Chapter 5: Endpoint Vulnerabilities, Attacks, and Defenses

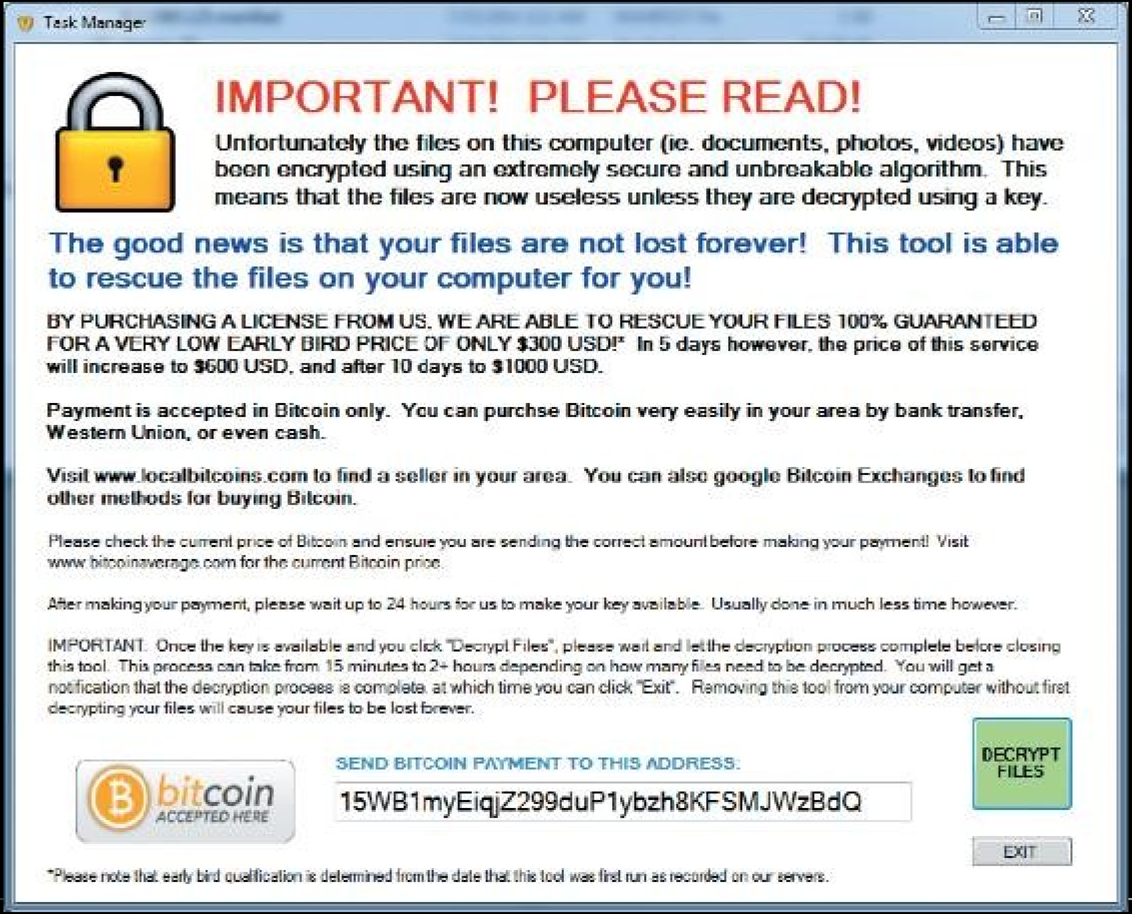
Malware Attacks

- **Malware** is a word that describes software designed to interfere with a computer’s normal functions and can be used to commit an unwanted and harmful action
- One attempt at classifying the diverse types of malware can be to examine the primary action that the malware performs, such as kidnap, eavesdrop, masquerade, and launch

Kidnap

- **Ransomware** is malicious software designed to extort money from victims in exchange for their endpoint device to be restored to its normal working state
- **Blocking ransomware** blocks the user from using their computer in a normal fashion
  - The ransomware infects the computer and then manipulates its OS in such a way as to block all normal access to the device
- **Locking ransomware** encrypts some or all of the files on the device so that they cannot be opened

Locking Ransomware Message



IMPORTANT! PLEASE READ!

Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.

The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!

BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.

Payment is accepted in Bitcoin only. You can purchse Bitcoin very easily in your area by bank transfer, Western Union, or even cash.

Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.

Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.

After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.

IMPORTANT. Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.

SEND BITCOIN PAYMENT TO THIS ADDRESS:

15WB1myEiqjZ299duP1ybzh8KFSMJWzBdQ

*Please note that early bird qualification is determined from the date that this tool was first run as recorded on our servers.

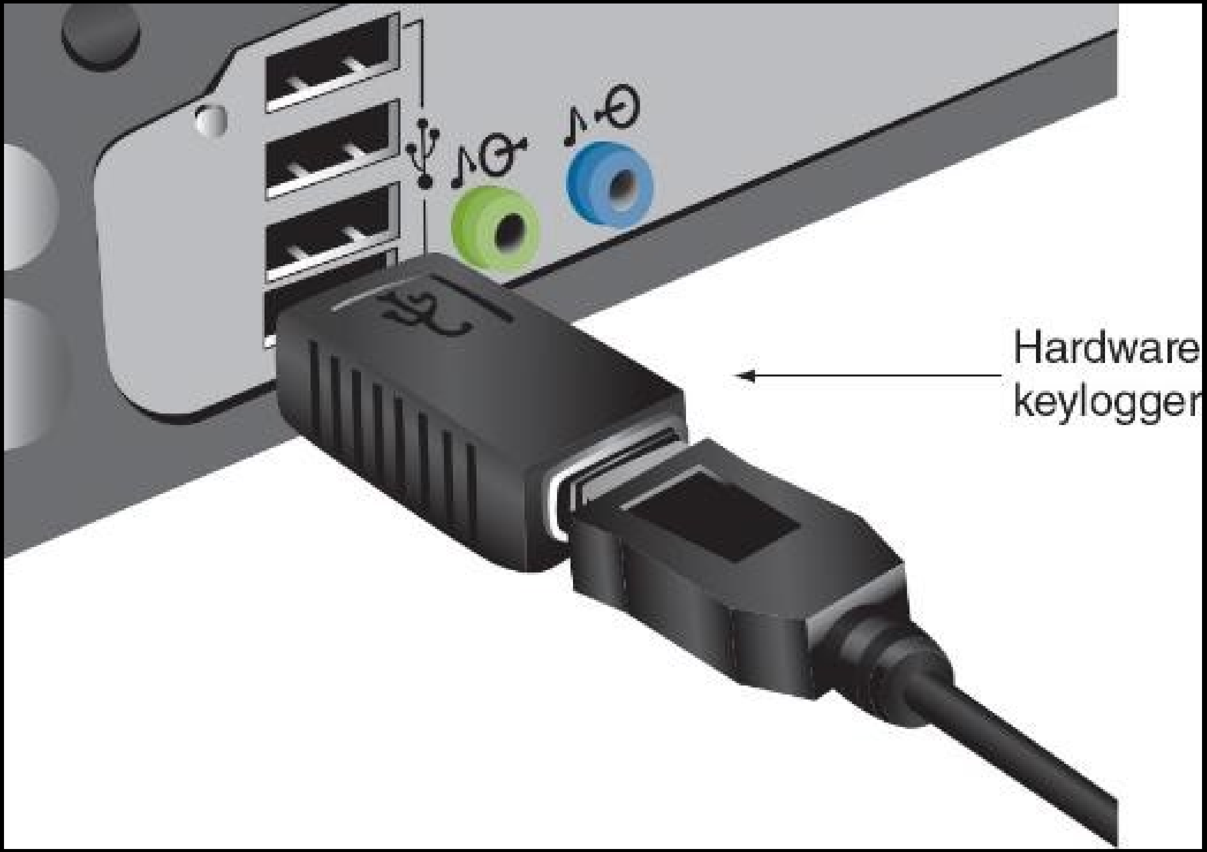
Kidnap

- Attackers have also encrypted all files on any network or storage device that is connected to a device
- Attackers may also publicly release the stolen information
- Ransomware is considered to be the most serious malware threat for the following reasons:
  - Low barrier to entry
  - Pervasive attacks
  - High impact

Eavesdrop

- Two types of eavesdropping malware are spyware and keyloggers
- A **keylogger** silently captures and stores each keystroke that a user types on the computer's keyboard
  - The threat actor can then search the captured text for any useful information such as passwords, credit card numbers, or personal information
  - A keylogger can be a software program or a small hardware device
- **Spyware** is tracking software that is deployed without the consent or control of the user

Hardware Keylogger



Masquerade

- Some malware can hide its true intentions
- A computer **Trojan** is an executable program that masquerades as performing a benign activity but also does something malicious
- A **remote access Trojan** (**RAT**) has the basic functionality of a Trojan but also gives the threat agent unauthorized remote access to the victim’s computer by using specially configured communication protocols
  - This creates an opening to the victim’s computer allowing the threat agent unrestricted access

Launch

- Malware that infects a computer to launch attacks on other computers includes a virus, worm, bloatware, and bot
- There are two types of viruses: a file-based virus and a fileless virus
  - A *file-based virus* is malicious code that is attached to a file that reproduces itself on the same computer without any human intervention
  - The virus first unloads a payload to perform a malicious action, then the virus replicates itself by inserting its code into another file (on the same computer)

Launch

- A **fileless virus** does not attach itself to a file but instead takes advantage of native services and processes that are part of the OS to avoid detection and carry out its attacks
  - It does not infect a file, instead the code is loaded directly in the computer’s random access memory (RAM)
- Advantages of a fileless virus over a file-based virus include the following:
  - Easy to infect, extensive control, persistent, difficult to detect, difficult to defend against

Launch

- A **worm** is a malicious program that uses a computer network to replicate (sometimes called a network virus)
  - It is designed to enter a computer through the network and then take advantage of a vulnerability in an application or an OS on the host computer
- Actions that worms have performed include deleting files on the computer or allowing the computer to be remotely controlled by an attacker

Launch

- **Bloatware** is software that is installed on a device without the user requesting it
  - It could contain malware or it could become a platform for other malware to exploit if the bloatware contains a vulnerability
- A category of bloatware is software that comes preinstalled on a new device
- Another category is software that a user does not intend to install but is installed as the result of overlooking the default installation options

Launch

- Another type of malware allows the infected computer to be placed under the remote control of an attacker for the purpose of launching attacks
  - The infected robot computer is known as a **bot** or zombie
  - When hundreds, thousands, or even millions of bot computers are gathered into a logical computer network, they create a botnet under the control of a bot herder
- Infected bot computers receive instructions through a command and control (C&C) structure from the bot herders

Sidestep

- A **logic bomb** is computer code that is typically added to a legitimate program but lies dormant and evades detection until a specific logical event triggers it
- A **rootkit** is malware that can hide its presence and the presence of other malware on the device
  - It does this by accessing “lower layers” of the OS to make alterations
- A **backdoor** gives access to a computer, program, or service that circumvents any normal security protections

Indicator of Attack (IoA)

Indicator	Description
Account lockout	A user account that is inaccessible through a normal login attempt can be an indication the account has been taken over by an attacker and is locking out a legitimate user.
Concurrent session usage	An indicator of attack in which both a legitimate user and an attacker are logged into the same account.
Blocked content	Data that is no longer accessible can be an IoA.
Impossible travel	Impossible travel is accessing a resource that is not possible due to geography; for example, a user who checks email from New York and then downloads a file from Los Angeles five minutes later is an example of impossible travel.
Resource consumption	System resources such as memory or processing capabilities that are suddenly depleted could indicate an attack.
Resource inaccessibility	A large-scale attack can block system resources from being accessed.
Out-of-cycle logging	Log records that do not correspond to actual events that have occurred can be an IoA.
Published/documented	Evidence from external sources of a current attack can be used to identify an attack.
Missing logs	Log files that have mysteriously been deleted is an indication of an ongoing attack taking place.

Question?

- Finn’s team leader has just texted him that an employee, who violated company policy by bringing in a file on a USB flash drive, has just reported that their computer is infected with locking ransomware. Why would Finn consider this a serious situation?

Answer

- Finn’s team leader has just texted him that an employee, who violated company policy by bringing in a file on a USB flash drive, has just reported that their computer is infected with locking ransomware. Why would Finn consider this a serious situation?
- It can encrypt all files on any network that is connected to the employee’s computer. In addition to encrypting files on the device’s local drive, new variants of locking ransomware encrypt all files on any network or attached device that is connected to that device. This includes secondary drives, USB drives, network-attached storage devices, network servers, and even cloud-based data repositories.

Application Vulnerabilities and Attacks

- Application attacks look for vulnerabilities in the application or manipulate the application in order to compromise it
- Application attacks frequently result in **privilege escalation**, which allows the attacker to gain illicit access of elevated rights or privileges beyond what is entitled for a user

Application Vulnerabilities

- A **buffer overflow attack** occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer
  - This extra data overflows into the adjacent memory locations
- These attacks are called injections or memory injections since they introduce something into RAM
- Some attacks are the result of poor coding on the part of software developers
  - Software that allows the user to enter data but has **improper input handling** features does not filter or validate user input to prevent a malicious action

Application Vulnerabilities

- Another improper handling situation is a NULL pointer/object dereference
  - When an application dereferences a pointer that has a value of NULL, it typically will cause a program to crash or exit
- A NULL pointer/object dereference can also be the result of a race condition
  - A **race condition** in software occurs when two concurrent threads of execution access a shared resource simultaneously

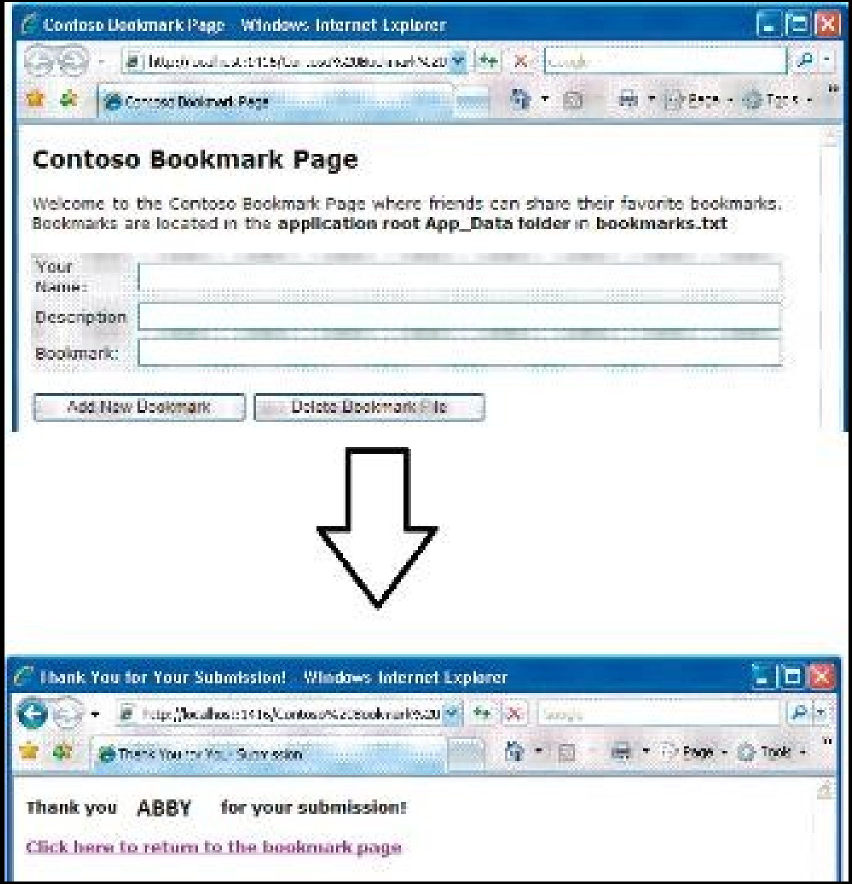
Application Attacks

- A common type of attack is an application attack directed at programs running on Internet web servers, known as **web-based attacks**
- A web server provides services that are implemented as “web applications” through software applications running on the server
- Web-based attacks frequently result in **directory traversal**
  - This type of attack takes advantage of a vulnerability so that a user can move from the root directory to other restricted directories

Application Attacks

- In a **cross-site scripting** (**XSS**) attack, a website that accepts user input without validating it and uses that input in a response can be exploited
- An attacker can take advantage in an XSS attack by tricking a valid website into feeding a malicious script to another user's web browser
- One of the most common injection attacks (**SQL injection**) inserts statements to manipulate a database server
  - SQL stands for **Structured Query Language**
- By entering crafted SQL statements as user input, information from the database can be extracted or the existing can be manipulated

Bookmark Page Accepts User Input



Contoso Bookmark Page - Windows Internet Explorer
Contoso Bookmark Page
Add New Bookmark
Delete Bookmark File
Thank You for Your Submission! - Windows Internet Explorer
Thank You for Your Submission

Contoso Bookmark Page

Welcome to the Contoso Bookmark Page where friends can share their favorite bookmarks. Bookmarks are located in the **application root App_Data folder** in **bookmarks.txt**

Your Name:

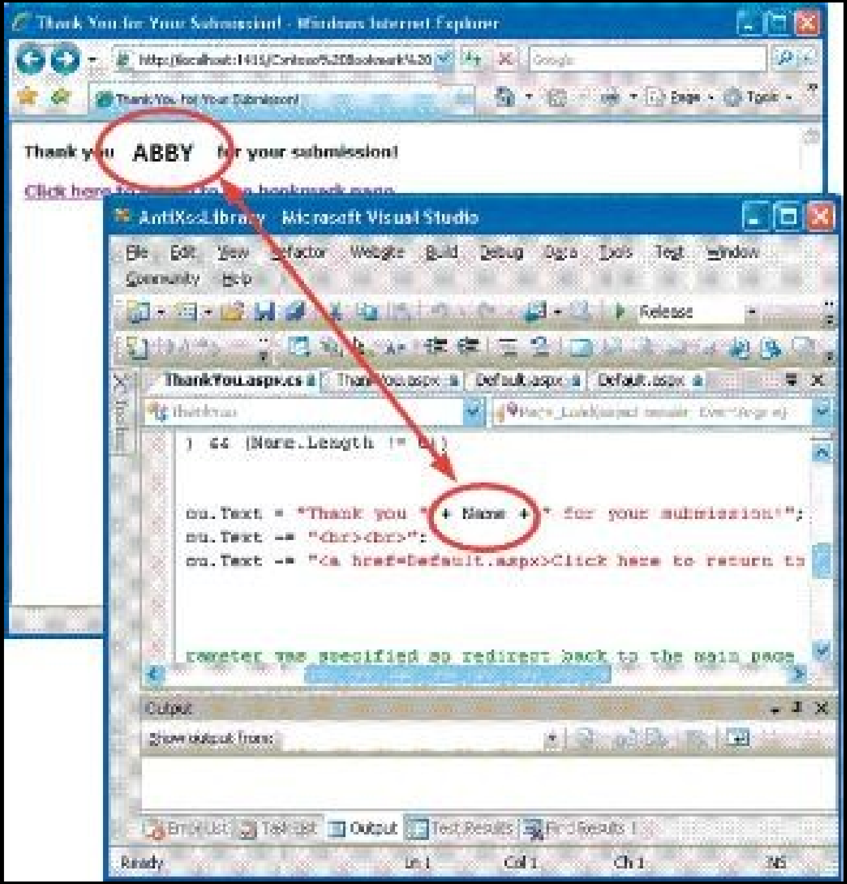
Description:

Bookmark:

Thank you ABBY **for your submission!**

Click here to return to the bookmark page

Input Used in Response


Thank You for Your Submission! - Windows Internet Explorer
http://localhost:1415/Contoso%20bookmark%20
Thank You for Your Submission!
Page
Tools
AntiXssLibrary - Microsoft Visual Studio
File Edit View Refactor Website Build Debug Data Tools Test Window Community Help
Release
ThankYou.aspx.cs
ThankYou.aspx
Default.aspx
Default.aspx
Output
Show output from:
Error List
Task List
Output
Test Results
Find Results 1
Ready
Ln 1
Col 1
Ch 1
INS

Thank you ABBY for your submission!

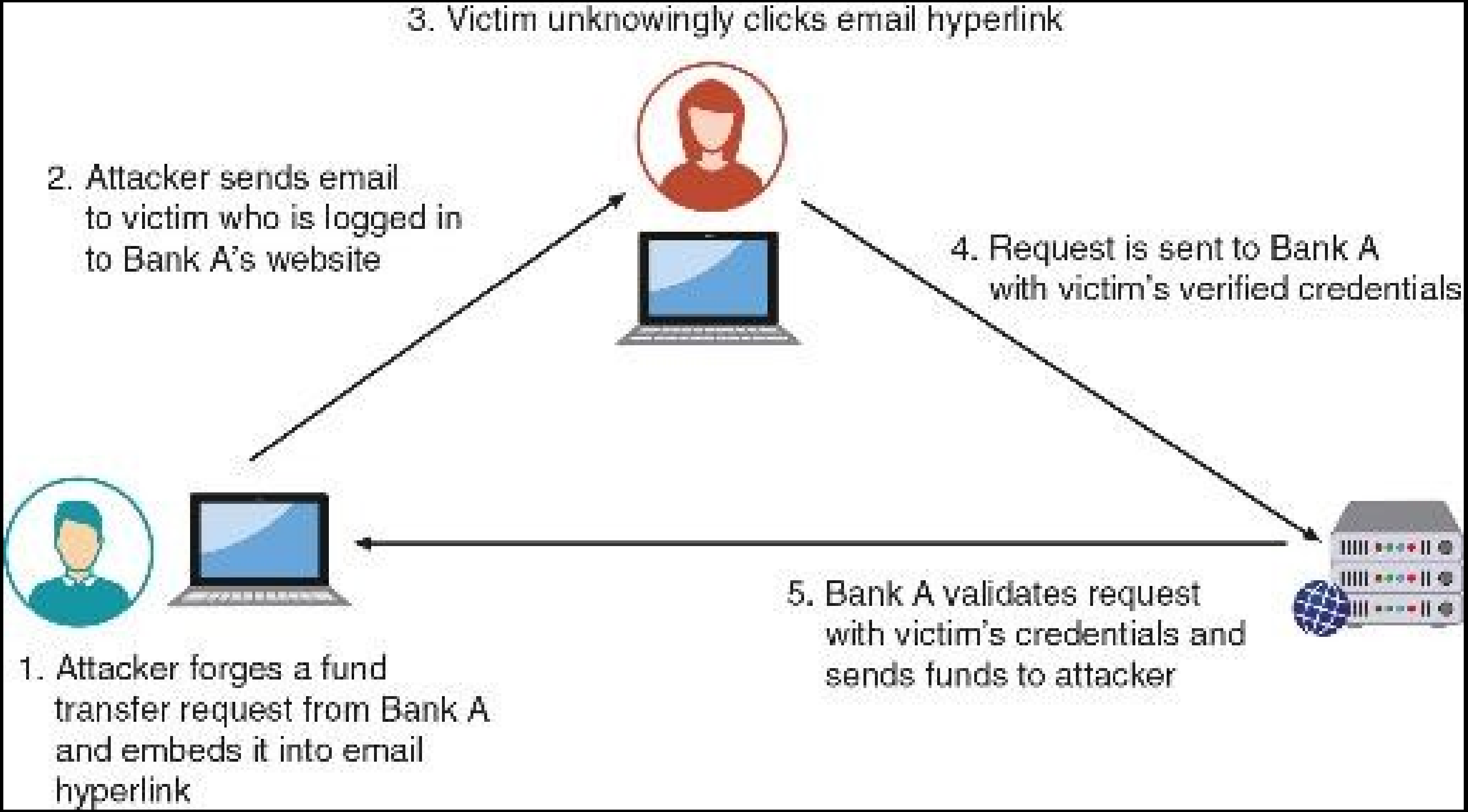
Click here to return to the bookmark page

```
) && (Name.Length != 0))


ou.Text = "Thank you " + Name + " for your submission!";
ou.Text += "<br><br>";
ou.Text += "<a href=Default.aspx>Click here to return to



rameter was specified so redirect back to the main page
```

Application Attacks

- Request forgery is a request that has been fabricated
- There are two types of request forgeries: cross-site request forgery (CSFR) and a server-site request forgery (SSRF)
- A **cross-site request forgery** (**CSRF**) takes advantage of an authentication “token” that a website sends to a user’s web browser
  - If a user is currently authenticated on a website and is tricked into loading another webpage, the new page inherits the identity and privileges of the victim, who may then perform an undesired function on the attacker’s behalf

Cross-Site Request Forgery



3. Victim unknowingly clicks email hyperlink

2. Attacker sends email to victim who is logged in to Bank A's website

4. Request is sent to Bank A with victim's verified credentials

5. Bank A validates request with victim's credentials and sends funds to attacker

1. Attacker forges a fund transfer request from Bank A and embeds it into email hyperlink

Application Attacks

- A **server-site request forgery** (**SSRF**) takes advantage of a trusting relationship between web servers
  - SSRF attacks exploit how a web server processes external information received from another server
  - Some web applications are designed to read information from or write information to a specific URL
  - If an attacker can modify that target URL, they can potentially extract sensitive information from the application or inject untrusted input into it

Application Attacks

- **Replay attacks** are commonly used against digital identities
  - After intercepting and copying data, the threat actor retransmits selected and edited portions of the copied communications later to impersonate the legitimate user
- Many digital identity replay attacks are between a user and an authentication server

Question?

- What type of attacks is based on website accepting user input without sanitizing it?

Answer

- What type of attacks is based on website accepting user input without sanitizing it?
- XSS. In a cross-site scripting (XSS) attack, a website that accepts user input without validating it (called “sanitizing”) and uses that input in a response can be exploited.

Protecting Endpoints

- Protection on computer endpoints can be accomplished through software installed on the endpoint, such as the following:
  - Antivirus, web browser protections, and monitoring and response systems
- **Antivirus** (**AV**) software can examine a computer for file-based virus infections and monitor computer activity and scan new documents that might contain a virus
  - Log files created by AV products can provide info regarding attacks
  - Older AV products use signature-based monitoring, called **static analysis**
  - A newer approach to AV is heuristic monitoring, called **dynamic analysis**

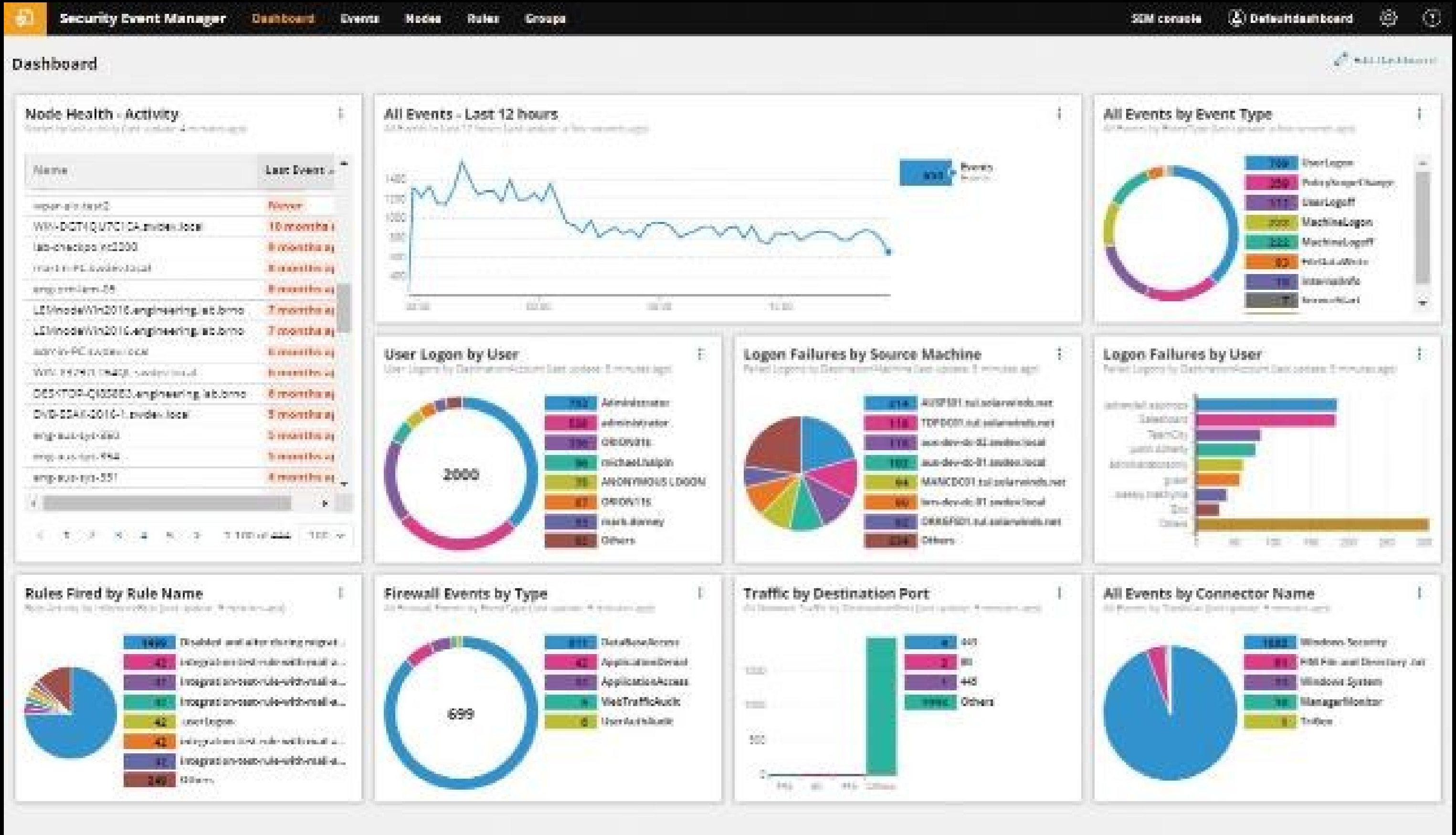
Protecting Endpoints

- Web browsers offer the following security on endpoint computers:
  - **Secure cookies** are sent to a web server with an encrypted request over the secure HTTPS protocol
    - This prevents an unauthorized person from intercepting a cookie that is being transmitted between the browser and the web server
  - **HTTP Response Headers** are headers that tell the browser how to behave while communicating with the website

Protecting Endpoints

- There are three types of monitoring and response systems for endpoint computers:
  - **Host Intrusion Detection Systems** (**HIDS**) is a software-based application that runs on an endpoint computer and can detect an attack has occurred
  - **Host Intrusion Prevention Systems** (**HIPS**) monitor endpoint activity to immediately block a malicious attack by following specific rules
  - **Endpoint Detection and Response** (**EDR**) tools are considered more robust than HIDS and HIPS

HIDS Dashboard



Name	Last Event
[illegible]	Never
WIN-DGT1QU7C1CA.swdev.local	10 months
[illegible]	8 months ag
[illegible]	8 months ag
[illegible]	8 months ag
LEMnodeWin2016.engineering.lab.brno	7 months ag
LEMnodeWin2016.engineering.lab.brno	7 months ag
[illegible]	6 months ag
[illegible]	6 months ag
DESKTOP-[illegible].engineering.lab.brno	6 months ag
DVB-DDAX-2016-1.swdev.local	5 months ag
[illegible]	5 months ag
[illegible]	5 months ag
[illegible]	4 months ag

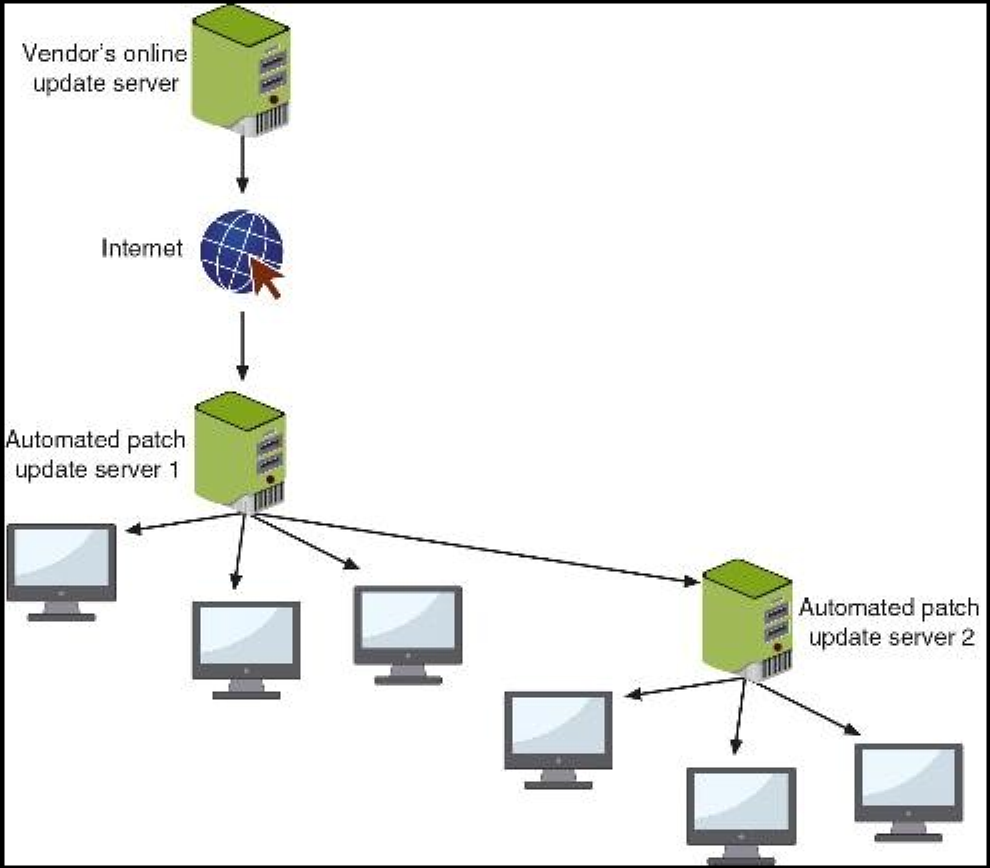
Protecting Endpoints

- Endpoint detection and response (EDR) tools can aggregate data from multiple endpoint computers to a centralized database so that security professionals can further investigate and gain a better picture of events
- EDR tools can perform more sophisticated analytics that identify patters and detect anomalies
  - This can help detect unusual or unrecognized activities by performing baseline comparisons of normal behavior

Hardening Endpoints

- Hardening endpoints involves patch management and OS protections
- Effective patch management involves two types of patch management tools to administer patches
  - Patch distribution using **automated patch management tools**
  - Patch reception in Microsoft Windows 11 can be delayed from one to five weeks
    - After that, the updates will resume
    - Users can set a time range when the computer will restart after an update has been installed

Automated Patch Update Service


Vendor's online update server
Internet
Automated patch update server 1
Automated patch update server 2

Hardening Endpoints

- Protections at the OS level include the following:
  - **Disabling unnecessary ports and protocols**
  - **Application allow list** – a list of approved applications to run on the OS so that any item not approved will not function
  - **Sandbox** – a “container” in which an application can be run so that it does not impact the underlying OS