ROBERT D. AUSTIN

The iPremier Company (A): Distributed Denial of Service Attack

January 12, 2018, 4:31 AM

Somewhere a phone was chirping. Bob Turley, CIO of the iPremier Company, turned beneath the bed sheets, wishing the sound would go away. Lifting his head, he tried to make sense of his surroundings. Where was he?

The Westin in Times Square. New York City. That's right. He was there to meet with Wall Street analysts. He'd gotten in late. By the time his head had hit the pillow it was nearly 1:30 AM. Now the digital display on the nearby clock made no sense. Who would be calling at this hour? Why would the hotel operator put a call through?

He reached for the phone at his bedside and held it to his ear. Nothing. The chirping was coming from his mobile. Staggering out of bed, he located the noisy phone and opened the call.

"This is Bob Turley."

"Mr. Turley?" There was panic in the voice. "I'm sorry to wake you, Joanne told me to call you."

"Who is this?"

"It's Leon. Ledbetter. I'm in Ops. We met last week. I'm new. I mean, I was new, last month."

"Why are you calling me at 4:30 in the morning, Leon?"

"I'm really sorry about that Mr. Turley, but Joanne said—"

"No, Leon, I mean tell me what's wrong."

"It's our website, sir. It's locked up. I've tried accessing it from three different computers and nothing's happening. Our customers can't access it either; the help desk is getting calls."

"What's causing it?"

Professor Robert D. Austin, Dr. Larry Leibrock (Chief Technology Officer, McCombs School of Business, University of Texas at Austin), and Alan Murray (Chief Scientist, Novell Service Provider Network) prepared this case. This revised version was prepared by HBS Emeritus Professor Richard L. Nolan, Professor Robert D. Austin (Ivey Business School), and Professor Michael Parent (Beedie School of Business, Simon Fraser University). HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management. The situation described in this case is based on real accounts of denial of service attacks directed against several companies during 2000 and 2001. Company names, product/service offerings, and the names of all individuals in the case are fictional, however. Any resemblance to actual companies, offerings, or individuals is accidental.

"Joanne thinks—if we could only—well, someone might have hacked us. Someone else might be controlling our site. Support has been getting these e-mails—we thought it was just the web server, but I can't access anything over there. Joanne is on her way to the data center. She said to call you. These weird e-mails, they're coming in about one per second."

"What do the e-mails say?"

"They say 'ha.'"

"Ha?"

"Yes, sir. Each one of them has one word in the subject line, 'ha.' It's like 'ha, ha, ha, ha.' Coming from an anonymous source. That's why we're thinking—."

"When you say they might have hacked us—could they be stealing customer information? Credit cards?"

"Well, I guess no firewall[1]—Joanne says—actually we're using a firewall service we purchase from the hosting company, so—."

"Can you call someone over there? We pay for monitoring 24/7, don't we?"

"Joanne is calling them. I'm pretty sure. Is there anything you want me to do?"

"Have we set our emergency procedures in motion?

"Joanne says we have a binder, but I can't find it. I don't think I've ever seen it. I'm new—"

"Yes, I got that. Does Joanne have her cell?"

"Yes sir, she's on her way to the data center. I just talked to her."

"Call me back if anything else happens."

"Yes sir."

Turley stood up, realizing only then that he had been sitting on the floor. His eyes were bleary but adrenaline was now pumping in his bloodstream. Steadying himself against a chair, he felt a wave of nausea. This was no way to wake up.

He made his way to the bathroom and splashed water on his face. This trip to New York was an important assignment for someone who had been with the company such a short time. It demonstrated the confidence CEO Jack Samuelson had in him as the new CIO. For a moment, Turley savored the memory of the meeting in which Samuelson had told him he would be the one to go to New York. As that memory passed another emerged, this one from an earlier session with the CEO. Samuelson was worried that the company might eventually suffer from "a deficit in operating procedures." "Make it one of your top priorities," he had said. "We need to run things professionally. I've hired you to take us to the next level."

[1] A "firewall" is a combination hardware/software platform that is designed to protect a local network and the computers that reside on it against unauthorized access.

Looking himself over in the mirror, seeing his hair tussled and face wet, Turley lodged a protest with no one in particular: "I've barely been here three months!"

The iPremier Company

Founded in 1996 by two students at Swarthmore College, the iPremier Company had evolved into a web-based commerce success story. From its humble beginnings, it had risen to become one of the top two retail businesses selling luxury, rare, and vintage goods on the web. Based in Seattle, Washington, the firm had grown and held off incursions into its space from a number of well-funded challengers. For the fiscal year 2017, profits were $20.1 million on sales of $320 million. Sales had grown at more than 20% annually for the last three years, and profits, though thin, had an overall favorable trend.

Immediately following its IPO in late 1998, the company's stock price had nearly tripled. It had continued up from there amid the euphoria of the 1999 markets, eventually tripling again. A follow-on offering had left the company in a strong cash position. During the NASDAQ bloodbath of 2000, the stock had fallen dramatically but had eventually stabilized and even climbed again, although not to pre-2000 levels. In the decade plus since, the company had held its own and consolidated its leading market position, enjoying better-than-average returns by streamlining and focusing its business to achieve profitability.

Most of the company's products were priced at a few hundred dollars, but there were a small number of items priced in the thousands and tens of thousands of dollars. Customers paid for items using their credit cards. The company had flexible return policies, which were intended to allow customers to thoroughly examine products before deciding whether to keep them. The iPremier customer base was high-end—so much so that credit limits on charge cards were rarely an issue, even for the highest-priced products. Trust was critical to this relationship. Customers had to believe and trust that the goods sold by iPremier were genuine. Otherwise, they could easily purchase the same sorts of goods from a number of other websites, including iPremier's fiercest competitor, MarketTop. iPremier's competitive advantage lay not necessarily in its array of goods, but more in its responsive and attractive website, order fulfillment, and after-sales service. iPremier led its industry segment in the quality of the "user experience" and constantly innovated to provide the best, and most seamless service. As a result, the company had over one million regular customers in its database, and another few hundred thousand casual buyers.

Management and Culture

The management team at iPremier was a mix of talented younger people who had been with the company for a long time, and more experienced managers who had been gradually hired as the firm grew. Recruitment had focused on well-educated technical and business professionals with reputations for high performance. Getting hired into a senior management position required excelling in an intense series of three-on-one interviews. The CEO interviewed every prospective manager at the director level and above. The reward, for those who made the grade, was base compensation above the average of managers at similar firms, and variable compensation, mainly in the form of stock options, that could be a significant multiple of the base. All employees were subject to quarterly performance reviews that were tied directly to their compensation. Unsuccessful managers did not last long. Most managers at iPremier described the environment as "intense."

Throughout the company, there was a strong commitment to doing "whatever it takes" to get projects done on schedule and on budget, especially when it came to system features that would benefit customers. The software development team was proud of its record of consistently launching new features and programs a few months ahead of MarketTop. Senior managers understood that their compensation and prospects with the company depended on executing to plan. They pursued "the numbers" with obsessive zeal.

Technical Architecture

The company had historically outsourced management of its technical architecture and had a long-standing relationship with Qdata, a company that hosted most of iPremier's computer equipment and databases, and provided connectivity to the Internet. Qdata was an early entrant into the Internet hosting business, but it had been battered by the contraction of the Internet bubble and lost any prospect of market leadership. Its data center was physically proximate to the corporate offices of iPremier; some felt there was little else to recommend it. The company had not been quick to invest in advanced technology and had had trouble retaining staff.

The iPremier Company had a long-standing initiative aimed at eventually moving its computing to an internal facility, but several factors had kept this from happening. First, and most significant, iPremier had been very busy growing, protecting its profits, and delivering new features to benefit customers; hence the move to a better facility had never quite made it to the top of the priority list. Second, the cost of more modern facilities was considerably higher—two to three times as expensive on a per-square-foot basis. Third, there was a perception that a move might risk service interruption to customers. Finally, one of the founders of iPremier felt a personal commitment to the owners of Qdata because they had been willing to renegotiate their contract at a particularly difficult time in iPremier's very early days.

4:39 AM

Sitting at the hotel room desk, Turley began scrolling through the phonebook on his phone. Before he could find the number for Joanne Ripley—his technical operations team leader—she called him.

"Well, Joanne. How are you this morning?"

A cautious laugh came from the other end of the call. "About the same as you, I'm guessing. I assume Leon reached you."

"He did, but he doesn't know anything. What's going on?"

"I don't know much either, yet. I'm in the car, on my way to the data center. I ought to be there in five minutes."

"How long after that until we are back up and running?"

"That depends on what's wrong. I'll try restarting the web server as soon as I get there, but if someone has penetrated our databases and stolen customer data, getting the server running will be the least of our worries. Did Leon tell you about the e-mails?"

"The 'ha, ha' e-mails? Yeah. Makes it sound like something deliberate."

"I'd have to agree."

"No chance it's a simple DDoS attack?"

"I doubt it's a *simple* DDoS attack; we've got software to deal with those."

"Can we track the e-mails?"

"Not soon enough. They're coming through an anonymizer that's probably in Europe or Asia. If we're lucky we'll find out sometime in the next decade who sent them. Then we'll discover they're originating from some laptop or smart thermometer in Podunk, Idaho, and their owner has no idea they've been compromised by hackers."

"What are the chances they're stealing credit cards? I know we don't keep credit card numbers on our database, but they could be stealing other sensitive information, right?"

Ripley paused before answering: "There's really no way of knowing."

"Should we pull the plug? Physically disconnect the communications lines?"

"If we start pulling cables out of the wall it may take us a while to put things back together."

"Joanne, don't we have emergency procedures for times like this? I don't think I've seen it but it comes up when people mention our business continuity plan (BCP)."

"We've got a BCP binder," said Ripley. "I've got a copy with me. Keep it in my car. There's one at the office too, and we store it electronically on our shared drive. But to be honest, well—it's out of date, and we don't really train people with it because of that. Lots of people on the call lists don't work here anymore. I don't think we can trust the phone numbers and I *know* some of the technology has changed since it was written. We've talked about practicing incident response but we've never made time for it."

"A Disaster Recovery Plan (DRP)? An Incident Response Plan (IRP)?" Turley was incredulous. It boggled his mind, and created more than a little career-anxiety that he hadn't thought to check these since his arrival. He'd assumed that, as a publicly-listed company, iPremier had to have such plans.

But now was not the time, he decided, to grill Ripley about it. So he changed the subject: "What's the plan when you reach the data center?"

"Let me restart the web server and see what happens. Maybe we can get out of this without too much customer impact."

Turley thought about it for a moment. "Okay. But if you see something that makes you think customer records or other information are being stolen, I want to know that immediately. We may have to take drastic action."

"Understood. I'll call you back as soon as I know anything."

“Good. One more thing: Who else knows this is going on?”

“I haven’t called anyone else. Leon might have. I’ll call him and call you right back.”

“Thanks.”

Turley disconnected. Just as he did so, his phone rang again.

"Damn." It was Warren Spangler, VP of business development. Turley recalled vaguely that Warren and Leon's father were college buddies or something. Ledbetter had almost certainly called Spangler.

"Hi, Warren," said Turley.

"Hi, Bob. I hear we've got some kind of incident going on. What's the story?"

"Something's definitely going on, but we're not sure what yet. We're trying to minimize customer impact. Fortunately for us, it's the middle of the night."

"Wow. So is it just a technical problem or is somebody actually doing it to us?"

Turley was eager to call the chief technology officer (CTO), so he didn't really have time for this discussion. But he didn't want to be abrupt. He was still getting to know his colleagues.

"We don't know. Look, I've got to—"

"Leon said something about e-mails—"

"Yes, there are suspicious e-mails coming in so it could be someone doing it."

"Oh, man. I bet the stock takes a hit tomorrow. Just when I was going to exercise some options. Shouldn't we call the police?"

"Sure, why don't you see what you can do there, that'd be a big help. Look, I've got to—"

"Seattle police? Do we know where the e-mails are coming from? Maybe we should call the FBI? No. Wait. If we call the police, the press might hear about this from them. Whoa. Then our stock would really take a hit."

"I've really got to go, Warren."

"Sure thing. I'll start thinking about PR. We got you covered here, bro. Keep the faith."

"Will do, Warren. Thanks."

Turley ended that call and began searching through his cell phone's memory to find the number for Tim Mandel, one of iPremier's co-Founders and now the company's CTO. He and Mandel had already cemented a great working relationship. Turley wanted his opinion. Just as Turley was about to initiate the call, though, another call came in from Ripley.

Turley answered the phone and said: "Leon called Spangler, I know. Anything else?"

"Ah, no. That's it for now. Bye."

Turley dialed Mandel. At first the call switched over to voicemail, but he retried immediately. This time Mandel answered sleepily. It took five full minutes to wake Mandel and tell him what was happening.

"So what do you think, should we just pull the plug?" Turley asked.

"I wouldn't. You might lose some logging data that would help us figure out what happened.

"I'm not sure knowing exactly what's happening is the most important thing to me right now."

"I suggest you change your mind about that. If you don't know what happened this time, it can happen again. And, if you don't know what happened, you won't know what, if anything, you need to disclose publicly. We might also need to preserve evidence of what has happened. A DDoS attack is a federal crime, and we might eventually need to involve the FBI."

Turley heard a thumping sound, as if Mandel had fallen getting out of bed; his phone clattered as it impacted something, the floor perhaps. A scant moment later, Mandel came back on the line and continued: "Come to think of it, Bob, preserving the logs is irrelevant because I'm pretty sure detailed logging is not enabled. Detailed logging adds a performance penalty of about 20%. Someone somewhere at some point decided that unacceptably impacts the customer experience."

"So we aren't going to have evidence of what happened anyway."

"There'll be some, but not as much as we, or the FBI, will want."

Another call was coming in.

"Hold on, Tim." Turley kicked the phone over to the waiting call. It was Peter Stewart, the company's legal counsel. What was he doing awake?

"This is Turley."

"Hey, Bob, it's Pete. Pull the plug, Bob. Shut off the power, pull the cords out of their sockets, go dark, kill it…everything. We can't risk having PII (Personally Identifiable Information) stolen."

"Spangler call you?"

"Huh? No, Jack. Samuelson. He called three minutes ago, said hackers had control of our web site and were stealing information. Told me in no uncertain terms to call you and 'provide a legal perspective.' That's exactly what he said: 'provide a legal perspective.'"

So the CEO was awake. The result, no doubt, of Spangler's "helping" from that end. Stewart continued to speak legalese at him for what seemed like an eternity. By this time, Turley was incapable of paying attention to him.

"Thanks for your thoughts, Pete. I've got to go, I've got Tim on the other line."

"Okay. For the record, though, I say pull the plug. I'll let Jack know you and I spoke, and will write a memo to file reflecting this conversation and my advice."

"Thanks, Pete," said Turley, acerbically.

Turley switched back over to the call with Mandel.

"Spangler's got bloody everybody awake, including Jack. I recommend you get dressed and head into the office, my friend."

"Is Joanne on this?"

"Yes, she's at Qdata by now." Turley's phone rang. "Got a call coming in from her now."

He switched the phone.

"What's up Joanne?"

"They won't let me into the NOC2," she said angrily. There's no one here who knows anything about the network monitoring and that's what I need to use to see the traffic coming into our site. The Qdata guy who can do it is vacationing in Aruba. I tried rebooting the web server, but we've still got a problem. My current theory is an attack directed at our firewall, but to be sure I've got to see the packets coming in, and the firewall is their equipment. You got an escalation contact to get these dudes off their butts?"

"I'm in New York, Joanne. I've got no Qdata contact information with me. But let me see what I can do."

"Okay. I'll keep working it from this end. The security guard doesn't look too fierce. I think I could take him."

"Do what you can."

Turley hung up. He noticed that Mandel had disconnected also. For a moment, Turley sat back in the chair, not sure what to do next.

5:27 AM

The phone rang again, and Turley could see from Caller ID that it was the call he had been dreading: Jack Samuelson, the CEO.

"Hi Jack."

"Bob. Exciting morning?"

"More than I like it."

"Are we working a plan?"

"Yes, sir. Not everything is going according to plan, but we are working a plan."

"Bob, the stock is probably going to be impacted and we'll have to put a solid PR face on this, but that's not your concern right now. You focus on getting us back up and running. Understand?"

"I do."

Samuelson hung up abruptly.

That had gone better than Turley had feared. He avoided the temptation to analyze Samuelson's every word for clues to his innermost thoughts. Instead, he called Ripley.

"Hi, Bob," she said, sounding mildly cheerful. "They let me in. I'm sitting in front of the console right now. It looks like a SYN flood from multiple sites directed at the router that runs our firewall service. So it *is* a DDoS attack. By the way, this is not a proper firewall, Bob; we need to work on something better." **(Exhibit 1 explains the different types of Denial of Service attacks).**

"Fine, but what can we do right now?"

[2] The "Network Operations Center" is the control room from which production computer operations and networks are monitored and operated.

"Well, looks like the attack is coming from about 3000 sites. If the guys here will let me, I'm going to start shutting down traffic from those sites. I'll have to set the phone down for a minute."

There was a pause of a couple of minutes. Turley heard some muffled conversation in the background, rapid keyboard clicks, then several epithets. Ripley came back on the line.

"Damn it, Bob, they're spawning zombies. It's Dawn of the Dead out there."

"You're going to have to translate that one for me, Ripley."

"Every time we shut down traffic from one address, the zombie we've shut off automatically triggers attacks from two other sites. I'll try it a few more times, but right now it looks like that's just going to make things worse. My guess is the hackers are using a 'bot net of enslaved machines."

"If it's a DDoS, they haven't hacked us, right? It means it's not an intrusion. They haven't gained entry to our system. So customer data are safe. Can we say that?" Turley was especially worried in light of recent, gigantic data breaches, and the ensuing class-action lawsuits they provoked (see **Exhibit 2**).

"There's nothing that makes a DDoS attack and an intrusion mutually exclusive, Bob."

Turley knew this, but had hoped otherwise in a moment of wishful weakness. Hearing Ripley remind him of the facts strengthened a growing, nauseating storm in his stomach. "I'll let you get back to it. Call me with regular updates."

Turley hung up and thought about whether to call Samuelson and what to tell him. He could say that it was a DDoS attack. He could say that the attack, by itself, was not evidence that customer information was at risk. But Turley wanted to think some more before he went on record.

Before he could do anything else, his cell phone rang again. It was Ripley.

"It stopped," she said excitedly. "The attack is over."

"What did you do?"

"Nothing. It just stopped. The attack just stopped at 5:46 AM."

"So—what now?"

"The website is running. A customer who visits our site now wouldn't know anything had ever been wrong. We can resume business as usual."

"Business as usual?"

"I'd recommend that we shut down, or at least disconnect from the public Internet, and give everything a proper going-over. In the longer run, we'll need to conduct a thorough forensic audit to ensure nothing else bad has happened. I've been thinking about how they targeted the firewall, and I don't think it sounds like script kiddies. With your approval, I'd like to reach out to some cybersecurity consultants and get them in ASAP."

What to Recommend

Post attack, Turley realized that he immediately faced a new decision: Whether to recommend shutting down – or, at least, disconnecting from the Internet as a precaution – while they figured out what had happened. Doing either would shut down normal business operations.

Shutting down to conduct a thorough forensic audit seemed like a prudent course, but it was unclear how long that would take. In such time, iPremier's customers could flee to a competitor. iPremier would have to explain a shutdown, and, for legal reasons, they'd probably have to admit that such a precaution was motivated by concerns about a data breach.

Shutting down, then, could freak out customers, sink the stock, even kill the company. And, Stewart's memo notwithstanding, there were plenty of good arguments to keep the business up and running. iPremier had done nothing to provoke the attack, and there was – as of this moment anyway – no actual evidence of an intrusion or breach. Turley knew that DDoS attacks were a daily occurrence, and that the bigger players like Amazon, Apple, Google, Yahoo and Microsoft were being attacked constantly. It was usually just a cost of doing business in this space, not a material event.

But – Ripley had observed that this seemed like a particularly sophisticated DDoS attack. And he realized, now, that the company had been lax in deploying and protecting its systems – the very thing he'd been hired to do. His new job honeymoon was over – he'd have to obtain the resources to secure company operations.

On the one hand, there was no *evidence-ba*sed reason to shut down. Indeed, doing so could be considered an irresponsible overreaction. After all, iPremier's corporate officers were first and foremost responsible to iPremier shareholders.

On the other hand, if customer data *had* been stolen, and if the site *was* insecure, keeping the site running could lead to more mischief by hackers – and kill the company in a different way, by exposing it to reputation damage, liability, and lawsuits.

Turley knew that the company's senior management team would be conflicted and angry about all this, and that he would have to make a recommendation soon. He guessed that Peter Stewart (Legal) and, probably, Joanne Ripley (Tech Ops) would want to shut the site down for an indefinite period, until such time as they would be reasonably assured that no data had been taken, or no ticking time bomb had been planted within iPremier systems. But he could easily imagine that some members of the senior management team would object to a shutdown; they would argue that until demonstrated otherwise, it should be assumed that nothing bad had happened beyond what they already knew – that iPremier had 'dodged a bullet'.

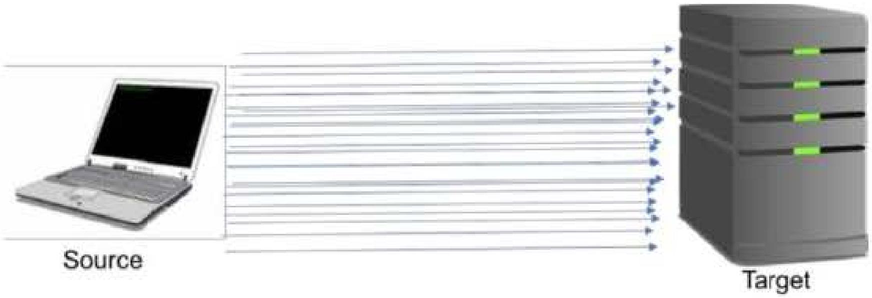
Samuelson and the Board of Directors would be looking to Turley for guidance, and his recommendation would have a profound impact on the future of the company.

Exhibit 1 Denial of Service Attacks Explained

Keying-in a website's URL (Uniform Resource Locator), or web address on a web browser or search engine's input line begins a conversation with the web server that will eventually return, or send the requestor the web page requested.

Each such "conversation" with a web server begins with a sequence of "handshake" interactions. The initiating computer first sends a "SYNCHRONIZE" or "SYN." The contacted web server responds with a "SYNCHRONIZE-ACKNOWLEDGE" or "SYN-ACK." The initiating computer then completes the handshake with an "ACKNOWLEDGE" or "ACK." A "SYN flood" is an attack on a web server intended to make it think a very large number of "conversations" are being initiated in rapid succession. Because each interaction looks like real traffic to the website, the web server expends resources dealing with each one. By flooding the site, an attacker can effectively paralyze the web server by trying to start too many conversations with it. This is the essence of a Denial of Service, or DoS attack.

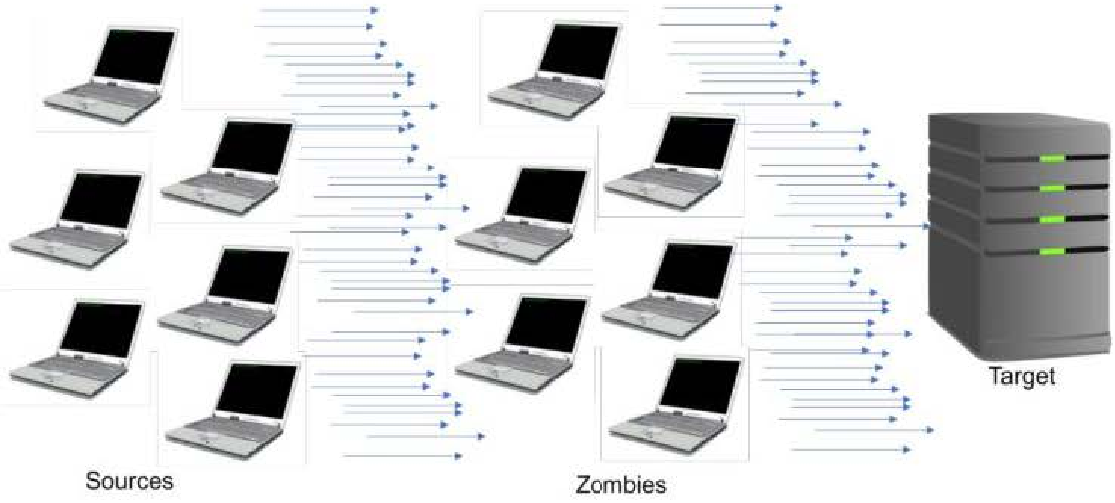
In its simplest form, an attacker uses a single computer to send many requests in rapid succession. Because these types of attacks (single source) can be more easily traced, they are seldom used, except for the most unskilled of script kiddies.



More sophisticated hackers engage in Distributed denial-of-service (DDoS) attacks, such as described in the case, where many requests come in rapid succession from many computers. This might include the use of "Botnets", large clusters of Internet-enabled devices such as cellphones, computers, and even smart devices like thermometers, that have been infected with malware, allowing hackers to control these devices - sometimes called "zombies" - remotely. In one recent example, the Mirai Botnet was used to attack Internet service company Dyn in October 2016.

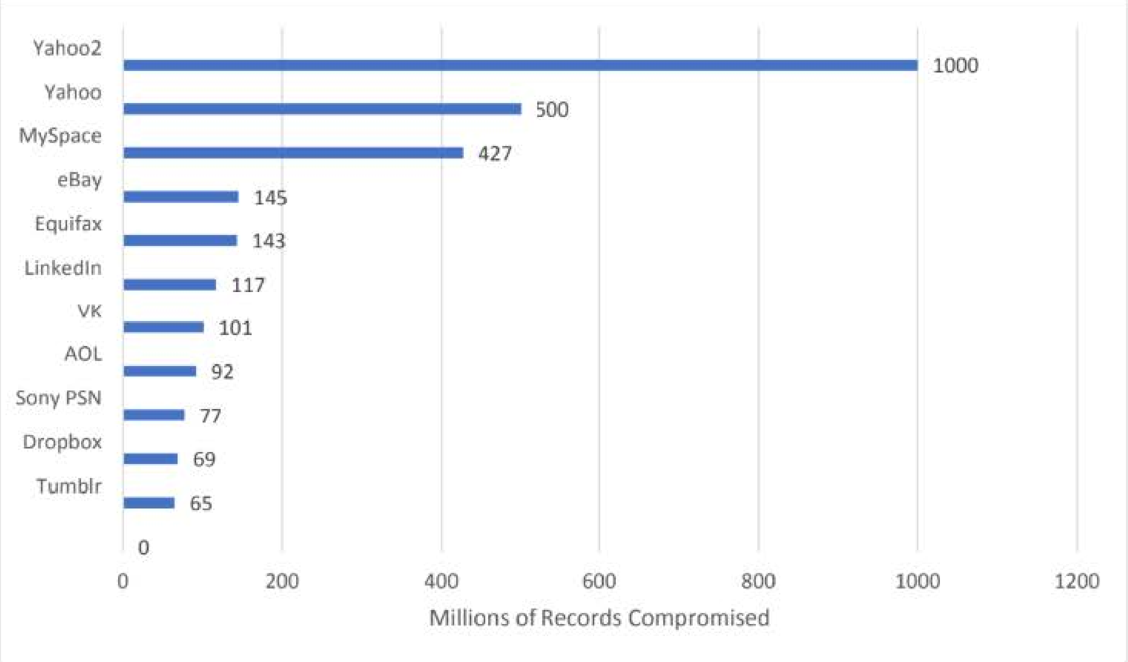
Exhibit 1 Denial of Service Attacks Explained (continued)

The most sophisticated denial-of-service attacks target other parts of source codes used by companies' websites. In one advanced case, many computers send requests to many *other* computers. However, by using IP (Internet Protocol) spoofing, the source address of these many other computers is set to the *target's* address, causing replies to go to the target address and flood it. This is called a Distributed *Reflected* denial-of-service, or DrDoS, attack.



Source: Casewriters.

Exhibit 2 A History of Large Data Breaches



Source: Casewriters.