6

Unwilling Accomplices

How Spammers Mask Their Identities Using Email Relaying

IN THIS CHAPTER

- **Blocked Because of Relay**
- **Knowing Where to Look**
- **The Syndicate**
- **Return to Sender**

In Chapter 5, "Would the Real Sender Please Stand Up?" you saw how attackers can easily spoof their email addresses and give the appearance that an email is from someone else. However, the email headers tell the true tale if you know where to look. In this chapter, you see how a misconfigured email server can take away the advantage of header information. If an email server is vulnerable to a relay attack, the email really comes from the vulnerable server and is not spoofed.

This chapter is all about how email attackers can use innocent people. By hiding behind innocent people, spammers take on less of the risk, and the innocents pay the price. In this chapter, you learn how to protect yourself from being used as an unwilling pawn in a spammer's attack.

Blocked Because of Relay

When an email server isn't configured properly or is misconfigured, it could be vulnerable to being abused by email attackers. In this section, you see how spammers can take advantage of this situation to send email messages that are traced back to the victim rather than the spammer.

Case Study 6-1

Lance sent an email to all his customers letting them know about a new promotion offering a significant discount. A short while later, he heard his email ding and checked to see whether it was one of his customers who wanted to make a purchase.

The email was about one of his customers, but not the email he was expecting. The email informed Lance that all email from his company was being blocked because of excessive spam emails. Lance knew his company used email to send messages to their customers, but it had strict policies about sending email only to users who requested it. Lance didn't want to lose this account, so he called his contact to resolve the issue.

His contact was happy to hear about the discounts and promised to look into the problem. Later that afternoon, his contact called back. He said the system administrators had gathered huge numbers of spam messages from Lance's company and were unwilling to release the blocks they had put into place. Lance promised to check with his technical staff to make sure they hadn't been sending these emails.

How the Attack Works

To understand how this attack works, first you need to know how email relaying works. As with most attacks, email relaying is based on abusing a legitimate technology and twisting the intended usage to meet the attacker's needs. Figure 6.1 shows the path of a typical email relay attack.

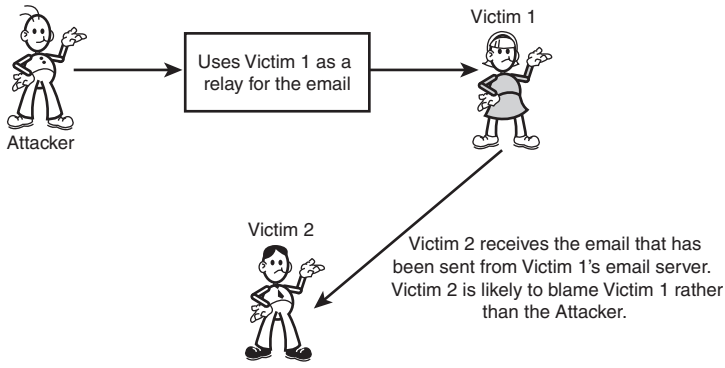

Figure 6.1 *The path of a relay attack.*

When Lance sends an email, it could be relayed through multiple email servers at his company. This relay process enables network administrators to route email traffic through certain servers, set up a redundancy process, and mask the internal network configuration. In the same way, his customer might have email routed through multiple servers when it arrives in his company's network. This use of relaying is acceptable and necessary to configure company networks properly.

The problem occurs when an email server is misconfigured and allows an outside attacker to relay email through the server. This can occur if the server isn't configured to limit what IP addresses can relay email through the server. Many email servers are preconfigured to allow relaying, so administrators often must take action to prevent unauthorized access.

The attacker simply configures his email software to route his emails through the IP address of the vulnerable email server so that all email messages appear to be coming from the victim instead of the attacker. This relaying gives the attacker a number of benefits—primarily, a level of anonymity. Instead of his email servers being blocked by blacklists, the only server that's blocked is the victim's. The attacker then simply moves on to another email relay and starts the process over.

Many costs associated with email relaying all fall on the victim. These costs include bandwidth use, storage capacity, and cleanup from the attack. This attack has the potential to crash servers if they aren't able to handle the traffic the attack generates.

An Ounce of Prevention

The responsibility for preventing this attack against email servers falls solely on the email administrator. The first step is ensuring that the email software has been upgraded and includes the latest security patches available. Older versions of email software can be difficult or impossible to configure to prevent email relay attacks.

The next step is to make sure the email server has been properly configured to prevent relay attacks. The specific steps vary widely for each email server and often for each version of the software. The basic premise is to make sure that only certain trusted servers are allowed to relay email through the server. When all servers are allowed to relay email, the server is wide open to relay attacks. For details on how to prevent this attack against your specific email server, see the following URL:

`http://mail-abuse.org/tsi/ar-fix.html`

A Pound of Cure

If you have already fallen victim to a relay attack, first you must take the necessary steps to prevent your system from being vulnerable. If you succeed in getting the blocks removed and the same attack is conducted again, getting the blocks lifted the next time might be difficult or impossible.

To get your system removed from a blacklist, you need to contact the list that's blocking your emails. Remember that your email messages might be blocked, so you need to use an alternative ISP or another means of communication. This process is specific to each list, and you might have different levels of success with each list. This process can also take a lot of time to resolve, so taking a proactive approach can be beneficial.

Checklist

- ✔ Upgrade email software to the latest version.
- ✔ Ensure that all security patches have been made to the operating system and email server.
- ✔ Configure the server to ensure that only trusted sources can relay email through the server.
- ✔ Contact the blocking list and inform them of the steps you have taken.

Knowing Where to Look

Locating a Web server on the Internet is often the easiest task in the world. Type in `www.<anyword>.com`, and you'll probably land on a valid Web site. Finding an email server might take a little more effort, but it's still a simple task. If an email server is exposed on the Internet, it's just a matter of time until an attacker locates it.

Case Study 6-2

Arnold was on a mission to get a job with a company that made computer games. He wasn't completely sure how to go about this, but he knew a few tricks and had plenty of resources on the Internet to help him. He had tried to get hired at the biggest gaming company, ILTPG Inc., but he didn't have enough experience.

Arnold knew he was better than most of the ILTPG employees and decided to pull a scam to get the job he wanted. He went to ILTPG's main competitor, Sore Thumbs. On his resume, he indicated that he had worked at ILTPG for several years. He figured that because Sore Thumbs was a competitor, his references might not be checked as closely.

Arnold was wrong. Sore Thumbs was impressed with his fabricated resume, but wanted a reference from ILTPG. Arnold thought quickly. He decided if he could send an email from ILTPG to Sore Thumbs with glowing information about Arnold's skills, he might just pull this off. Arnold realized that Sore Thumbs would probably detect a simple spoof right off the bat, so he decided to relay the attack through the ILTPG email server. However, the main server wasn't vulnerable to a relay attack. Not a problem for Arnold. He simply searched their network for another server. He figured that a company as big as ILTPG must have a number of other email servers that could be exploited.

How the Attack Works

The process of finding email servers is not difficult. It involves two steps. First, determine the IP addresses that belong to the company or organization being scanned. Often, this scanning can be done by simply querying the WHOIS database to determine what IP addresses have been assigned to that company. Go to the following URL:

```
http://ws.arin.net/cgi-bin/whois.pl
```

Enter your IP address and look at the result. If it says that your OrgName is the Internet Assigned Numbers Authority and "This block is reserved for special purposes," you have supplied an internal, nonroutable address. You need to enter the IP address you have on the Internet. If you don't know

that IP address, go to the following URL, which displays your IP address and attempts to show you where that IP address is physically located:

```
http://www.geobytes.com/IpLocator.htm?GetLocation
```

When you enter your IP address into the WHOIS page, you'll probably see your company or ISP information displayed. A range of IP addresses is also displayed that shows what IP addresses have been assigned to your company or ISP. This information gives you a good starting point for which IP addresses you can check for additional mail servers.

The next step is determining which of those IP addresses include servers running email software. Typically, you use a port scan to find this information. There are numerous port scanning tools. I often use Nmap for my security work. A typical Nmap run might look like this:

```
% nmap -p 25 -v -v 192.168.0.64 192.168.0.65 192.168.0.66
192.168.0.67

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
No TCP, UDP, or ICMP scantype specified,
assuming vanilla tcp connect() scan.
Use -sP if you really don't want to portscan
(and just want to see what hosts are up).
Machine 192.168.0.66 MIGHT actually be listening on probe
port 80
Machine 192.168.0.67 MIGHT actually be listening on probe
port 80

Host  (192.168.0.64) appears to be down, skipping it.

Host victim2 (192.168.0.65) appears to be up ... good.
Initiating Connect() Scan against victim2 (192.168.0.65)
The Connect() Scan took 0 seconds to scan 1 ports.
The 1 scanned port on victim2 (192.168.0.65) is: closed

Host victim3 (192.168.0.66) appears to be up ... good.
Initiating Connect() Scan against victim3 (192.168.0.66)
Adding open port 25/tcp
The Connect() Scan took 0 seconds to scan 1 ports.
Interesting ports on victim3 (192.168.0.66):
Port       State       Service
25/tcp     open        smtp

Host victim4 (192.168.0.67) appears to be up ... good.
Initiating Connect() Scan against victim4 (192.168.0.67)
Adding open port 25/tcp
The Connect() Scan took 0 seconds to scan 1 ports.
Interesting ports on victim4 (192.168.0.67):
```

```
Port        State       Service
25/tcp      open        smtp

Nmap run completed -- 4 IP addresses (3 hosts up) scanned
in 2 seconds
```

From this port scan, you can see that the first machine isn't running and the second machine isn't running an email SMTP server on the standard port. However, the next two machines are running an email server and could be tested to see whether they are vulnerable to a relay attack.

Finally, remember that when email messages are sent. the server information is stored in the email header. By viewing the headers of email messages sent from the company, you might be able to determine other email servers as well. If those email servers are exposed to the Internet, they can be probed to determine whether they are vulnerable to a relay attack.

An Ounce of Prevention

Before you can lock down all the email servers on your network, you need to know what email servers you have. In some cases, this information might seem straightforward, but in larger organizations, often it's difficult to keep track of all the servers, what's installed on them, and how they are used. Knowing which products or operating systems include a mail server is an important piece of the puzzle. Sometimes a system can act as a mail server, even though that's not the machine's intended use.

To limit your exposure to relay attacks, treat all email servers the same. If all email servers have the latest patches and are configured to protect against relay attacks, the risk of a development or test email server being exposed to the public is lessened greatly. The idea is that no one can get to the development mail server, but if attackers do, they won't be able to relay through the server because it's configured correctly.

Use your firewall to restrict access to all mail servers that don't need to be on the Internet. Although this restricted access is normal behavior for most companies and ISPs, having gaps in the network is common. A server might be on the Internet to handle Web traffic, but does it need to handle email requests? Set firewall rules to be as restrictive as possible.

A Pound of Cure

If you have already been hit with a relay attack, the first step is to secure the misconfigured machines as quickly as possible. Until that is done, you can't deal with the other repercussions.

If the attacked mail server was blocked but is used by only a small segment of the company, such as a particular team, simply giving the machine a new IP address within your range might be simpler than trying to get the block released. You can certainly use this strategy as a fallback position if getting the block released is proving difficult.

Checklist

- ✔ Know what email servers are deployed, including test or development servers.
- ✔ Make sure that all email servers are configured properly with the latest patches.
- ✔ Make sure firewalls block access to internal servers that don't need external access.
- ✔ If necessary, change IP addresses on additional mail servers to get around blocks. This change should be done only after the fixes are in place.

The Syndicate

By themselves, spam, viruses, Trojan horses, and hackers are serious threats that can be difficult to defend against. Think of them as Catwoman, the Joker, the Penguin, and the Riddler from the old *Batman* show. Alone, each villain was a formidable threat for the Dynamic Duo. However, in the *Batman* movie, the criminal masterminds teamed up to take on Batman and Robin. This chapter considers what happens when spammers, virus writers, Trojan horse authors, and hackers team up to defeat your defenses.

Case Study 6-3

Carl remembered the first time he created a virus. He was still in school and had done it just to see if he could. The virus caused some minor damage at the school, but didn't spread very far.

How things had changed since then. Now Carl was creating a virus and actually getting paid to do it. This virus was intended to infect computers and configure them to send out spam messages. By having access to a large number of zombie machines to relay spam through, the spammers could mask their identities and continue their assault.

The spammer who ordered this virus was very specific about what he wanted the software to do and how it needed to avoid detection. Viruses and spam had come together to enable each other and had become big business at the same time. Carl wasn't sure about all the implications, but his paycheck would pay for some new computer gear, and that was cool with him.

Case Study 6-4

Wendy had a letter from her ISP informing her that her cable modem contract would be terminated at the end of the month. The ISP accused her of using her cable modem connection to send spam and other unwanted email messages. Wendy had never done anything like that before. She and her family got a lot of use from the cable modem and having to go back to dial-up wasn't a welcome thought.

When Wendy called, the cable company employee told her that if she wasn't intentionally sending the emails, possibly her computer was being used as a zombie to send out spam. The employee asked if she had installed a firewall. Wendy hadn't and wasn't exactly sure what one was. The cable employee recommended that she purchase a firewall from the software store. However, her contract to use the cable modem stated that her usage could be terminated if she didn't take steps to secure her machine, so the decision to terminate the contract would still stand.

How the Attack Works

Hackers, virus writers, and spammers working together is one of the most dangerous trends in email security. It opens up all sorts of new and more threatening attacks than have ever been possible. Although these groups might have different agendas and goals, ultimately attacks by one group can be used to benefit the others. A spam message can be used to carry a virus that opens a connection on your PC that allows a hacker to break in. The hacker can then allow a spammer to use the collection of exploited or zombie machines to send out spam and viruses with a small chance of detection.

The growing trend toward broadband connections has made it easier for attackers to exploit home users. When users connect through a dial-up connection, their IP addresses typically change each time they connect. For example, if an ISP has IP addresses from 200.182.33.0 to 200.182.33.255, a dial-up user might get the following IP address when he or she connects:

- 200.182.33.14
- 200.182.33.43
- 200.182.33.231
- 200.182.33.187
- 200.182.33.82

For broadband users, their IP addresses usually remain constant or at least stay the same for long periods. This means if a machine with a broadband connection is compromised, an attacker can use that machine, knowing what its IP address will be the next time he needs to access it.

Broadband machines also tend to fall within distinct ranges of IP addresses. By concentrating on the IP address ranges broadband companies use for their customers, attackers can quickly locate a large number of target machines.

Unlike corporate users, home users typically don't have the resources or expertise at their disposal to deal with the security issues related to connecting a machine to the Internet. The result is that many home PCs are vulnerable to this attack and give attackers a network of machines that grants them anonymous, high-speed access to the Internet.

An Ounce of Prevention

All home users should install two pieces of software. One is a virus protection package. Modern virus protection software can be used to detect not

only viruses, but also malicious code, such as certain worms and Trojan horses.

Home users, especially those with broadband connections, should also install a firewall, which is simply a program that restricts how your computer is connected to other computers or, in this case, connected to the Internet. Without a firewall, you're dependent on having the latest security patches installed, making sure every tool is configured perfectly, and ensuring that none of your software has any security vulnerabilities. Meeting all those goals would be difficult for anyone, so a firewall provides a safety net. You can allow only certain computers to access yours or restrict Internet access to specific programs. This type of control makes it difficult for a Trojan horse to gain a foothold.

> ***If you run a wireless network, you need to protect yourself from the Internet as well as from anyone in proximity of your home. Sitting here at my desk, I can pick up two wireless networks that neighbors are running. If those networks aren't secured, I could gain access to their computers without their knowledge. With wireless, the network doesn't stop at the walls of your home, but extends outward in a fashion that you can't control. Default passwords need to be reset and encryption should be enabled on wireless networks.***

Finally, make sure to install all the latest patches and updates. This advice applies not only to your operating system, but also to your virus protection and firewall packages. Many computers are exploited every day because of problems that are well known but haven't been addressed.

A Pound of Cure

If your computer has already been taken over, a firewall and virus protection are the correct measures to seize control. In this case, getting some outside help might be best to ensure that you take all the proper steps. Malicious code needs to be purged from the system, including any disks, CDs, or backups. A firewall should be set up to restrict access to the computer, and virus protection should be run to ensure that no other malicious code is present. Passwords should be reset to make sure they haven't been compromised.

Also, be sure to report this attack to your ISP or corporate security department. By knowing what you have run into, they might be able to offer additional assistance to make sure the problem is solved. They also are in

a position to see the bigger picture. For example, they might realize that this attack is actually part of a broader attack against the same ISP or company.

Checklist

- ✔ Install a firewall on all machines that connect to the Internet.
- ✔ Make sure your firewall is configured to restrict access to your network as much as possible.
- ✔ Install virus protection software and keep it up to date.
- ✔ Make sure the latest security patches are installed.
- ✔ Report any suspicious activity to your ISP or corporate security department.

Return to Sender

Sometimes the victim of a spam attack isn't the person who receives the email but an innocent bystander. When a spammer forges a Reply-To header, all the bouncebacks and negative feedback are sent to victims rather than the spammer. Most recipients of these spam messages mistakenly direct their anger and frustration at the wrong target.

Case Study 6-5

Nancy came into work and started her email client. It was taking a long time to start up and Nancy was late for a meeting, so she left it on and headed off to her status meeting. When she returned, she saw something on her screen she had never seen before: 2,191 email messages in her inbox. Nancy didn't realize she could have that much email in her inbox at one time. Most of the messages seemed to have the same subject line: "RE: How to get filthy rich in just 2 weeks!!!" Nancy figured it was a major spam attack, but when she looked at some of the emails, they didn't look like any spam she had ever seen.

Many of the emails were automated responses that indicated why the recipient hadn't received the email. These reasons included the inbox being full, the user not having an active account, or the server having a communication problem.

Nancy also discovered a group of emails stating, in extremely derogatory terms, what the recipients thought of Nancy, her lineage, and the spam she was peddling. Finally, there were a few orders for a get-rich-quick brochure that included people's names, addresses, and credit card numbers.

For some reason, all these people seemed to think that Nancy had sent this spam, even though she had never done anything like this. Nancy hoped the problem would go away. She didn't want to know what would happen if she kept getting that many email messages every day.

How the Attack Works

In Chapter 5, you saw how easy it is for email attackers to spoof email headers and send email claiming to be from other users. The "Joe Job" attack described in this case study is just as simple; it involves changing a different header line from the one used for spoofing. In spoofing, the From header is altered; in the Joe Job attack, the Reply-To header is modified.

> *In 1996, Joe Doll, the owner of Joes.com, a hosting company, killed a user's account who was spamming other users. The spammer got back at Joe by sending millions of spam messages, but in each one, he spoofed the return email address to make it look like Joe Doll was sending the spam. The people who were spammed overwhelmed Joe's inbox with angry complaints and eventually caused a denial of service of the Joes.com server. Since then, any attack in which the sender spoofs the return address to attack another person is known as a "Joe Job."*

Joe Job attacks can cause a lot of problems for the person who's targeted. Attackers mask their identity and let the victim take the brunt of any bouncebacks or upset users. To mask their identity, they simply place the victim's email address in the spam message's Reply-To header and then send the email to a list of targets. Any replies from targeted recipients go to the victim rather than the attacker. If the attacker is selling a product, he usually provides a link to a Web site to purchase the product because he won't see the email traffic coming back.

If there was any doubt as to the true character of spammers, this attack should put those doubts to rest. Spammers are not entrepreneurs just trying to make an honest buck. The concept of setting up an innocent bystander to take the punishment for their spam isn't a technique you'll find in books about best business practices. Spammers are attackers, just like hackers and virus writers, and should be treated the same.

An Ounce of Prevention

As discussed extensively in Chapter 1, "Stealing Candy from a Baby: How Spammers Harvest Email Addresses," be cautious with your email address. You can reduce your chances of being targeted for a Joe Job attack by not placing your email address on your Web site, not using it to sign up for things on the Web, and giving it out only to people who need it. You could be randomly selected by an attacker, but at least in that case, the chances of being repeatedly attacked are lower.

Try to fly under the radar when dealing with spammers. Although receiving spam messages can be frustrating, be careful not to resort to their tactics in dealing with them. From time to time, people recommend using vigilante-style justice to deal with spammers and hackers. This response might be tempting, but more often than not, it simply results in more targeted attacks.

A Pound of Cure

If you are under a Joe Job attack, the best way to deal with it is to add a filter that deletes the email messages being directed at you from the spam message. Typically, the numbers of emails are very high at first and then begin to taper off as time goes on. If you can weather the initial hit and get a filter in place to make the attack more manageable, you can usually get through it without too much trouble.

You should definitely report this attack to your ISP or corporate security department. If it's an isolated case, there's nothing they can do. However, if it becomes a regular pattern, they might be able to add some upstream filtering or even track down the source of the problem for you.

Checklist

- ✔ Be cautious with your email address.
- ✔ Avoid becoming a target by taking retaliatory action against a spammer.
- ✔ If you're being hit with a Joe Job attack, add a filter to delete the emails being returned.
- ✔ Report these attacks to your ISP or corporate security department.

Summary

In this chapter, you have seen how a misconfigured email server can take away the one piece of information that detects a spoofing attack: the header information. If an email server is vulnerable to a relay attack, the email really comes from the vulnerable server and doesn't require spoofing by the attacker.

Email attackers often hide behind innocent people to reduce their risk, and the innocents pay the price. For example, relay attacks can be used to direct spam through your email server, and attackers can locate email servers running on your network. You have also learned about Joe Job attacks, in which spam is sent with a victim's email address in the Reply-To header.

One of the biggest risks to the Internet is when virus writers, hackers, and spammers work together. The attacks described in this chapter show why retaliation is not an option against spammers and other email attackers. Many times, innocent users pay the price.