain the core at exactly the right temperature. It was all self-monitoring and self-adjusting. Until this moment, Favor had considered it impossible for the reactor to increase in heat without his ordering the computer to make the change.

"Watch the pressure," Favor said. Pressure was key to being certain the nuclear core was always covered with water. The crew at Three Mile Island had notoriously failed to ensure that single necessity and, as a result, had brought disgrace on themselves and an end to new nuclear plants in the United States.

"Pressure's up," Whistle said, his face paling. "And it's rising fast."

The Klaxon sounded, repeating every three seconds. Atop the curved wall, red lights began to blink. The computer had taken them to Code Red.

"Shut it down!" Barney shouted. "Josh, call Central Iowa and inform them we're going off-line now!"

"Jesus, Barney, they'll raise hell. Half of Des Moines will go dark."

"Do it, Orin, shut it down now!"

Orin hesitated. "We've got a few minutes to figure this out, Barney. There'll be hell to pay if we act too fast."

"We aren't going to figure this out." Favor knew there was no point in delay. Trying to outthink a computer, even one making a mistake if that proved the case, was foolhardy. "The computers run things now. Tell them we're shutting the reactors down now!"

Orin typed commands on his keyboard and punched the ENTER button.

"Didn't you hear me?" Favor asked when nothing changed.

"Sure thing, Barney," said Orin, his eyes frantically scanning the gauges. "But there's no response."

Josh cupped his hand over the mouth of the telephone. "Central Iowa wants to know why they aren't getting the standard three-hour notice so they can pull juice from elsewhere."

"Tell them we'll call back," Favor said. "Orin, give it the command again. Josh, check the temperature. And turn off the damn Klaxon and lights!"

Favor had moved so he could monitor the key indicators, his soft drink unopened and unnoticed in his hand. The noise stopped and the red lights were extinguished. Several workers from other sections had filed into the room, but they stood well back, watching nervously.

"The temperature's spiking, Barney. I've never seen it this high," Josh said. "The turbines are screaming."

The men heard a high-pitched whistle. "What's that?" Orin said, his face now chalk white.

"Oh, shit," Favor muttered. "We're venting coolant. The water's turned to steam. Orin, shut the fucker off!"

"I've given it the command four times, Barney. Nothing's happening! Don't blame me."

Though a nuclear reactor is complicated, in one aspect it's quite simple. Left alone, uranium runs into an uncontrolled chain reaction. But it's not left alone. Control rods are inserted in a regular pattern through it. They absorb neutrons and have the power to turn the core cold. The plant is heated simply by raising the rods. All that is necessary to regulate heat, or shut the plant down, for that matter, is to lower the rods.

But the computers were refusing to do just that.

Favor flashed back to a key meeting held during the overhaul. The systems analyst who'd installed the computers and multiple backups had just explained to the company's operations director and his deputy that nothing could go wrong. "This system is utterly foolproof."

The deputy had learned forward and said, "Nothing's foolproof. We're dealing with a nuclear power plant. What if all your fancy systems go wrong?"

"That can't happen, sir. Not if you follow directions and update the software."

"Of course it can happen. Where's the fail-safe?"

"I don't understand." The systems analyst had looked genuinely perplexed.

"If it all goes to hell and we're facing a meltdown and don't want those boys to be stuck telling some computer what to do, how do we pull the plug ourselves?"

"I assure you—"

"There isn't one, in other words," the deputy said to his boss. "They want us to trust the computers to do it." He fixed his gaze on the analyst. "We need a mechanical switch to crash this plant, if it comes to that."

The director had agreed, and at a cost in excess of $1 million, a fail-safe had been installed. Both the director and his deputy had been forced out the following year for spending too much money on the overhaul, but the safety system had remained in place.

"Josh, Orin, come with me," Barney said now, before running to the far wall and two large red handles, much like those of a fire alarm. Above them was written MECHANICAL SHUTDOWN. USE ONLY IN AN EMERGENCY.

"Josh, yank that one." Barney grabbed the first and pulled. The handle refused to budge. Josh tried his, with the same result. "Orin, give me a hand," Barney shouted. The Klaxon and the pulsating red lights resumed. Some of the workers who'd been watching bolted from the room, making their way to exits.

"We're in overload, Barney," Orin shouted as he wrapped his hand around half of the lever while Favor took the other. "On three. One, two, three!" The men pulled. Slowly, the handle moved. It stopped some five inches out. Applying leverage to it, they forced the red handle fully down.

Favor turned to the other. Josh had managed to move the switch an inch from the wall. All three men grabbed a piece of it and pulled. Slowly the handle moved until it too was in the down position. The men stood silently, panting, waiting.

The fail-safe was a direct cable to the control rods. The levers severed the cable holding them aloft. In theory, the control rods would drop into the core by gravity, shutting down the reactors.

"Do you think it worked?" Orin asked in a near whisper.

"I hope to God it did, Orin. I sure hope it did."

Josh glanced nervously toward the door. "Maybe we should get out of here, just in case." Nodding their agreement, the others followed.

At the door, Favor turned back and looked at the elaborate control panel one more time. *How could this happen?* He wiped his bare hand across his face, which was drenched with sweat. A thought chilled him to the bone. *What if the thing isn't dead? What if it is just playing possum?*

Favor turned and walked away. Within a few feet, he was running.

**BROOKLYN, NEW YORK**

**MERCY HOSPITAL**

**MONDAY, AUGUST 14**

**5:09 P.M.**

At Brooklyn's Mercy Hospital, the fourth hospital Daryl Haugen had visited in the city since arriving early that afternoon, she presented her US-CERT credential to the IT manager. "How many now?" she asked once he'd closed the door to his office.

Willy Winfield was perhaps thirty-five years old, balding, with thick glasses. He understood the question at once. "Still four, so far. We've taken all the patients off the computers and are handling medication manually, as we used to."

"Have you figured out yet what happened?"

"Our medication software was scrambled." Winfield's tone was matter-of-fact, but Daryl could hear the heartache behind it. "Patients were given medicines and dosages unrelated to their needs. It's been a disaster and put us at considerable risk from lawsuits. My people are working on it, but we can use all the help we can get. Would you care to see?"

"Yes, I would. That's why I'm here." This was one reason why she'd insisted on getting into the field. Whatever this was, it had already shown itself to be deadly, and she needed to be on the ground to understand its true scope and impact.

They walked along hallways with confusing turns. Modern hospitals had been expanding so rapidly there was often little logic to their layout. Winfield steered right, then right again, then left three times. Some of the hallways turned off at less than right angles. Within a few turns, she was hopelessly lost.

At last he said, "Here." Winfield took her into ICU, where a young girl lay fighting for her life. She looked perhaps eight years old. The number of wires running from her body were distressing, as was the steady beep of the monitor. A nurse hovered beside the girl poised for immediate action. Daryl was

anything but sentimental. As she gazed at the inert form of the helpless child, though, the objective software engineer threatened to give way to the woman who adored children and was devastated to see one in such condition. Pulling herself together, she asked, "What happened?"

"Her medication was mixed, like the others. Her heart stopped—for an undetermined period of time, since she wasn't on a monitor. There was no need…" The man was near tears.

Not far away a young couple watched the girl through a large window. Seeing where Daryl looked, Winfield said, "Her parents. Very nice people."

"What's going to happen?"

"We're waiting for her signs to improve before we take her off the ventilator." He touched Daryl's sleeve and gently led her away. "The doctor believes she suffered severe brain damage. She's young and strong. He's hoping she'll recover, but it's not looking good. I wanted you to see the human toll this has taken."

Daryl nodded. "I see it. I'd like to look at your system, if I could, and talk with your IT people." She forced herself to remain steady. She'd need a clear head to unravel this disaster.

"Of course." As they walked back through hallways toward the computer room, Winfield asked, "Why would anyone do something like this?"

"I have no idea."

**MOSCOW, RUSSIAN FEDERATION**


**DMITROSVSKY ADMINISTRATIVE DISTRICT**


**MONDAY, AUGUST 14**


**11:07 P.M.**


A cold drizzle streaked the cracked window. It was already fall in Moscow. It seemed to Vladimir Koskov as if summer had been the briefest illusion. He reached out and pressed the aging tape back against the pane, but it rolled away almost immediately. He could feel the cold air leaching through the glass onto his hand.

Vladimir sighed, then picked up the butt of his unfiltered Turkish cigarette and used it to light another. He inhaled deeply, then coughed as he jabbed out the old cigarette and laid the fresh one on the edge of the ashtray.

The small apartment was typical of those built during Soviet days. Of shoddy construction, rushed to completion to meet an arbitrary deadline, it was small, less than five hundred square feet, one room with a cramped kitchenette in one corner, and a bathroom with a shower. The tiny kitchen table, with room for just two, the bed, and his computers all but filled the remaining space. A path was kept clear to his workstation, with three keyboards for three computers he'd built himself and which he never turned off. He could roll his wheelchair to the refrigerator, and to the doorway of the bathroom to empty his bladder sack if Ivana was at work or shopping.

This was twenty-nine-year-old Vladimir's world. At one time the confinement, the limits of his physical existence, had nearly driven him insane. On the brink of life-ending despair he'd discovered a universe, one he could access without ever leaving this room. His portals were there on the desk and at his keyboards, on his screens, where he was the same as everyone else. It was liberating. Empowering. He had thought at one time to be an engineer, but his sudden awakening as a cripple had forced on him a fresh evaluation of life expectations. Instead, he'd taken his computer skills and morphed them into a kind of expertise that had saved him.

The new Russia was brimming with opportunity, but few ways to make any money if you were not a prostitute, mobster, or drug dealer. If it had not been for Ivana, none of this would have been

possible. She'd worked one job after another, never complaining. Sometimes he found her endless self-sacrifice to be all but unbearable.

Vladimir tapped the keys and returned to the Web site he'd been browsing. He spent twenty minutes scrolling through the various forums, examining the code posted there. Little of it was fresh or unknown to him. On occasion he'd see something that caught his attention, code he thought he could use, something new and creative. But on examination it was usually rubbish, or pointless.

Code was the essence of any computer, and of the Internet, which was simply a connection of millions of computers. Code was the machination behind the curtain that made everything else work. Code turned keystrokes into words in word processing, code made images, code produced color, code created hyperlinks.

Everything on a computer screen came from code. Those who could write code at a sophisticated level were creators; a handful were, in their way, godlike, for what they wrote produced marvelous manifestations.

But there was code, and there was code. Like a child painting a tiger by the numbers, some hackers, as code writers were generally called, did little more than follow the lines created by others. These script kiddies copied and pasted this from here, added a little of that from there, and counted themselves lucky when it actually produced something that worked.

Code generated in such a way looked as childish to the skilled hacker as that child's colored picture of a tiger. Other bits were repeatedly written, to the point of being counterproductive. One section might create an action, another would stop it; then it would be created again, then stopped again, sometimes in long, pointless strings. An amazing amount of code could be written to produce almost nothing. Useless code lay everywhere, occupying a cyber universe with its clutter.

Then there were the hackers such as Vladimir. These were artists of the most rare and talented sort. Their code was lean and strong, producing results with the sparest of keystrokes. What they wrote was elegant, masterful.

The Russian had made his cyber reputation by discovering a vulnerability in Windows XP. He'd posted the details in various chat rooms to claim the credit. Several weeks later, Microsoft confirmed the vulnerability when it released a patch to repair it. Vladimir had responded by posting the details of a second vulnerability. This time it took Microsoft three months to release a patch.

In standard computer protocol, Vladimir had no business publishing the vulnerabilities. He should have given the information directly to the company. By taking the approach he had, he'd gained an initial reputation for himself, but he'd also exposed many thousands of Windows XP owners to virus attacks. By posting, he had been able to claim full credit. Had he notified Microsoft, then posted the details only *after* the security patch was released, he would have been mocked.

Vladimir's reputation had grown when he posted the first vulnerability in Windows Vista within hours of its being released. In fact, he'd discovered three vulnerabilities while examining the beta

version—but by that time he was losing interest in what he considered the juvenile game of claiming credit for finding weaknesses in the software giant's programs. It was impossible to produce a complex program to serve so many millions of users and not leave *something* vulnerable. He'd claimed the one, but had quietly informed Microsoft of the other two.

Still, Vladimir's reputation had been made. He'd had no lasting desire to involve himself daily in the cyber-hacker world and had always been a private person, so with the posting of the first Windows Vista vulnerability, he'd withdrawn from regular active exposure in the hacker chat rooms and forums.

By this time Vladimir had realized he possessed an extraordinary aptitude. It took another two years to turn it into meaningful income. Now his services were much sought after, and he could pick and choose his assignments. He maintained an e-gold account—a digital gold currency created to allow the instant transfer of gold ownership between users—into which his fees were deposited outside Russia. There were over 3 million e-gold accounts and nearly 4 million ounces of gold in storage. But one of the unintended uses of the accounts was to, in essence, allow the laundering of payments.

For his immediate need, Vladimir decided no help was to be found on the Internet. He returned to the code he was writing and tried again. Still … something eluded him. He went back and rewrote a section, then nodded. He copied the sequence and dropped it into his test computer. It worked.

Vladimir smiled. Slick. This last was his best. Even he was impressed.

**MANHATTAN, NYC**

**IT CENTER**

**FISCHERMAN, PLATT & COHEN**

**TUESDAY, AUGUST 15**

**2:32 A.M.**

As was his habit when working, Jeff set his digital watch to chirp every two hours. When it went off, he would stand from his station, stretch, then take a walk around the offices to exercise his body and clear his head, though a part of him never let go of the problem he was grappling with. He'd drink a Coke or a cup of black coffee, use the restroom, wash his face, then return to his place.

Respectful of his dedication, Sue didn't break his concentration with idle chatter or questions about what she was seeing over his shoulder. She took her breaks at different times, always returning with the smell of cigarette smoke about her. He'd sniffed once before realizing it came from her. She'd said, "I know. A disgusting habit. I just *have* to quit."

At one point some hours into the process, Harold disappeared. It could have been the middle of the night or broad daylight. Jeff had no idea. But when Harold returned with food from the all-night diner, Jeff realized how hungry he was. He wolfed down a ham-and-cheese sandwich just as the new framework dropped the unencrypted copy of the code onto his disk. He chewed as he analyzed it.

So far, he had discovered mostly negatives. The single most troubling development had been an attempt by the virus to replicate itself. In this case, it had failed, but, he realized, in other environments it might well be succeeding. It didn't affect what he was doing today, though it could mean disaster for thousands of other businesses. But that was in the future. Right now he had to concentrate on what he was getting paid to do. As he finished the food and wiped his hands on a napkin, Jeff mentally groaned at what he saw. Even the decrypted code he'd labored so long to produce was obtuse. The cracker was using tricks that ran in the low-level environment. That meant that this approach was a dead end.

Jeff didn't realize that Sue had been gone until she reentered the room. She came up behind him and leaned down at a time when he had his screen filled with the string output. Her proximity reminded him for a moment that she was an attractive woman. But almost as quickly as the sensation came, it vanished. It had happened before when he'd been drawn to a woman. He knew the shutting down of his emotions was related to Cynthia's death, and the guilt he felt about not having done more to prevent it.

But nothing would ever change what had happened.

His BlackBerry rang, snapping him out of his gloom. "Excuse me," he muttered to Sue, as he answered.

Sue took the opportunity to examine Jeff much more closely as he listened to his caller. She'd been attracted from the start and, having watched him work, was now even more impressed. Now she could take him in as a man and liked what she saw. She wondered if he mixed business with pleasure. In her experience, most men did, given the chance.

"I'm in Manhattan too, on a system crash. I've never seen anything like it. I'm sorry to hear about the deaths." Jeff paused. "Sure, sure. That sounds good, Daryl. Maybe I'll know something by then." Slipping his BlackBerry back in his pocket, he looked up at Sue. "Sorry about that. A colleague. She's in town working on something similar."

"She's obviously dedicated. It's the middle of the night. Could it be the same virus?"

Jeff considered what Daryl had told him. "It's possible, except her virus didn't crash the system. Just caused it to malfunction in a deadly way."

"I guess we should be thankful no one's died even with all the problems we're having. This could be a lot worse. Any luck? You've been at this for some time, and I thought I worked long hours."

Jeff grinned. "It's why I get the big bucks. I may not solve the problem, but they can't complain about the time I put in." Jeff's smile vanished. "What I've found so far isn't making much sense."

"Any guesses?"

"Unfortunately, a few." Leaning back in his chair, Jeff folded his arms across his chest. "So far, whatever you contracted isn't a known variant of a virus. It doesn't look very sophisticated, since it killed itself, and in probability is a cut-and-paste job at its core. But it was plenty destructive. It wanted to replicate, which is bad news for other computers. It's also encrypted and deeply embedded, which is making my job very tough. From how some of the code is written, I can speculate that the author may be Russian. If true, that's not reassuring at all. The Russian Mafia is heavily involved in financial fraud through malware."

Jeff stopped and thought about the implications of what he'd just said. In recent years the Russian Mafia had hired the best software engineers in the former Soviet Union to create new viruses

and unleashed them on the cyber world. They were making hundreds of millions a year, and the more they made, the more aggressive and creative they'd become.

"I'm surprised the virus has been so hard to find," Sue said, focusing his thoughts.

"They usually aren't," Jeff agreed. "Typically, I spend most of my time recovering information and rebuilding systems. But lately I've been seeing more and more of this kind of thing. A cracker gets into your system to do damage, not to steal information. Not long ago a guy was caught who hired a cracker to shut down the Web sites of his major competitors. These were Internet businesses; as long as he got away with it, everyone's customers went to him."

"That's terrible!" Sue knew the Internet was used for scams, but she'd never before heard such a story. To her, the Internet should be benign, a resource to make life better, not a destructive force.

Jeff knew what Sue was feeling. He often felt the same way. "I hate to say it, but that's only one of hundreds of ways to profit from cybercrime. In the good old days, hackers were geeks out to make a name for themselves. Now they can earn money, sometimes big money, with the same skills and malicious intentions. There are even Web sites where you can download malware. You graft on something you've cooked up yourself, and you're off and running. One guy got into a bank's system and had a tenth of a penny—that's all, just a tenth of a penny—taken from every transaction over one hundred dollars and wired into an offshore account. The bank's computer was programmed to round pennies up, so it kept covering the shortage."

"What's a tenth of a penny?"

"I have no idea." Jeff shrugged. "I guess they break currency down as far as they can. He could have asked for a twentieth, or a hundredth."

"What happened?"

"Within four months he'd made over six hundred thousand dollars. Even then the bank's computer kept covering for him. I don't know how long it would have gone on if he hadn't made the mistake of not deleting all bank-employee accounts from his scam. See, these people knew the system, and a lot of them balanced their checkbooks to the penny. One of them spotted that the accounting system was skewing and checked the programming. He found the virus, and it didn't take long to find the crook." Jeff took a sip of coffee. That hadn't been his case, but he'd cracked one like it, and it had felt very, very good. In some ways the satisfaction he took from his work was more important than the pay.

"I'm surprised our security measures didn't stop this. They were supposed to," Sue said.

"All security systems are reactive in nature. That means the virus has a head start in infecting computers *before* it's identified and enters the log of the antivirus and firewall programs. There are very sophisticated crooks who have taken to hiring crackers to deliver viruses that steal financial information.

Computer security has become much more difficult now that there's a great deal of money to be made. Russian crackers looted a French bank of more than one million dollars in 2006."

Sue shook her head in amazement.

"Since your firewall and antivirus software didn't spot whatever it is, it's something off the charts," Jeff said, rubbing his forehead, trying to ease his exhaustion away. "Something new, or something very sneaky—perhaps something targeted specifically at you. Any business makes enemies."

"I hadn't considered that." Sue shifted in her chair and pointed at Jeff's computer screen. "But you think this is Russian."

"I can't really put my finger on it. I've been able to read some of the code, and it's just got a Russian feel to it."

"Maybe somebody copied some Russian code."

"Could be, could be. But like I said, the Russians have lots of computer-savvy people, and they lease themselves out to criminal groups."

"You think something like that happened to us?"

"I can't say at this point. I see sophisticated along with sloppy work. The virus might have been after your data or bank records, but something went wrong because the code was carelessly written."

"So you think this is about our financial data?"

Jeff grinned. "I don't know. I'm just speculating here. It might also be an attack meant to create the destruction it's causing, or something gone awry. It's possible it steals information, sends it out, then destroys itself to cover its tracks. I just don't know enough yet."

Harold was long gone and no one was working in the outside offices. The building was quiet, almost as if it were asleep. "Let's get some more coffee," Sue said. In the break room she emptied the coffee machine, rinsed out the pot, filled it with bottled water, opened a container of coffee, and placed it into a new filter. She turned the machine on, then leaned back against the counter to wait. "So you still play video games," she said with an amused look.

Jeff smiled. "My secret vice. Actually, it's all related. At least that's what I tell myself. I prefer online first-person shooting scenarios. It's how I deal with stress and it's something I can do anywhere. I also like brainteasers."

"That's where your work comes in."

"Right. I hate to lose. I'll stick with a virus until I have it figured out, no matter how long it takes."

Sue arched an eyebrow. "That must get expensive for the client."

He shook his head. "No, there's a point beyond which it makes no sense to keep billing. After I've fixed the problem, though, I'll take the virus home and work on it there until I've got it." He met her eyes. "How long have you been here?"

Sue gave him her nonoffice smile. "Just over four years." Pouring them each a fresh cup of strong coffee, she motioned to Jeff to sit down at the well-used table. Placing his coffee in front of him, she seated herself, took a sip, and sighed with satisfaction before continuing, "I'm from northern California, went to UC Berkeley for computer science. I worked at Microsoft, then took a job in San Francisco before moving here. I've worked at Cohen ever since. Until Saturday, it was a good job. Greene's a pain sometimes, but as long as the system works, he leaves us alone, and Harold has no life away from work. Sadly, that makes two of us. And so you don't have to ask, my dad's white and my mom is third-generation San Francisco Chinese. Big scandal in the family. What about you?"

"I'm from Philly originally. I majored in math, enjoyed computer science, so went to the University of Michigan for my Ph.D."

Sue flashed that friendly smile again. "I have to say, Jeff, you certainly don't look like a computer geek."

He laughed. "Genetics, mostly, though I played rugby in college and football in high school."

"Then what?"

"I taught at Carnegie Mellon, but like almost everybody who isn't a suck-up, it became clear I wouldn't get tenure. I went to work for the Cyber Security Division at the CIA, in 1998."

Sue lit up. "A spook, huh?"

"Hardly," Jeff said, eager to discourage any romantic notions about his CIA work. "I worked in a crummy office just like yours, only buried in the basement at Langley. Technically I was head of a three-man team called the Cyberterrorism Unit, but my two assistants were always off doing standard IT work for the division."

"What'd they have you doing, or can't you say?"

"No, I can talk about my duties, within reason," Jeff said. "The only danger is I'd bore you to death."

"I'm listening."

"Trust me, it wasn't glamorous." He filled her in on his years at the Company, telling her he'd held no illusions when he was recruited for the position. "Government work is government work. But I figured it couldn't possibly be worse than academia. I was wrong."

Though the threat to the Internet was real enough, at that time it was considered to be largely abstract. The Company budget was allocated primarily to the traditional physical threats. When it came

to computers and the Internet, the threat was generally perceived as the possible physical destruction of facilities.

As their primary mission, Jeff and his truncated team worked on recovering data from computers seized from suspects and known terrorists. But they were also responsible for tracking the use of the Internet for terrorist activities and for potential threats.

During the years of his employment, as the Internet grew and spread its tentacles into every aspect of American life and the world community, the potential for a cyber-terrorist attack rose exponentially. The safety of the Internet, and of those computers connected to it, was dependent solely on the security of each individual computer that formed part of the network.

Jeff had certainly seen the threat. He had reasoned that as more government agencies conducted both external and internal business through the Internet, as more banks came online, as nuclear power plants continued linking to one another, and as the U.S. military came to increasingly rely on the Internet and computers to conduct its operations, his unit would receive greater resources and command more attention. He'd been wrong.

The irony was that the Internet had originally been developed as a national security system. In the 1960s, the Department of Defense had been concerned about the vulnerability of its mainframe computers—back in the days when all computers were mainframes—and of its increasingly computer-linked communications system. Several well-placed ICBMs, or even one at a critical point, could potentially cripple America's ability to defend itself. The air force was especially concerned about maintaining real-time control over its nuclear missiles.

What then emerged was a government-funded system of interconnected computer redundancy. The idea was that even if several computer hubs at key installations were nuked, the system, the actual Internet, would reroute itself around them. In theory, like the multiheaded Hydra of Greek mythology, it would be impossible to defeat. It might be slow, it might electronically hiccup, but the system would function. Jeff wasn't so sure. The designers had only considered outside threats. They'd never contemplated the ultimate digital universe they'd created, or that the real threat to the Internet might well come from within.

Although the Internet had proven itself enormously popular with the worldwide community and had become increasingly vital to the lives of individuals and the welfare of Fortune 500 companies, interest in safeguarding it wasn't as high as it ought to be. Jeff was convinced that it would take a significant failure of the system or a coordinated cyber-attack to awaken everyone. Just as it had been impossible to put the United States on a proper war footing before Pearl Harbor, the same fate seemed to await the future of Internet security. No one liked being Cassandra, but he'd found himself playing that role, seen as an alarmist while his warnings were ignored.

Jeff dragged his thoughts back to the present. "Though my primary concern was cyber-security, I knew the Internet could be used to organize and coordinate terrorist attacks," he told Sue, taking up where he'd left off. "I wore out my welcome arguing for resources. I finally decided that only a seriously

mounted terrorist attack against us with significant damage against a target that mattered was going to shake the lethargy of the intelligence community."

"I guess we got that on 9/11, didn't we?" Jeff seemed to wince, and for a moment Sue feared she'd misspoken.

After a pause he said, "You'd think so, but I'm still not sure they got the point."

Sue freshened their coffee and pushed the container of skim milk closer to Jeff. "Go on," she encouraged.

Jeff prepared his coffee as he continued, "In those days I spent a lot of nights trolling hacker chat rooms looking for signs of a plot."

"Not much of a social life."

Jeff smiled. "No. Probably about as active as yours."

"I might surprise you." She pointed her raised cup toward him. "But finish the story. I'm waiting for the part about bosses not listening."

Jeff looked away. How much did he really want to say? He'd avoided the subject until now. But maybe it would be good to talk about it.

First he told her how for most of 2001, he and his team, when available, worked to retrieve information from the hard-drive disks sent to him. Seized from various terrorists or terrorist suspects by a wide range of agencies throughout the world, the disks, or copies of them, had ended up in the hands of the CIA. If British SAS captured an IRA suspect, the hard drive from his computer, or its clone, would at some point find its way to Jeff's desk. It was the same for the Mossad. Even the CIA's own meager foreign-agent force produced disks from time to time.

As is generally the case in intelligence, the individual bits of data he produced from these sources by themselves meant little. Once he plucked them from the disks, though, they were fed into a master program by his unit, where they might, or might not, assume their proper place in the database about the terrorist world. He never knew. In fact, he had no idea if anyone was routinely consulting the growing body of data his unit was compiling on the operations of various worldwide terror groups.

"So what happened?" Sue asked. Jeff saw how eager she was and wondered for a moment how she'd react to the whole story.

"I really can't go into it. Let's just say, my boss and I had a disagreement, and I left."

"There's a story there you'll have to trust me with sometime," she said mischievously. "Is that when you started your own company?"

"Yes," Jeff said, glad to change the subject. "Turns out all those contacts I made with the Company were good for something. It's been a bigger success than I ever expected. One job after

another. So no complaints there." He sipped his coffee and turned to the problem at hand. "Let's get back to you. The bad news is that your records, financial as well as work product, are all but a total loss from what I can see. I keep holding out hope they'll turn up somewhere, but I don't think so."

"Is there anything you can do for us?" She looked hopeful and he hated having to disappoint her.

"I'm trying to identify the virus sufficiently so that we can be certain it's not in your nightly or weekly backup. With that information we can determine if they're clean." He held up a hand of caution at seeing her become crestfallen. "I haven't found a hint of when you picked this up, so I can't tell from the time frame which, if any, of your backups are clean. It could have been lurking in there a very long time."

Sue bit her lower lip. "I was afraid that might be the case." She thought a moment, then gave him a wan smile. "So the worst-case scenario is that our current computers are fried. Useless. Whether or not we can recover the data from the backups, I'll still have to install a brand-new system. It will kill me." She made a face at the very thought of it. "It's going to take weeks to physically put everything in place, then load and link the software, then at least a month to get all the bugs out. And we have to know how to find this virus before I can activate it with our old data so that someone doesn't inadvertently reintroduce it. I don't even want to think about that." She looked into his eyes. "Save me from it all, will you? I'll be very grateful." She drained her coffee, then yawned. "Have you noticed these marathon sessions are getting tougher and tougher, the older you get?"

"Give me a break, Sue. You're a kid compared to me."

Sue smiled. "It's been good talking, though. If I get canned, I might come looking for a job."

"It won't come to that, I'm sure," he said, though it wouldn't surprise him if she ended up being the scapegoat. It wouldn't be the first time he'd seen that happen.

"I might come looking anyway." With that, she gave him a warm smile and left for the IT Center, her short hair bouncing, lean hips swinging.

*   *   *


Back at the office a bit later, Jeff asked if she'd found anything useful.

"Almost nothing." She grimaced. "I examined the logs. As I'm sure you know, we're hit thousands of times a day by malware looking for a vulnerability. Some of it's generated by a living hacker, but most are by automated worms, trolling the Internet. It was a bit daunting, realizing how under assault we constantly are, but I didn't see any failure in our protection. This obviously got through, but I can't see when or how. Wish I could be more help."

"And Harold?"

"I've had him reimaging the lawyer workstations and laptop systems in the office with clean system installs of the operating system and necessary applications. He's also checking the e-mail archives and database for signs of tampering." She yawned, covering her mouth with the back of a hand. "Last, but not least, I've got him screening all the complaint calls we're getting from associates. They don't pay me enough to do that."

She hesitated as if considering something, then said, "I've been meaning to mention a string I came across in your printouts, but you were awfully busy. I don't think it's anything important, but look at this." Jeff leaned over and read:

Sh3 w!ll n3v3r 13t ur sp!r!tz d0wn


Sh3s a v#ry k!nk! g!r7


Jeff realized he'd missed the text in his earlier scan. Sometimes the clues to a cracker were in the ego parts, those sections of code about himself he couldn't resist inserting. "I never saw that. What is it?"

"Don't laugh, but I think it's leet-speak," she said, straightening up.

*Leet-speak* was hacker language. Malware authors often left their calling cards in their code, even if it was only for them and other hackers to see. Since this one was originally encrypted, it was obviously not meant for the eyes of security investigators.

"It's 'Super Freak,'" Sue said, dropping her arms.

"'Super Freak'? The song?"

"I think so." Sue wrinkled her brow. "How does it go? 'She's a very kinky girl, the kind you don't take home to mother.'" Sue's singing voice was surprising deep and guttural. Now that she had the words and the tune, she was really getting into the song, swinging her hips, raising her voice. "Yeah! I've still got it! Our hacker likes Rick James punk funk. He's not *all* bad."

"Aren't you a bit young to know Rick James? 'Super Freak' was … what? Sometime in the early '80s?"

"Rick James is classic."

Jeff looked back at the screen. "Okay, 'Super Freak.' But what does it mean? Is that the name of the virus? Or the cracker's handle? Someone who's a Rick James fan?"

"Super Freak" might be significant, then again it might not, Jeff thought. Some virus code changed hands so many times all kinds of leet-speak from script kiddies crept in. It might not be connected to the virus's author at all.

"It might be his cyber handle," Sue suggested. "You should be looking for it in any code you find. I'll see if I can turn anything up in hacker chat rooms later." She yawned again. "I'm beat." She gave him a winning smile. "I'm going to lie down for a bit. I haven't pulled an all-nighter since college." She turned and walked away toward the couch, stretching as she did.

"No problem," Jeff murmured. "I'll probably lie down a bit later myself. I've still got some juice, though, and will feel better if I can get something definite before taking a real break. Your boss will ask, I'm certain." He looked over at Sue; she was already asleep.

**BROOKLYN, NEW YORK**

**MERCY HOSPITAL**

**TUESDAY, AUGUST 15**

**8:09 A.M.**

Daryl Haugen was given full access to the IT center in the basement of Mercy Hospital, where she found the staff cooperative. They'd taken the deaths of patients personally. Winfield had dropped by several times, but she had nothing to give him. Working not far from a furnace at an unused station, it had taken nearly a day of work to unlock the code she detected in the server. Yet, so far, she'd turned up nothing useful.

She felt the adrenaline coursing through her despite the long hours. These crackers were so full of themselves, so certain they could fool everything, she went after them with a vengeance. She'd never been able to tolerate such self-satisfaction. She found it interesting that George Carlton, officially the man responsible for stopping this sort of thing, was no less egocentric. For some time she'd thought he was just pitching his department when he crowed about his accomplishments, but she'd come to realize he actually believed he was doing an effective job. *Contempt* scarcely described her true feelings toward him.

Something had scrambled the hospital medication program; she just couldn't identify it. Her staff in Virginia was on this, but thus far they'd come up with nothing useful. The more people of talent and skill she had engaged, the sooner they'd have a solution, so she'd been glad Jeff Aiken was available. He was bright, creative, and hardworking. From her experience she knew he had the knack of thinking outside the box.

Daryl had located suspect code from a corrupted registry file and was now running it through a string analyzer, a program that dumped any data values in the file that could be represented with a printable character. Many code values translated to printable characters so there was a lot of garbage, but she also saw strings the programmer had in the code that referenced registry settings and files. Programmers often left debugging code that included messages in place that would be revealed in the string output. It took Daryl a few minutes to go over the strings, which largely looked like this:

rX + %”/

Lep

ccc