Cyber Exploits: Understand the Threat

Begin video

News Anchor 1 John Doe We interrupt our regularly scheduled programming for this breaking news. WHITLEY, the international telecommunications firm, has announced that it has fallen victim to a cyber attack, forcing it to shut down operations and disrupting corporate communications all over the globe. Our business reporter, Laura Brown, is here to give us an update. Over to you, Laura.

News Anchor 2 Laura Brown: Thank you, John. We've received a statement from WHITLEY'S Chief Information Officer Bob Smith. A massive DDoS ransomware attack with UDP flood power between 400 and 500 gigabits per second has completely shut down the company's computer networks. The famous hacker, l33th@cker156b **NOTE: Pronounced "LEET HACKER ONE FIFTY SIX BEE"]**, has claimed responsibility and is demanding a half million dollars payable in Bitcoin to restore operations. This shut-down is disrupting WHITLEY's business all over the world, costing the company millions in revenue.

News Anchor 1 John Doe: Laura, is there any indication as to *how* such a massive security breach happened?

News Anchor 2 Laura Brown: Well, John, there's speculation that a global IoT botnet was used to disrupt service, but the incident response team is still investigating.

News Anchor 1 John Doe: Thank you, Laura. As news develops, we'll be bringing you live updates.

[Seemingly Off Air]

News Anchor 1 John Doe: [TURNS TO OTHER ANCHOR] So a DDoS attack? And IoT botnet?

News Anchor 2 Laura Brown: [shrugs] I have no idea. I just read the teleprompter. Those technical terms are totally over my head.

[Guy with headphones and a clipboard runs on]; Uh, guys… we're still on the air. [Both anchors look right into the camera like a deer in the headlights]

[Screen goes to static, then black.]

End video

Botnets, crypto-ransomware, RATs, cross-site scripting…come again? You've heard these terms on the news. Do you know what they mean? These are just a few examples of sophisticated cyber attacks that proliferate our online existence every day. Give this course a little bit of your time and attention, and we promise – it'll all be easier to understand.

Not everyone needs to be a cyber subject matter expert. But it's critical to understand the risks that are all around us, from: computers & devices, cars, household appliances.

Get Used To It.

Cyber breaches are everywhere. Anyone who has an email address, a social media account, or a mobile device has been spoofed, hacked, and attacked… or they will be. As fast as technologies evolve, cyber attacks adapt and expand. They put citizens, businesses, financial institutions, online commerce providers, and even national security at risk. And because attackers invent new tactics at breakneck speed, it's critical that you stay educated and up-to-date on what's out there and where you're vulnerable. This course is designed to help you do just that.

The estimated cost of cyber crime globally is $100 billion.

Ninety-nine percent of computers are vulnerable to cyber attacks.

Seventy-nine percent of U.S. organizations were victims of cyber security attacks in 2016.

Over the next thirty minutes or so, we're going to look at some of the broader categories of cyber attacks. Within each of these categories, you'll learn specific terminology and real-world applications so you can recognize a threat when you see it.

As our daily activities depend progressively more on computerized technology, we are increasingly vulnerable to cyber attacks.

Let's get started.

Module & Objectives

Hover over any of the five modules to read their corresponding summary.

The Knowledge Checks at the end of each section will give you a chance to review, reinforce, and see just what you've learned.

01. Denial of Service (DoS) -- A DoS attack floods a site with false activity, overloading it to a point that legitimate users can't access it.
02. Compromised Trusted Websites -- Well-known, seemingly secure websites are still vulnerable to attacks – often more dangerous because they are so unexpected.
03. Spyware -- Spyware is malicious software secretly installed on your computer and used to collect your private information.
04. Man-in-the-Middle -- MITM attacks allow hackers to get between users and their internet services, gaining access to any information a victim views online.

05. Ransomware. -- Ransomware uses malware to remotely block access to all of the files on a device or network until the victim pays a ransom.

Click the button to continue. It’s safe… we promise.

Module 1

Denial-of-Service (DoS)

We've all been there. You go to one of your frequently visited websites to shop online, get the latest news, or read up on your favorite celebrity… but, inexplicably, you can't connect to the site.

If you're wondering what's going on behind the scenes, it's likely a Denial-of-Service attack.

A Denial-of Service (DoS) attack

This attack uses a single computer or internet connection to populate a targeted site or system with falsified activity, traffic, and requests which overload the site and prevent legitimate users from getting through.

Distributed Denial-of-Service (DDoS) Attack

A DDoS attack is similar and has the same result, but it uses multiple computers —typically thousands or even hundreds of thousands –and internet connections to overload target servers and deny access to would-be visitors.

Let's dig in.

Individual small attacks can be combined to create a major incident.

Here are some examples of DoS/DDoS attacks: Botnets & Zombies.

Botnets

A "bot" is a type of malware that allows an attacker to take control of an affected computer during a DoS/DDoS attack. A network of these infected machines is a "botnet," and can grow to include victim computers across the globe. And it's not just computers that are at risk.

The Internet of Things (IoT) – a term used to describe any devices connecting to the internet that aren't primarily computers, from hydroelectric turbines and industrial sensors to home thermostats, kitchen appliances, and medical device monitors – has become a favorite target for hackers.

Poor security practices in the billions of IoT devices that we've grown to love make them particularly vulnerable to creating a network of compromised devices.

Zombie

This is a bot-infected computer connected to the internet that a hacker uses to remotely perform malicious tasks. Most owners of "zombie" computers are unaware that their system is being used

in this way, but there are indications that you've been infected, like slower performance, unexplained error messages, and frequent crashes.

Saturday is the most popular day for DDoS attacks.

Let's Get Real

The Mirai botnet is estimated to control up to 1.5 million devices on the IoT, mainly through everyday online consumer items, like digital IP cameras and home wireless routers. This dangerous international network is responsible for generating record-setting DDoS attacks. These include shutting down the website of cybercrime journalist Brian Krebs, infiltrating French web host OVH, and shutting down large swaths of internet services in Europe and North America during the Dyn attack. The massive speed and scale with which the Mirai botnet can carry out an attack is a major threat – and it's still active.

Knowledge Check Module 1

Use what you've learned about DoS/DDoS attacks to select the best answer to the following questions.

An army of computers infected with the same malware that allows a hacker to take control is considered a:

a. Distributed Denial of Service (DDoS)
b. Denial of Service (DoS)
c. Botnet
d. Robot

The correct answer is C.

A botnet is a network of infected machines that might be used to carry out a Denial of Service (DoS) attack or a Distributed Denial of Service (DDoS) attack.

For a couple hours, high-profile websites including Etsy, Github, Wired, and Twitter suffered service interruptions or went offline altogether when their internet infrastructure company was overwhelmed with malicious requests from tens of millions of IP addresses. This is an example of:

a. Escalation of Privileges
b. Distributed Denial of Service (DDoS)
c. Spoofing
d. Phishing

The correct answer is B.

A Distributed Denial of Service (DDoS) uses multiple computers and internet connections to overload target servers and deny access to would-be visitors.

Module 2

A Compromised Trusted Website

What's a trusted website? Take a look at the image below. These are just a few visual indicators: lock icon, https, Verisign [images of https:, Lock icon, VeriSign]

Seeing them assures that a given site should be secure.

Here's the scenario. You visit a large reputable organization online. You believe it's secure because you see one of the visual indicators above. You expect that, because it's a well-established business, it has the resources and capabilities needed to secure its website. Wrong. Any site can be vulnerable to attack - and visitors and users would have no way of knowing that they are at risk. As a matter of fact, IT professionals can't diagnose some breaches until it's too late.

Let's dig in.

Hackers have countless ways to try to access a site illegally.

Here are some ways even trusted websites can come under attack:

- Cookies
- Cross-Site Scripting
- Watering Holes

Cookies

A cookie is a small piece of data sent from a website and stored on your computer while you are browsing. For example, cookies track your history on shopping sites. They allow you to choose "keep me logged in" for an online service even when you close your browser or shut down your computer.

Forged Cookies

Hackers can forge these kinds of cookies to impersonate a victim, tricking a website into giving them access to the victim's account.

Malicious Cookies

Many sites use cookies for profiling and tracking for legitimate purposes, like advertising and analytics. Malicious cookies, however, extract private information from websites when you haven't logged out, or that contain unexpired cookies used to maintain sessions over short periods of time.

Supercookies

Supercookies identify and persistently track visitors, without having to worry about users enabling private browsing or deleting cookies.

Cross-Site Scripting (XSS)

Cross-site scripting is an attack that delivers malicious code to end-users through trusted websites and applications. With XSS, an attacker does not target a victim directly, but uses a vulnerability within a website or application as a vehicle to deliver a malicious script to the victim's web browser. The script can have several negative side effects, including allowing the attacker to impersonate the victim, gaining access to passwords and other sensitive information, and hijacking a victim's browsing session altogether.

Watering Holes

Watering holes implant malware into reputable websites that targeted victims are likely to visit. The goal is to infect victims' computers and gain access to their networks. New research suggests that these tactics have been used as first steps in espionage attacks against defense, government, academia, financial services, healthcare, and utilities targets.

XXS attack is the number one vulnerability found in web applications.

Let's Get Real

Yahoo and Forbes are two examples of trusted websites that have been compromised by hackers. Yahoo suffered a forged cookie attack in which hackers stole data from more than a billion customer accounts. The Forbes compromise occurred when a Chinese group infected the Forbes.com website with a watering hole attack. Millions of users visited the site during the attack. The protections in place shielded most of the would-be-victims from the attack, according to two malware protection companies, iSight and Invincia. The attackers were seeking the user profiles of leaders in the defense and financial industries in order to gain access to their respective networks.

Knowledge Check Module 2:

Use what you've learned about compromises to trusted websites to select the best answer to the following questions.

This is a small piece of data sent from a website and stored on your computer while you are browsing. It allows the server to deliver tailored content and "remember" the user-provided data.

a. Cookie
b. Denial of Service (DoS)
c. Botnet
d. Cross-Site Scripting (XSS)

The correct answer is A.

A cookie is a small piece of data sent from a website and stored on your computer while you are browsing. Hackers can forge these kinds of cookies to impersonate a victim, tricking a website into giving them access to the victim's account.

Hackers apparently exploited a vulnerability on eBay to inject malware into several listings for cheap iPhones. When users clicked on the listing, they were taken to what appeared to be an eBay log-in page. In reality, it was a fake website set up to harvest user credentials. This is an example of:

a. Malicious Cookies
b. Forged Cookies
c. Denial of Service (DoS)
d. Cross-Site Scripting (XSS)

The correct answer is d.

Cross-site scripting is an attack that delivers malicious code to end-users through trusted websites and applications. With XSS, an attacker does not target a victim directly, but uses a vulnerability within a website or application as a vehicle to deliver a malicious script to the victim's browser.

Module 3

Spyware

When you think of a cyber attack, what's the first thing that comes to mind? Probably the stereotypical hoodied hacker infiltrating your personal computer and stealing sensitive data like passwords, financial information, social security numbers, and the like. This kind of attack involves spyware. Spyware is malicious software installed on a computer without your knowledge, and it's used to collect your private information. Spyware comes in many forms.

Let's dig in.

Less concerning spyware includes adware, which generates unwanted advertising like pop-ups, and tracking cookies, which track which sites the user has visited. However, some spyware has serious consequences.

A few of these nefarious types are keyloggers, rootkits, and Remote Access Trojans (RATs).

Keyloggers

Keystroke logging hardware or software tracks and records every keystroke entry a user makes on their computer. It's not always necessarily malicious, as some keyloggers are legitimate IT monitoring tools, but more often than not, it's used by hackers to capture sensitive information to exploit unsuspecting users.

Rootkits

A rootkit is a software collection typically designed to enable administrator-level access to a computer and often masks its existence. This unauthorized access can allow existing software to be modified, including software that might otherwise be used to detect or circumvent it. Rootkits typically enter a computer through a Trojan horse virus, suspicious email attachment, or the installation of a "special" plugin (pretending to be legitimate) needed to correctly view a webpage.

Remote Access Trojans (RATs)

RATs are a common form of spyware that give attackers complete control over a victim's system**.** They can be used to steal sensitive information, spy on victims through the system's microphone and web camera, and remotely control the computers they infect. Social engineering and spear phishing are common ways RAT attacks are carried out. Look out for anyone trying to convince you to give up personal information, and be wary of emails, even from trusted sources, containing unrequested links and downloads.

ZLOB, a common Trojan, is estimated to update every 15 or 60 minutes to avoid detection.

Let's Get Real

NSO Group Technologies, an internet software security solutions company that operates in the international intelligence field, created a proprietary monitoring tool called Pegasus. Pegasus was discovered to have been used in a targeted attack on human rights activists through a malicious link texted to an iOS phone. Clicking on the link allowed Pegasus to be installed on the device, gathering all communications and locations on the targeted phones including data from Gmail, Facebook, iMessage, Viber, WhatsApp, Telegram and Skype communications. Once the phone was infected, spies could actively record with the phone's microphone or video camera, grab personal data like calendars, contacts, and passwords, or download all the data on the device including emails, photos, and browser history.

Knowledge Check Module 3:

Use what you've learned about spyware to select the best answer to the following questions.

The Sakula malware is believed to be associated with the OPM and Anthem attack. It looked like benign software and provided the attacker with remote administration capabilities over the victim machines which enabled the attackers to steal sensitive information. Sakula is an example of a:

a. Remote Access Trojan (RAT)
b. Watering Hole
c. Distributed Denial of Service (DDoS)
d. Compromised Trusted Website

The correct answer is a.

Remote Access Trojans (RATs) give attackers complete control over a victim's system. They can be used to steal sensitive information, spy on victims through the system's microphone and web camera, and remotely control the computers they infect.

You've created a complex password and you steer clear of public WiFi. So you think your computer is safe, right? Wrong. This type of malicious software can be installed on your computer to capture each and every entry you make. It's called:

a. Watering Hole
b. Spyware
c. Watering Hole
d. Keylogger

The correct answer is d.

Keystroke logging tracks and records every keystroke entry a user makes on their computer. When used maliciously by hackers, it captures sensitive information and puts unsuspecting users at risk.

Module 4

Man-in-the-Middle (MITM)

You've heard that you shouldn't do your online banking at a coffee shop. Do you know why? One of the biggest cyber threats that consumers face comes from man-in-the-middle attacks (MITM), in which hackers can see or manipulate a user's private internet traffic.

Man-in-the-middle (MITM) attack

An MITM allows hackers to read the victim's emails, see what websites they're visiting, steal valuable personal information, and even impersonate the user by stealing session cookies, passwords, and more.

Let's dig in.

MITM attacks allow hackers to insert themselves between users and the websites or internet services they use.

Hackers gather sensitive information through:

- Wi-Fi Eavesdropping
- Karma Attacks

Wi-Fi Eavesdropping

Wi-Fi eavesdropping is the most common form of MITM attack. It occurs when a Wi-Fi connection is hijacked in order to spy on a user. It's easiest for a hacker to snoop over public networks, but you need to know that it can also happen in the privacy of your own home. Almost any type of internet connection can be hacked if the end user is targeted or the platform itself is vulnerable.

There are several ways hackers can hijack a Wi-Fi connection. They can create a fake Wi-Fi node called an "evil twin" that impersonates a legitimate Wi-Fi access point in order to trick users into connecting to it. Another method is to observe a user's web traffic over an unencrypted connection and look for known openings to hijack accounts. And for attackers not particularly interested in being creative, they can simply find a router still using default settings or hack the user's Wi-Fi password to gain access.

Karma Attacks

Karma's good, right? Not this kind. You know how your smartphone is always scanning for open Wi-Fi access points to keep you connected, especially to familiar networks? That's called probing. In a karma attack, a hacker waits for your phone to send out a probe request. The attacker then replies to the probe and creates an access point with a matching network name that your phone recognizes thereafter, enabling ongoing MITM attacks without you being any the wiser.

Ninety-five percent of HTTPS servers are vulnerable to MITM attacks.

Let's Get Real

49 suspects spread throughout Europe were arrested in simultaneous raids on suspicion of using Man-in-the-Middle attacks to commit bank fraud against a number of medium-to-large European companies. Through social engineering, the suspects planted the MITM-enabling malware on the targeted companies' networks to monitor communications. They used that access to monitor corporate email accounts for payment requests. When a request was made, they faked a transaction with a targeted company's real site, tricking the victim into entering password and payment information that they used to divert an unauthorized payment to themselves.

Knowledge Check Module 4:

Use what you've learned about MITM attacks to select the best answer to the following questions.

When a hacker places himself between the user and their internet service or website, it is considered a:

a. Denial of Service (DoS) attack
b. Cross-Site Scripting (XSS) attack
c. Man-in-the-Middle (MITM) attack
d. Remote Access Trojan (RAT) attack

The correct answer is c.

MITM attacks allow hackers to insert themselves between users and the websites or internet services they use. This allows hackers to read the victim's emails, see what websites they're visiting, steal valuable personal information, and even impersonate the user by stealing session cookies, passwords, and more.

While attempting to access a public Wi-Fi network, you notice a second Wi-Fi option that is similarly named. This could be a legitimate node or an evil twin. If it's an evil twin, it would be an example of a:

a. Denial of Service (DoS)
b. Wi-Fi Eavesdropping
c. Watering Hole
d. Remote Access Trojan (RAT)

The correct answer is b.

Wi-Fi eavesdropping is the most common form of MITM attack. It occurs when a Wi-Fi connection is hijacked in order to spy on a user. Hackers can create a fake Wi-Fi node called an "evil twin" that impersonates a legitimate Wi-Fi access point in order to trick users into connecting to it.

Module 5

Ransomware

Ransomware

This cyber attack blocks all access to files on an individual's device or network until a victim pays a ransom.

Ransomware, how it works: A hacker uses a sophisticated piece of malware to remotely disable the targeted device, completely blocking access to the victim's files or in the case of a corporate attack, disabling an organization's network. Only by paying a demanded ransom can victims regain access – and even then there is no guarantee cyber criminals will be true to their word and return what was stolen.

Internet security company Symantec considers ransomware the most dangerous of cyber threats, with the number of attempted attacks spiking from just over 3 million in 2014 and 2015 to *638* million in 2016. The Federal Bureau of Investigation(FBI) estimated that ransomware payouts totaled $209 million for the first quarter of 2016 and would soon reach $1 billion annually.

Let's dig in.

Ransomware is such a prevalent attack that you're sure to hear about it, and probably on a large scale.

Here are a couple of ransomware tactics to look out for:

- Fake Apps
- Lockers

Fake Apps

Fake Apps are fraudulent applications for mobile devices that look legitimate, either by mimicking actual apps from reputable companies or by offering fake services, like virus scanning. When a user downloads a fake app, it infects the targeted device with ransomware.

Lockers

Lockers infect personal computers, scouring targeted devices in search of file extensions to encrypt. Once the files are encrypted, the locker virus opens a window containing details about the infection and the terms of the ransom demanded in exchange for the decryption key.

Seven out of ten malicious email attacks delivery Locky, a locker device hidden within a Microsoft Word document.

Let's Get Real.

Hackers seized control of the Hollywood Presbyterian Medical Center's computer systems, paralyzing the hospital's communications for about 10 days. To get operations back on track, Hollywood Presbyterian paid the hackers with Bitcoin–an alternative digital currency not based on a centralized banking system. The ransom was equivalent to $17,000 and was paid before authorities were contacted. Hospital president Allen Stefanek believed it was "the quickest and most efficient way" to free the Los Angeles hospital's network. The Hollywood Presbyterian Hospital situation highlights why ransomware is so dangerous. Most of the time, there is no other solution than to pay the ransom, especially in cases where critical services depend on the hijacked information.

Knowledge Check Module 5:

Use what you've learned about ransomware to select the best answer to the following questions.

Europol estimated that the "WannaCry" attack had hit at least 150 countries and infected 200,000 machines. Hospitals, universities, manufacturers and government agencies in Britain, China, Russia, Germany and Spain have all been affected. WannaCry locks down files and asks the administrator to pay a fee to regain control. This is an example of:

a. Watering Hole
b. Malicious Cookies
c. Wi-Fi Eavesdropping
d. Ransomware

The correct answer is d.

Ransomware is a cyber attack that blocks all access to files on an individual's device or network until a victim pays a ransom. Only by paying a demanded ransom can victims regain access – and even then, there is no guarantee cyber criminals will be true to their word and return what was stolen.

EnergyRescue was available for four days in the official marketplace for Android apps. Users who downloaded the app received the following message: "You need to pay for us, otherwise we will sell portion of your personal information on black market every 30 minutes…"

This is an example of:

a. Denial of Service (DoS)
b. Keylogger
c. Man-in-the-Middle (MITM)
d. Fake App (Ransomware)

The correct answer is d.

Fake Apps are fraudulent applications for mobile devices that look legitimate, either by mimicking actual apps from reputable companies or by offering a fake service, like a virus scanning. When a user downloads a fake app, it infects the targeted device with ransomware. Users are discouraged from downloading apps from third-party sites; however, sometimes fake apps elude the security of legitimate app stores, putting many more users at risk.

Conclusion

Congratulations! You have completed the Cyber Exploits course.

With the information provided in this course, you should be able to easily recognize some of the more technical terms related to common cyber attacks. Take advantage of the knowledge you've gained concerning computer attacks and how they affect their targets, to better protect your own cyber security. Share what you know with friends and family as well to promote a greater awareness of the widespread threats we face in our digital world. Be safe.

Click here to download your certificate of completion.