Chapter 2

Getting to Know Common Cyberattacks

IN THIS CHAPTER

» Exploring attacks that can inflict damage

» Discovering the difference between impersonation, data interception, and data theft

» Looking at the various types of malware, poisoning, and malvertising

» Understanding how cyberattackers exploit the challenges of maintaining complex technology infrastructures

» Finding out about forms of advanced cyberattacks

Many different types of cyberattacks exist — so many that I could write an entire series of books about them. In this book, however, I do not cover all types of threats in detail because the reality is, that you're likely reading this book to learn about how to keep yourself cybersecure, not to learn about matters that have no impact on you, such as forms of attacks that are normally directed at espionage agencies, industrial equipment, or military armaments.

In this chapter, you find out about the different types of problems that cyberattackers can create through the use of attacks that commonly impact individuals and small businesses.

Attacks That Inflict Damage

Attackers launch some forms of cyberattacks with the intent to inflict damage to victims. The threat posed by such attacks is not that a criminal will directly steal your money or data, but that the attackers will inflict harm to you in some other specific manner — a manner that may ultimately translate into financial, military, political, or other benefit to the attacker and (potentially) damage of some sort to the victim.

Types of attacks that inflict damage include

- Denial-of-service (DoS) attacks
- Distributed denial-of-service (DDoS) attacks
- Botnets and zombies
- Data destruction attacks

Denial-of-service (DoS) attacks

A *denial-of-service attack* is one in which an attacker intentionally attempts to paralyze a computer or computer network by flooding it with large amounts of requests or data, which overload the target and make it incapable of responding properly to legitimate requests.

In many cases, the requests sent by the attacker are each, on their own, legitimate — for example, a normal request to load a web page.

In other cases, the requests aren't normal requests. Instead, they leverage knowledge of various protocols to send requests that optimize, or even magnify, the effect of the attack.

In any case, denial-of-service attacks work by overwhelming computer systems' Central Processing Units (CPU)s and/or memory, utilizing all the available network communications bandwidth, and/or exhausting networking infrastructure resources such as routers.

Distributed denial-of-service (DDoS) attacks

A *Distributed DoS attack* is a DoS attack in which many individual computers or other connected devices across disparate regions simultaneously flood the target with requests. In recent years, nearly all major denial-of-service attacks have been distributed in nature — and some have involved the use of Internet-connected cameras and other devices as attack vehicles, rather than classic computers. Figure 2-1 illustrates the anatomy of a simple DDoS attack.

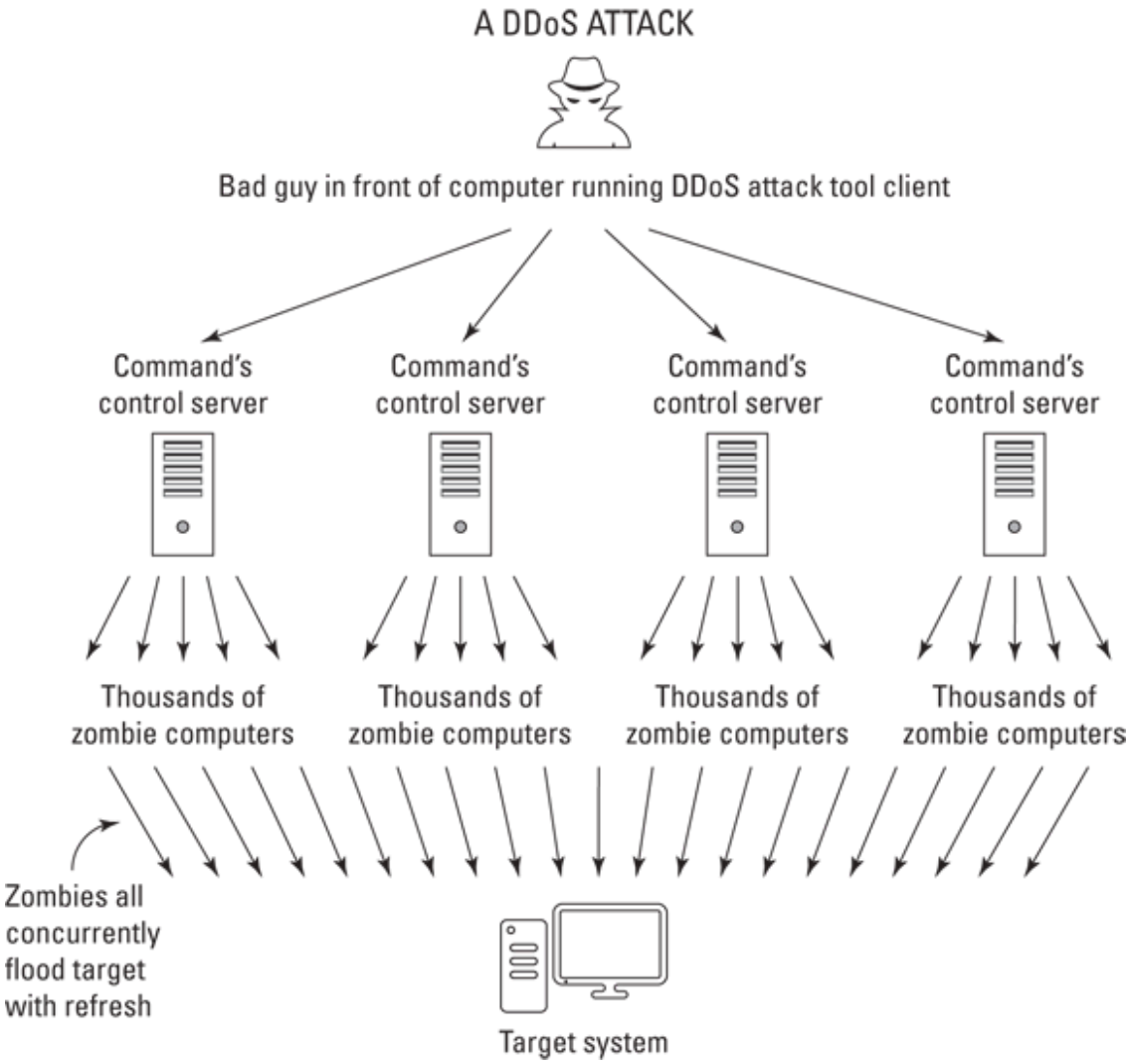

FIGURE 2-1: A DDoS attack.

The goal of a DDoS attack is to knock the victim offline, and the motivation for doing so varies.

Sometimes the goal is financial: Imagine, for example, the damage that may result to an online retailer's business if an unscrupulous competitor knocked the former's site offline during Black Friday weekend. Imagine a crook who shorts the stock of a major retailer of toys right before launching a DDoS attack against the retailer two weeks before Christmas.

DDoS attacks remain a serious and growing threat. Criminal enterprises even offer DDoS for hire services, which are advertised on the dark web as offering, for a fee, to "take your competitor's websites offline in a cost-effective manner."

In some cases, DDoS launchers may have political, rather than financial, motives. For example, a corrupt politician may seek to have his or her opponent's website taken down during an election season, thereby reducing the competitor's ability to spread messages and receive online campaign contributions. Hacktivists may also launch DDoS attacks in order to take down sites in the name of "justice" — for example, targeting law enforcement sites after an unarmed person is killed during an altercation with police.

In fact, according to a 2017 study by Kaspersky Lab and B2B International, almost half of companies worldwide that experienced a DDoS attack suspect that their competitors may have been involved.

DDoS attacks can impact individuals in three significant ways:

- **A DDoS attack on a local network can significantly slow down all Internet access from that network.** Sometimes these attacks make connectivity so slow that connections to sites fail due to *session timeout* settings, meaning that the systems terminate the connections after seeing requests take longer to elicit responses than some maximum permissible threshold.
- **A DDoS attack can render inaccessible a site that a person plans on using.** On October 21, 2016, for example, many users were unable to reach several high-profile sites, including Twitter, PayPal, CNN, HBO Now, The Guardian, and dozens of other popular sites, due to a massive DDoS attack launched against a third party providing various technical services for these sites and many more.

  

  TIP The possibility of DDoS attacks is one of the reasons that you should never wait until the last minute to perform an online banking transaction — the site that you need to utilize may be inaccessible for a number of reasons, one of which is an ongoing DDoS attack.
- **A DDoS attack can lead users to obtain information from one site instead of another.** By making one site unavailable, Internet users looking for specific information are likely to obtain it from another site — a phenomenon that allows attackers to either spread misinformation or prevent people from hearing cer-

tain information or vantage points on important issues. As such, DDoS attacks can be used as an effective mechanism — at least over the short term — for censoring opposing points of view.

Botnets and zombies

Often, DDoS attacks use what are known as *botnets.* Botnets are a collection of compromised computers that belong to other parties, but that a hacker remotely controls and uses to perform tasks without the legitimate owners' knowledge.

Criminals who successfully infect one million computers with malware can, for example, potentially use those machines, known as *zombies,* to simultaneously make many requests from a single server or server farm in an attempt to overload the target with traffic.

Data destruction attacks

Sometimes attackers want to do more than take a party temporarily offline by overwhelming it with requests — they may want to damage the victim by destroying or corrupting the target's information and/or information systems. A criminal may seek to destroy a user's data through a *data destruction attack* — for example, if the user refuses to pay a ransomware ransom that the crook demands.

Of course, all the reasons for launching DDoS attacks (see preceding section) are also reasons that a hacker may attempt to destroy someone's data as well.

Wiper attacks are advanced data destruction attacks in which a criminal uses malware to wipe the data on a victim's hard drive or SSD, in such a fashion that the data is difficult or impossible to recover.

To put it simply, unless the victim has backups, someone whose computer is wiped by a wiper is likely to lose access to all the data and software that was previously stored on the attacked device.

Impersonation

One of the great dangers that the Internet creates is the ease with which mischievous parties can impersonate others. Prior to the Internet era, for example, criminals could not easily impersonate a bank or a store and convince people to hand over their money in exchange for some promised rate of interest or goods. Physically mailed letters and later telephone calls became the tools of scammers, but none of those earlier communication techniques ever came close to the power of the Internet to aid criminals attempting to impersonate law-abiding parties.

Creating a website that mimics the website of a bank, store, or government agency is quite simple and can sometimes be done within minutes. Criminals can find a near-endless supply of domain names that are close enough to those of legitimate parties to trick some folks into believing that a site that they are seeing is the real deal when it's not, giving crooks the typical first ingredient in the recipe for online impersonation.

WARNING Sending an email that appears to have come from someone else is simple and allows criminals to perpetrate all sorts of crimes online. I myself demonstrated over 20 years ago how I could defeat various defenses and send an email that was delivered to recipients on a secure system — the message appeared to readers to have been sent from `god@heaven.sky`. Figure 2-2 shows another email message that may have been faked.

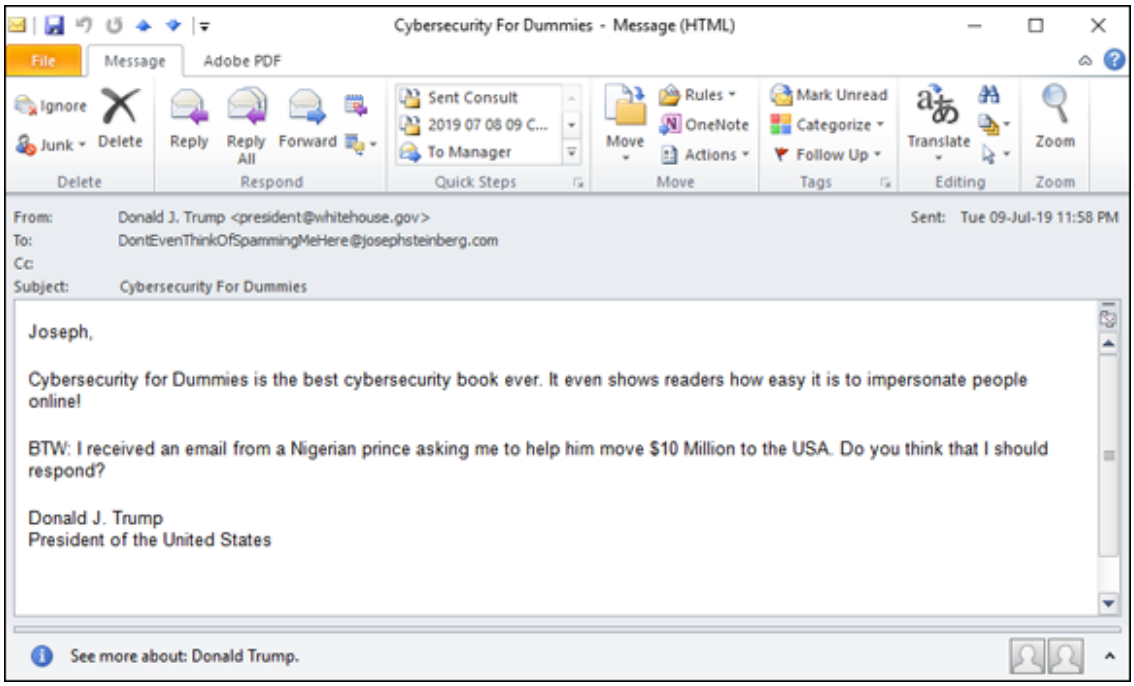

FIGURE 2-2: An impersonation message.

Phishing

Phishing refers to an attempt to convince a person to take some action by impersonating a trustworthy party that reasonably may legitimately ask the user to take such action.

For example, a criminal may send an email that appears to have been sent by a major bank and that asks the recipient to click on a link in order to reset his or her password due to a possible data breach. When the user clicks the link, he or she is directed to a website that appears to belong to the bank, but is actually a replica run by the criminal. As such, the criminal uses the fraudulent website to collect usernames and passwords to the banking site.

Spear phishing

Spear phishing refers to phishing attacks that are designed and sent to target a specific person, business, or organization. If a criminal seeks to obtain credentials into a specific company's email system, for example, he or she may send emails crafted specifically for particular targeted individuals within the organization. Often, criminals who spear phish research their targets online and leverage overshared information on social media in order to craft especially legitimate-sounding emails.

For example, the following type of email is typically a lot more convincing than "Please login to the mail server and reset your password.":

> *"Hi, I am going to be getting on my flight in ten minutes. Can you please login to the Exchange server and check when my meeting is? For some reason, I cannot get in. You can try to call me by phone first for security reasons, but, if you miss me, just go ahead, check the information, and email it to me — as you know that I am getting on a flight that is about to take off."*

CEO fraud

CEO fraud is similar to spear phishing (see preceding section) in that it involves a criminal impersonating the CEO or other senior executive of a particular business, but the instructions provided by "the CEO" may be to take an action directly, not to log in to a system, and the goal may not be to capture usernames and passwords or the like.

The crook, for example, may send an email to the firm's CFO instructing her or him to issue a wire payment to a particular new vendor or to send all the organization's W2 forms for the year to a particular email address belonging to the firm's accountant. See Figure 2-3.

CEO fraud often nets significant returns for criminals and makes employees who fall for the scams appear incompetent. As a result, people who fall prey to such scams are often fired from their jobs.

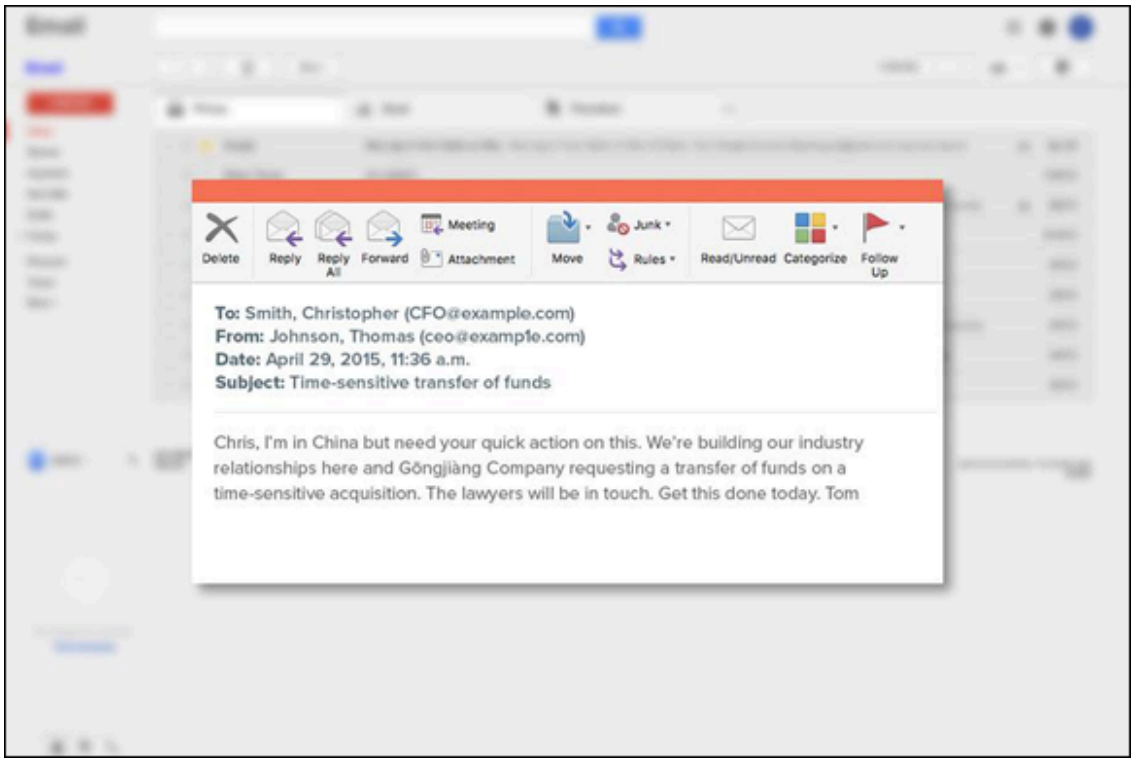

FIGURE 2-3: A fraudulent email.

Smishing

Smishing refers to cases of phishing in which the attackers deliver their messages via text messages (SMS) rather than email. The goal may be to capture usernames and passwords or to trick the user into installing malware.

Vishing

Vishing, or voice-based phishing, is phishing via POTS — that stands for "plain old telephone service." Yes, criminals use old, time-tested methods for scamming people. Today, most such calls are transmitted by Voice Over IP systems, but, in the end, the scammers are calling people on regular telephones much the same way that scammers have been doing for decades.

Whaling

Whaling refers to spear phishing that targets high-profile business executives or government officials. For more on spear phishing, see the section earlier in this chapter.

Tampering

Sometimes attackers don't want to disrupt an organization's normal activities, but instead seek to exploit those activities for financial gain. Often, crooks achieve such objectives by manipulating data in transit or as it resides on systems of their targets in a process known as *tampering*.

In a basic case of tampering with data in transit, for example, imagine that a user of online banking has instructed his bank to wire money to a particular account, but somehow a criminal intercepted the request and changed the relevant routing and account number to his own.

A criminal may also hack into a system and manipulate information for similar purposes. Using the previous example, imagine if a criminal changed the payment address associated with a particular payee so that when the Accounts Payable department makes an online payment, the funds are sent to the wrong destination (well, at least it is wrong in the eyes of the payer).

Interception

Interception occurs when attackers capture information in transit between computers. If the data isn't properly encrypted, the party intercepting it may be able to misuse it.

One special type of interception is known as a *man-in-the-middle attack*. In this type of an attack, the interceptor proxies the data between the sender and recipient in an attempt to disguise the fact that the data is being intercepted. *Proxying* in such a case refers to the man-in-the-middle intercepting requests and then transmitting them (either in modified form or unmodified) to their original intended destinations and then receiving the responses from those destination and transmitting them (in modified form or unmodified) back to the sender. By employing proxying, the man-in-the-middle makes it difficult for the sender to know that his communications are being intercepted because when he communicates with a server, he receives the responses that he expects.

For example, a criminal may set up a bogus bank site (see the earlier "Phishing" section) and relay any information that anyone enters on the bogus site to the actual bank site so that the criminal can respond with the same information that the legitimate bank would have sent. Proxying of this sort not only helps the criminal avoid detection — a user who provides the crook with his or her password and then performs his or her normal online banking tasks may have no idea that anything abnormal occurred during the online banking session — but, also helps the criminal ensure that he or she captures the right password. If a user enters an incorrect password, the criminal will know to prompt for the correct one.

Figure 2-4 shows the anatomy of a man-in-the-middle intercepting and relaying communications.

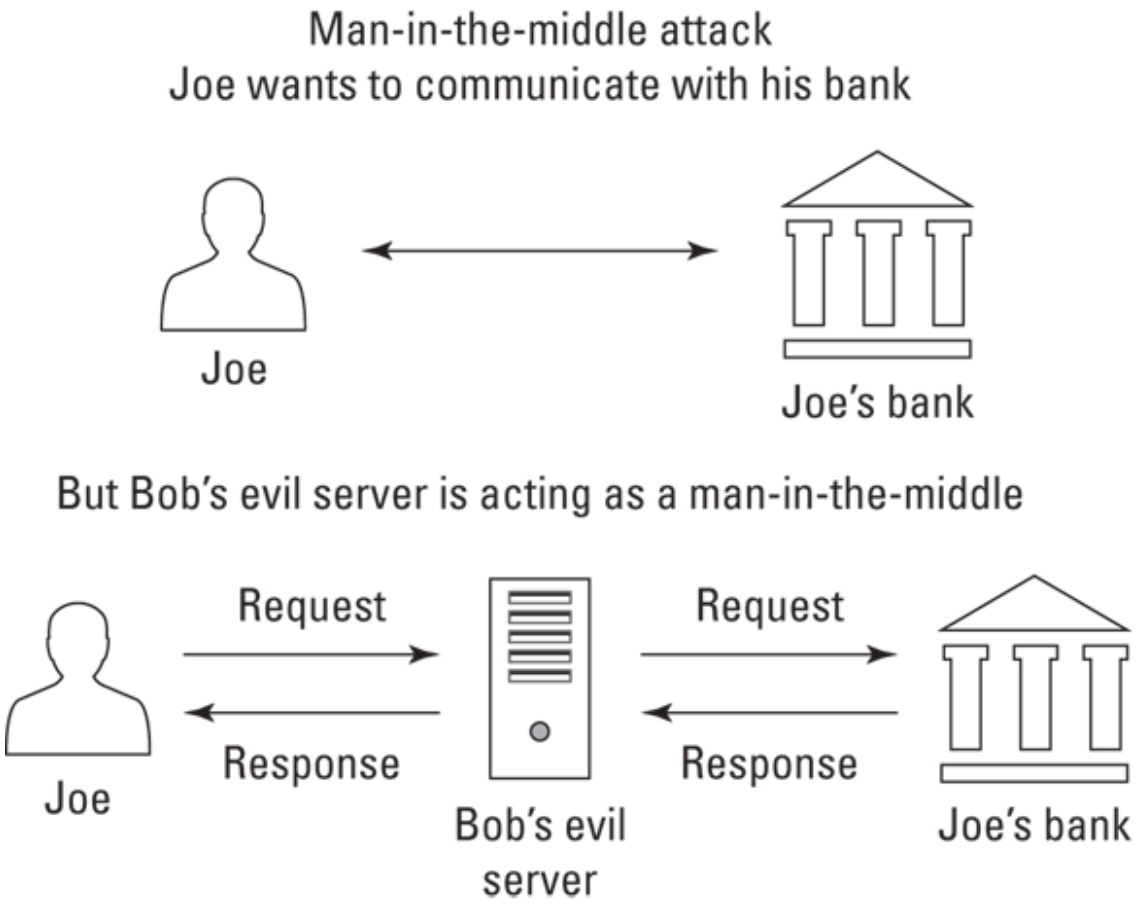

FIGURE 2-4: A man-in-the-middle interception.

Data Theft

Many cyberattacks involve stealing the victim's data. An attacker may want to steal data belonging to individuals, businesses, or a government agency for one or more of many possible reasons.

People, businesses, nonprofits, and governments are all vulnerable to data theft.

Personal data theft

Criminals often try to steal people's data in the hope of finding items that they can monetize, including:

- Data that can be used for identity theft or sold to identity thieves
- Compromising photos or health-related data that may be sellable or used as part of blackmail schemes
- Information that is stolen and then erased from the user's machine that can be ransomed to the user
- Password lists that can be used for breaching other systems
- Confidential information about work-related matters that may be used to make illegal stock trades based on insider information
- Information about upcoming travel plans that may be used to plan robberies of the victim's home

Business data theft

Criminals can use data stolen from businesses for a number of nefarious purposes:

- **Making stock trades:** Having advance knowledge of how a quarter is going to turn out gives a criminal insider information on which he or she can illegally trade stocks or options and potentially make a significant profit.
- **Selling data to unscrupulous competitors:** Criminals who steal sales pipeline information, documents containing details of future products, or other sensitive information can sell that data to unscrupulous competitors or to unscrupulous employees working at competitors whose management may never find out how such employees suddenly improved their performance.
- **Leaking data to the media:** Sensitive data can embarrass the victim and cause its stock to decline (perhaps after selling short some shares).
- **Leaking data covered by privacy regulations:** The victim may be potentially fined.
- **Recruiting employees:** By recruiting employees or selling the information to other firms looking to hire employees with similar skills or with knowledge of competitions' systems, criminals who steal emails and discover communication between employees that indicates that one or more employees are unhappy in their current positions can sell that information to parties looking to hire.

- **Stealing and using intellectual property:** Parties that steal the source code for computer software may be able to avoid paying licensing fees to the software's rightful owner. Parties that steal design documents created by others after extensive research and development can easily save millions of dollars — and, sometimes, even billions of dollars — in research and development costs. For more on the effects of this type of theft, see the nearby sidebar "How a cyberbreach cost one company $1 billion without 1 cent being stolen."

HOW A CYBERBREACH COST ONE COMPANY $1 BILLION WITHOUT 1 CENT BEING STOLEN

Theft of intellectual property (IP), such as confidential design documents and computer source code, is an extremely serious matter and a growing area of cybercrime.

For example, in 2007, the Massachusetts-based technology firm American Superconductor, which manufactured software to control wind turbines, partnered with Sinovel, a Chinese firm that manufactured wind turbines, to start selling the turbines in China.

In 2011, Sinovel suddenly refused to pay American Superconductor $70 million that it owed the firm and began to sell turbines with its own software. An investigation revealed that Sinovel had illegally obtained the IP of American Superconductor by bribing a single employee at the American firm to help it steal the source code.

American Superconductor nearly went bankrupt as a result, declined in value by more than $1 billion, and had to let go of 700 employees, nearly half of its workforce.

Malware

Malware, or malicious software, is an all-encompassing term for software that intentionally inflicts damage on its users who typically have no idea that they are running it.

Malware includes computer viruses, worms, Trojans, ransomware, scareware, spyware, cryptocurrency miners, adware, and other programs intended to exploit computer resources for nefarious purposes.

Viruses

Computer viruses are instances of malware that, when executed, replicate by inserting their own code into computer systems. Typically, the insertion is in data files (for example, as rogue macros within a Word document), the special portion of hard drives or solid state drives that contain the code and data used to boot a computer or disk (also known as *boot sectors*), or other computer programs.

Like biological viruses, computer viruses can't spread without having hosts to infect. Some computer viruses significantly impact the performance of their hosts, while others are, at least at times, hardly noticeable.

While computer viruses still inflict tremendous damage worldwide, the majority of serious malware threats today arrive in the form of worms and Trojans.

Worms

Computer worms are stand-alone pieces of malware that replicate themselves without the need for hosts in order to spread. Worms often propagate over connections by exploiting security vulnerabilities on target computers and networks.

Because they normally consume network bandwidth, worms can inflict harm even without modifying systems or stealing data. They can slow down network connections — and few people, if any, like to see their internal and Internet connections slow down.

Trojans

Trojans (appropriately named after the historical Trojan horse) is malware that is either disguised as nonmalicious software or hidden within a legitimate, nonmalicious application or piece of digital data.

Trojans are most often spread by some form of social engineering — for example, by tricking people into clicking on a link, installing an app, or running some email attachment. Unlike viruses and worms, Trojans typi-

cally don't self-propagate using technology — instead, they rely on the effort (or more accurately, the mistakes) of humans.

Ransomware

Ransomware is malware that demands that a ransom be paid to some criminal in exchange for the infected party not suffering some harm.

Ransomware often encrypts user files and threatens to delete the encryption key if a ransom isn't paid within some relatively short period of time, but other forms of ransomware involve a criminal actually stealing user data and threatening to publish it online if a ransom is not paid.

Some ransomware actually steals the files from users' computers, rather than simply encrypting data, so as to ensure that the user has no possible way to recover his or her data (for example, using an anti-ransomware utility) without paying the ransom.

Ransomware is most often delivered to victims as a Trojan or a virus, but has also been successfully spread by criminals who packaged it in a worm. In recent years sophisticated criminals have even crafted targeted ransomware campaigns that leverage knowledge about what data is most valuable to a particular target and how much that target can afford to pay in ransoms.

Figure 2-5 shows the ransom demand screen of WannaCry — a flavor of ransomware that inflicted at least hundreds of millions of dollars in damage (if not billions), after initially spreading in May 2017. Many security experts believe that the North Korean government or others working for it created WannaCry, which, within four days, infected hundreds of thousands of computers in about 150 countries.

FIGURE 2-5: Ransomware demanding ransom.

Scareware

Scareware is malware that scares people into taking some action. One common example is malware that scares people into buying security software. A message appears on a device that the device is infected with some virus that only a particular security package can remove, with a link to purchase that "security software."

Spyware

Spyware is software that surreptitiously, and without permission, collects information from a device. Spyware may capture a user's keystrokes (in which case it is called a *keylogger*), video from a video camera, audio from a microphone, screen images, and so on.

It is important to understand the difference between spyware and invasive programs. Some technologies that may technically be considered spyware if users had not been told that they were being tracked online are in use by legitimate businesses; they may be invasive, but they are not malware. These types of *nonspyware that also spies* includes beacons that

check whether a user loaded a particular web page and tracking cookies installed by websites or apps. Some experts have argued that any software that tracks a smartphone's location while the app is not being actively used by the device's user also falls into the category of *nonspyware that also spies* — a definition that would include popular apps, such as Uber.

Cryptocurrency miners

Cryptocurrency miners are malware that, without any permission from devices' owners, commandeers infected devices' brainpower (its CPU cycles) to generate new units of a particular cryptocurrency (which the malware gives to the criminals operating the malware) by completing complex math problems that require significant processing power to solve.

The proliferation of cryptocurrency miners exploded in 2017 with the rise of cryptocurrency values. Even after price levels subsequently dropped, the miners are still ubiquitous as once criminals have invested in creating the miners, there is little cost in continuing to deploy them. Not surprisingly, as cryptocurrency prices began to rise again in 2019, new strains of cryptominers began to appear as well — some of which specifically target Android smartphones.

Many low-end cybercriminals favor using cryptominers. Even if each miner, on its own, pays the attacker very little, miners are easy to obtain and directly monetize cyberattacks without the need for extra steps (such as collecting a ransom) or the need for sophisticated command and control systems.

Adware

Adware is software that generates revenue for the party operating it by displaying online advertisements on a device. Adware may be malware — that is, installed and run without the permission of a device's owner — or it may be a legitimate component of software (for example, installed knowingly by users as part of some free, ad-supported package).

TIP Some security professionals refer to the former as *adware malware,* and the latter as adware. Because no consensus exists, it's best to clarify which of the two is being discussed when you hear someone mention just the generic term adware.

Blended malware

Blended malware is malware that utilizes multiple types of malware technology as part of an attack — for example, combining features of Trojans, worms, and viruses.

Blended malware can be quite sophisticated and often stems from skilled attackers.

Zero day malware

Zero day malware is any malware that exploits a vulnerability not previously known to the public or to the vendor of the technology containing the vulnerability, and is, as such, often extremely potent.

Regularly creating zero day malware requires significant resource and development. It's quite expensive and is often crafted by the cyber armies of nation states rather than by other hackers.

Commercial purveyors of zero day malware have been known to charge over $1 million for a single exploit.

Poisoned Web Service Attacks

Many different types of attacks leverage vulnerabilities in servers, and new weaknesses are constantly discovered, which is why cybersecurity professionals have full-time jobs keeping servers safe. Entire books — or even several series of books — can be written on such a topic, which is, obviously, beyond the scope of this work.

That said, it is important for you to understand the basic concepts of server-based attacks because some such attacks can directly impact you.

One such form of attack is a *poisoned web service attack*, or a *poisoned web page attack*. In this type of attack, an attacker hacks into a web server and inserts code onto it that causes it to attack users when they access a page or set of pages that the server is serving.

For example, a hacker may compromise the web server serving `www.abc123.com` and modify the home page that is served to users accessing the site so that the home page contains malware.

But, a hacker does not even need to necessarily breach a system in order to poison web pages!

If a site that allows users to comment on posts isn't properly secured, for example, it may allow a user to add the text of various commands within a comment — commands that, if crafted properly, may be executed by users' browsers any time they load the page that displays the comment. A criminal can insert a command to run a script on the criminal's website, which can receive the authentication credentials of the user to the original site because it is called within the context of one of that site's web pages. Such an attack is known as *cross site scripting*, and it continues to be a problem even after over a decade of being addressed.

Network Infrastructure Poisoning

As with web servers, many different types of attacks leverage vulnerabilities in network infrastructure, and new weaknesses are constantly discovered. The vast majority of this topic is beyond the scope of this book. That said, as is the case with poisoned web servers, you need to understand the basic concepts of server-based attacks because some such attacks can directly impact you.

For example, criminals may exploit various weaknesses in order to add corrupt domain name system (DNS) data into a DNS server.

DNS is the directory of the Internet that translates human readable addresses into their numeric, computer-usable equivalents (IP addresses). For example, if you type `https://JosephSteinberg.com` into your web browser, DNS directs your connection to an address of 104.18.45.53.

By inserting incorrect information into DNS tables, a criminal can cause a DNS server to return an incorrect IP address to a user's computer. Such an attack can easily result in a user's traffic being diverted to a computer of the attacker's choice instead of the user's intended destination. If the criminal sets up a phony bank site on the server to which traffic is being diverted, for example, and impersonates on that server a bank that the user was trying to reach, even a user who enters the bank URL into his or her browser (as opposed to just clicking on a link) may fall prey after being diverted to the bogus site. (This type of attack is known as *DNS poisoning* or *pharming*.)

Network infrastructure attacks take many forms. Some seek to route people to the wrong destinations. Others seek to capture data, while others seek to effectuate denial-of-service conditions. The main point to understand is that the piping of the Internet is quite complex was not initially designed with security in mind, and is vulnerable to many forms of misuse.

Malvertising

Malvertising is an abbreviation of the words malicious advertising and refers to the use of online advertising as a vehicle to spread malware or to launch some other form of a cyberattack.

Because many websites display ads that are served and managed by third-party networks and that contain links to various other third parties, online advertisements are a great vehicle for attackers. Even companies that adequately secure their websites may not take proper precautions to ensure that they do not deliver problematic advertisements created by, and managed by, someone else.

As such, malvertising sometimes allows criminals to insert their content into reputable and high-profile websites with large numbers of visitors (something that would be difficult for crooks to achieve otherwise), many of whom may be security conscious and who would not have been exposed to the criminal's content had it been posted on a less reputable site.

Furthermore, because websites often earn money for their owners based on the number of people who click on various ads, website owners generally place ads on their sites in a manner that will attract users to the ads.

As such, malvertising allows criminals to reach large audiences via a trusted site without having to hack anything.

Some malvertising requires users to click on the ads in order to become infected with malware; others do not require any user participation — users' devices are infected the moment that the ad displays.

Drive-by downloads

Drive-by downloads is somewhat of a euphemism that refers to software that a user downloads without understanding what he or she is doing. A drive-by download may occur, for example, if a user downloads malware by going to a poisoned website that automatically sends the malware to the user's device when he or she opens the site.

Drive-by downloads also include cases in which a user knows that he or she is downloading software, but is not aware of the full consequences of doing so. For example, if a user is presented with a web page that says that a security vulnerability is present on his or her computer and that tells the user to click on a button that says Download to install a security patch, the user has provided authorization for the (malicious) download — but only because he or she was tricked into believing that the nature of the download was far different than it truly is.

Stealing passwords

Criminals can steal passwords many different ways. Two common methods include

- **Thefts of password databases:** If a criminal steals a password database from an online store, anyone whose password appears in the database is at risk of having his or her password compromised. (If the store properly encrypted its passwords, it may take time for the criminal to perform what is known as a *hash attack*, but nonetheless, passwords — especially those that are likely to be tested early on — may still be at risk. To date, stealing passwords is the most common way that passwords are undermined.
- **Social engineering attacks:** *Social engineering attacks* are attacks in which a criminal tricks someone into doing something that he would not have done had he realized that the person making the request was tricking him in some way. One example of stealing a password via social engineering is when a criminal pretends to be a member of the tech support department of his target's employer and tells his target that the target must reset a particular password to a particular value to have the associated account tested as is needed after the recovery from some breach, and the target obeys. (For more information, see the earlier section on phishing.)
- **Credential attacks:** Credential attacks are attacks that seek to gain entry into a system by entering, without authorization, a valid username and password combination (or other authentication information as needed). These attacks fall into four primary categories:
  - *Brute force:* Criminals use automated tools that try all possible passwords until they hit the correct one.
  - *Dictionary attacks:* Criminals use automated tools to feed every word in the dictionary to a site until they hit the correct one.
  - *Calculated attacks:* Criminals leverage information about a target to guess his or her password. Criminals may, for example, try someone's mother's maiden name because they can easily garner it for many people by looking at the most common last names of their Facebook friends or from posts on social media. (A Facebook post of "Happy Mother's Day to my wonderful mother!" that includes a user tag to a woman with a different last name than the user himself/herself is a good giveaway.)
  - *Blended attacks:* Some attacks leverage a mix of the preceding techniques — for example, utilizing a list of common last names, or performing a brute force attack technology that dramatically improves its efficiency by leveraging knowledge about how users often form passwords.
- **Malware:** If crooks manage to get malware onto someone's device, it may capture passwords. (For more details, see the section on malware, earlier in this chapter.)
- **Network sniffing:** If someone transmits his or her password to a site without proper encryption while using a public Wi-Fi network, a criminal using the same network may be able to see that password in transit — as can potentially

other criminals connected to networks along the path from the user to the site in question.

- **Credential stuffing:** In credential stuffing, someone attempts to log in to one site using usernames and passwords combinations stolen from another site.

REMEMBER You can utilize passwords and a password strategy that can help defeat all these techniques —see Chapter 7.

Exploiting Maintenance Difficulties

Maintaining computer systems is no trivial matter. Software vendors often release updates, many of which may impact other programs running on a machine. Yet, some patches are absolutely critical to be installed in a timely fashion because they fix bugs in software — bugs that may introduce exploitable security vulnerabilities. The conflict between security and following proper maintenance procedures is a never-ending battle — and security doesn't often win.

As a result, the vast majority of computers aren't kept up to date. Even people who do enable automatic updates on their devices may not be up to date — both because checks for updates are done periodically, not every second of every day, and because not all software offers automatic updating. Furthermore, sometimes updates to one piece of software introduce vulnerabilities into another piece of software running on the same device.

Advanced Attacks

If you listen to the news during a report of a major cyberbreach, you'll frequently hear commentators referring to advanced attacks. While some cyberattacks are clearly more complex than others and require greater technical prowess to launch, no specific, objective definition of an advanced attack exists. That said, from a subjective perspective, you may consider any attack that requires a significant investment in research and development to be successfully executed to be advanced. Of course, the

definition of significant investment is also subjective. In some cases, R&D expenditures are so high and attacks are so sophisticated that there is near universal agreement that an attack was advanced. Some experts consider any zero-day attack to be advanced, but others disagree.

Advanced attacks may be opportunistic, targeted, or a combination of both.

Opportunistic attacks are attacks aimed at as many possible targets as possible in order to find some that are susceptible to the attack that was launched. The attacker doesn't have a list of predefined targets — his targets are effectively any and all reachable systems that are vulnerable to the attack that he is launching. These attacks are similar to someone firing a massive shotgun in an area with many targets in the hope that one or more pellets will hit a target that it can penetrate.

Targeted attacks are attacks that target a specific party and typically involve utilizing a series of attack techniques until one eventually succeeds in penetrating into the target. Additional attacks may be launched subsequently in order to move around within the target's systems.

Opportunistic attacks

The goal of most opportunistic attacks is usually to make money — which is why the attackers don't care whose systems they breach; money is the same regardless of whose systems are breached in order to make it.

Furthermore, in many cases, opportunistic attackers may not care about hiding the fact that a breach occurred — especially after they've had time to monetize the breach, for example, by selling lists of passwords or credit card numbers that they stole.

While not all opportunistic attacks are advanced, some certainly are.

Opportunistic attacks are quite different than targeted attacks.

Targeted attacks

When it comes to targeted attacks, successfully breaching any systems not on the target list isn't considered even a minor success.

the Democratic and Republican parties' email systems and steal copies of all the email on the parties' email servers, his or her mission is going to be deemed a success only if he achieves those exact aims. If he manages to steal $1 million from an online bank using the same hacking techniques that he is directing at his targets, it will not change a failure to breach the intended targets into even a small success. Likewise, if the goal of an attacker launching a targeted attack is to take down the website of a former employer that fired him, taking down other websites doesn't accomplish anything in the attacker's mind.

Because such attackers need to breach their targets no matter how well defended those parties may be, targeted attacks often utilize advanced attack methods — for example, exploiting vulnerabilities not known to the public or to the vendors who would need to fix them.

As you may surmise, advanced targeted attacks are typically carried out by parties with much greater technical prowess than those who carry out opportunistic attacks. Often, but not always, the goal of targeted attacks is to steal data undetected or to inflict serious damage — not to make money. After all, if one's goal is to make money, why expend resources targeting a well-defended site? Take an opportunistic approach and go after the most poorly defended, relevant sites.

Some advanced threats that are used in targeted attacks are described as *advanced persistent threats* (APTs):

- **Advanced:** Uses advanced hacking techniques, likely with a major budget to support R&D
- **Persistent:** Keeps trying different techniques to breach a targeted system and won't move on to target some other system just because the initial target is well protected
- **Threat:** Has the potential to inflict serious damage

Blended (opportunistic and targeted) attacks

Another type of advanced attack is the opportunistic, semi-targeted attack.

If a criminal wants to steal credit card numbers, for example, he may not care whether he successfully steals an equivalent number of active numbers from Best Buy, Walmart, or Barnes & Noble. All that he or she likely cares about is obtaining credit card numbers — from whom the numbers are pilfered isn't relevant.

At the same time, launching attacks against sites that don't have credit card data is a waste of the attacker's time and resources.