**Day 06 Assignment**

**Cybersecurity and Asset Management**

1. **What is Cyber security:**

* Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.
* It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies.
* So basically, Cyber Security is protecting cyber space including critical information  
  infrastructure from attack, damage and misuse.
* Cyber Space: A global domain within the information environment consisting of  
  the interdependent network of information technology infrastructures, including the  
  Internet, telecommunications networks, computer systems, and embedded  
  processors and controllers.
* Cyber Attack: It is a malicious and deliberate attempt by an individual or  
  organization to breach the information system of another individual or organization.

1. **Motives behind Cyber Attacks:**

* To seek commercial gain by hacking banks and financial institutions.  
  To attack critical assets of a nation.
* To penetrate into both corporate and military data servers to obtain plans and  
  intelligence.
* To hack sites to virally communicate a message for some specific campaign related to  
  politics and society.

1. **How Cyber security Works :**

Cybersecurity systems detect, examine, and fix potential system weaknesses and vulnerabilities before hackers or malicious software exploit them. An organization, its employees, and the processes and technologies must come together to create a solid cybersecurity layer that protects it from potential attacks.

* **Steps followed for Cyber Security:**

**Identify risks:**Assess the risks to your organization's systems and information.

**Protect systems:**Use strong passwords, multi-factor authentication, and secure configurations.

**Detect threats:**Use monitoring and analytics to identify potential threats.

**Respond to threats:**React to security threats and vulnerabilities in a timely manner.

**Recover from threats:**Recover from any damage caused by cyber attacks.

**Types of Cyber Attacks:**

1. **Phishing attacks:** A [phishing attack](https://www.fortinet.com/resources/cyberglossary/phishing) occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target.

**Working:** To execute the attack, the bad actor may send a link that brings you to a website that then fools you into downloading malware such as viruses, or giving the attacker your private information. In many cases, the target may not realize they have been compromised, which allows the attacker to go after others in the same organization without anyone suspecting malicious activity.

**Prevention:** You can prevent phishing attacks from achieving their objectives by thinking carefully about the kinds of emails you open and the links you click on. Pay close attention to email headers, and do not click on anything that looks suspicious. Check the parameters for “Reply-to” and “Return-path.” They need to connect to the same domain presented in the email.

1. **Ransomware:** With [Ransomware](https://www.fortinet.com/resources/cyberglossary/ransomware), the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware” is appropriate because the malware demands a ransom from the victim.

**Working:** In a [**ransomware attack**](https://www.fortinet.com/resources/cyberglossary/ransomware), the target downloads ransomware, either from a website or from within an email attachment. The malware is written to exploit vulnerabilities that have not been addressed by either the system’s manufacturer or the IT team. The ransomware then encrypts the target's workstation. At times, ransomware can be used to attack multiple parties by denying access to either several computers or a central server essential to business operations.

**Prevention:** Backup Data – Regularly back up important files and store them offline. Update Software – Keep operating systems, software, and antivirus updated. Use Strong Security – Install and enable firewalls, antivirus, and anti-ransomware tools. Beware of Phishing – Avoid clicking on suspicious emails, links, or attachments. Restrict Access – Limit user permissions and disable unnecessary remote access (e.g., RDP). Enable Multi-Factor Authentication (MFA) – Adds extra security to logins. Network Segmentation – Isolate critical systems to limit ransomware spread. Security Awareness – Train employees/users to recognize threats.

1. **Malware attack:** [Malware](https://www.fortinet.com/resources/cyberglossary/malware) is a general term for malicious software, hence the “mal” at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device.

**Working:** Malware, or malicious software, is designed to infiltrate and harm devices, networks, or data. It usually enters a system through phishing emails, malicious downloads, or security vulnerabilities. Once inside, it executes hidden processes, often disguising itself as legitimate files to avoid detection. Some types of malware, like worms, can spread automatically across networks, while others, such as ransomware, encrypt files and demand payment for decryption. Malware can steal sensitive data, disrupt system operations, or even grant hackers remote control over infected devices.

**Prevention:** To prevent malware attacks, it is essential to use strong security measures. Installing antivirus software and firewalls helps detect and block threats in real time. Keeping operating systems and applications updated ensures that security flaws are patched. Users should avoid clicking on suspicious links, downloading unknown attachments, or visiting untrusted websites. Enabling multi-factor authentication (MFA) adds an extra layer of security to logins, making unauthorized access more difficult. Regular backups of important data, stored offline, can help recover lost files in case of an attack. Restricting administrative privileges, using strong passwords, and securing networks with VPNs and intrusion detection systems further enhance protection against malware threats.

1. **Password Attacks:** Passwords are the access verification tool of choice for most people, so figuring out a target’s password is an attractive proposition for a hacker. This can be done using a few different methods. Often, people keep copies of their passwords on pieces of paper or sticky notes around or on their desks. An attacker can either find the password themselves or pay someone on the inside to get it for them.

**Working:** Attackers also often use brute-force methods to guess passwords. A brute-force password hack uses basic information about the individual or their job title to try to guess their password. For example, their name, birthdate, anniversary, or other personal but easy-to-discover details can be used in different combinations to decipher their password. Information that users put on social media can also be leveraged in a brute-force password hack.

**Prevention:** One effective method of preventing brute-force and dictionary password attacks is to set up a lock-out policy. This locks out access to devices, websites, or applications automatically after a certain number of failed attempts. With a lock-out policy, the attacker only has a few tries before they get banned from access. If you have a lockout policy in place already and discover that your account has been locked out because of too many login attempts, it is wise to change your password.

1. **DoS and DDoS attacks:** A [denial-of-service (DoS) attack](https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos) is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system. A [DDoS attack](https://www.fortinet.com/resources/cyberglossary/ddos-attack) is initiated by a vast array of malware-infected host machines controlled by the attacker. These are referred to as “denial of service” attacks because the victim site is unable to provide service to those who want to access it.

**Prevention:** To prevent DoS and DDoS attacks, organizations should use firewalls, intrusion detection systems (IDS), and anti-DDoS services to filter malicious traffic. Rate limiting and load balancing help distribute traffic and prevent overload. Keeping software updated patches vulnerabilities that attackers may exploit. Using CDNs (Content Delivery Networks) and cloud-based DDoS protection adds extra layers of security. Monitoring network traffic regularly and setting up automatic mitigation responses can help detect and stop attacks early.

1. **Drive-By Download (DoD):**

**Working:** A Drive-By Download attack occurs when malicious software is automatically downloaded onto a user's device without their knowledge or consent. This can happen simply by visiting a compromised website, clicking on an infected ad, or interacting with a fake pop-up. Cybercriminals exploit security vulnerabilities in web browsers, plugins, or operating systems to install malware, spyware, or ransomware. Once executed, the malware can steal sensitive data, take control of the system, or create backdoors for further attacks.

**Prevention:** To prevent Drive-By Download attacks, keep your operating system, browsers, and plugins updated to patch vulnerabilities. Enable automatic security updates and use trusted antivirus software to detect threats. Avoid visiting unknown or suspicious websites and be cautious of pop-ups and ads. Disable unnecessary browser plugins and use ad blockers to reduce exposure to malicious content. Enable click-to-play for Flash and Java to prevent automatic script execution. Lastly, avoid downloading software from untrusted sources and use firewalls to block malicious connections.

1. **Different types of Cyber Security:**

|  |  |  |
| --- | --- | --- |
| **No.** | **Name** | **Explanation** |
| 1. | Network Security | Most [cyberattacks](https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-a-cyberattack/) take place over a network. Network security should, therefore, detect, monitor, and block attacks that seek unauthorized access to the network. This is done by using VPNs, intrusion detection and prevention systems, and firewalls protecting the network infrastructure, which includes switches, bridges, servers, and routers. |
| 2. | Cloud Security | Now, with the growing use of cloud computing, securing the systems as well as the data hosted in platforms like Google Cloud and Amazon Web Services (AWS) has become indispensable. [Cloud security](https://www.sentinelone.com/platform/cloud-security/) is referred to as policies, services, administrative, and technical controls that protect the cloud deployment and its components like infrastructure and data from attacks. |
| 3. | Endpoint Security | This includes servers, mobile devices, laptops, and desktops to name a few. The securing of these devices, as well as the data they carry, is regarded as [endpoint security](https://www.sentinelone.com/cybersecurity-101/endpoint-security/). Advanced threat prevention software includes anti-ransomware, anti-phishing protocols, as well as endpoint detection and response solutions to ensure that these end-user devices stay secure. |
| 4. | Mobile Security | Mobile devices primarily contain access to corporate data, so businesses are highly prone to instant messaging attacks, phishing, and malicious apps. This is where mobile security comes into play- applying protection to the mobile device against these attacks and preventing unauthorized access from jailbreaking and rooting. |
| 5. | IoT Security | IoT security reduces the vulnerabilities of wearables, smartphones, and all connected devices found in smart homes. It secures the device but also secures the network that connects them all. The manner it does this is by discovering the type of connected devices and automatically segmenting the network activities to be controlled by it, along with intrusions that protect vulnerable IoT devices from exploitation. |
| 6. | Application Security | Application security against cyber attacks is a concept of identifying vulnerabilities from the application development and publication stages.  Application security involves checking code testing and review, point frequency security testing, and ensuring that no applications have security flaws or vulnerabilities that may be exploited for example cross-site scripting and broken authentications. |
| 7. | Zero Trust | The traditional perimeter-focused way of building walls around the most important systems and assets of a company can be breached by insider threats, as well as by the dissolution of that perimeter. Moreover, with the ever-growing trend toward cloud computing and moving away its assets off premises, what is needed is stronger security than perimeter-focused can offer. [Zero trust security](https://www.sentinelone.com/platform/zero-trust/) is the answer. It follows a more granular approach and protects individual resources by using methods such as role-based access controls, least privilege access, micro-segmenting networks, and not trusting any internal or external user. |

1. **Need of Cyber Security:**

Cybersecurity is essential to protect sensitive data, systems, and networks from cyber threats like malware, hacking, and phishing attacks. It ensures the privacy, integrity, and availability of personal and organizational information, preventing financial losses and identity theft. With increasing digital dependence, strong cybersecurity measures safeguard critical infrastructure, businesses, and individuals from cybercriminal activities. It also helps maintain trust in online transactions and services by preventing unauthorized access and data breaches.

**For Individuals:** Photos, videos and other personal information shared by an  
individual on social networking sites can be inappropriately used by others, leading  
to serious and even life-threatening incidents.

**For Business Organizations:** Companies have a lot of data and information on  
their systems. A cyber attack may lead to loss of competitive information (such as  
patents or original work), loss of employees/customers private data resulting into  
complete loss of public trust on the integrity of the organization.

**For Government:** A local, state or central government maintains huge amount of  
confidential data related to country (geographical, military strategic assets etc.) and  
citizens. Unauthorized access to the data can lead to serious threats on a country.

**Asset Management:**

1. **What is Asset?**

Assets hold economic value and contribute to an individual's or organisation's net worth. Or we can say anything crucial.

1. **Asset Management:**

Asset management is the practice of buying, selling, and managing investments, commensurate with specific risk tolerances, to increase wealth over time. Asset management professionals perform this service for clients. They may also be called portfolio managers or financial advisors. Many work independently while others work for an asset management company, [investment bank](https://www.investopedia.com/terms/i/investmentbank.asp), or other type of financial institution.

The goal of asset management is to maximize the value of an investment portfolio over time while maintaining an acceptable level of risk.

 It may apply both to tangible [assets](https://en.wikipedia.org/wiki/Asset) (physical objects such as complex process or manufacturing plants, infrastructure, buildings or equipment) and to intangible assets (such as [intellectual property](https://en.wikipedia.org/wiki/Intellectual_property), [goodwill](https://en.wikipedia.org/wiki/Goodwill_(accounting)) or [financial assets](https://en.wikipedia.org/wiki/Financial_assets)). Asset management is a systematic process of developing, operating, maintaining, upgrading, and disposing of assets in the most cost-effective manner (including all costs, risks, and performance attributes).

**How does it Works?**

* **Asset Identification** – List and categorize all assets, including hardware, software, data, and networks, to maintain a complete inventory.
* **Asset Classification & Valuation** – Assess the importance of each asset based on its role, value, and potential impact on business operations if compromised.
* **Asset Tracking & Monitoring** – Continuously track asset locations, ownership, and usage to prevent loss, theft, or unauthorized access.
* **Risk Assessment & Security Measures** – Identify vulnerabilities and implement security controls like encryption, access control, and backups to protect critical assets.
* **Asset Maintenance & Updates** – Regularly update and maintain hardware and software to ensure optimal performance and security.
* **Compliance & Documentation** – Ensure assets comply with industry regulations and maintain records for audits, security policies, and asset life cycles.
* **Asset Disposal & Decommissioning** – Securely remove outdated or unused assets through proper data wiping, recycling, or destruction to prevent unauthorized access.

1. **IT Asset Management:**

IT asset management (also known as ITAM) is the process of ensuring an organization’s assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. Put simply, it’s making sure that the valuable items, tangible and intangible, in your organization are tracked and being used.  So, what’s an IT asset? Defined simply, an IT asset includes hardware, software systems, or information an organization values. In Atlassian’s IT department, some of our most important assets are the computers and software licenses that help us build, sell, and support our software and the servers we host it on.

**The IT asset management process**

1. **Inventory assets** - The first step in the IT asset management process is to create a detailed inventory of all IT assets. Your inventory includes what assets you have, where they are located when they were purchased, and for how much.
2. **Calculate lifecycle costs** - The second step is to calculate lifecycle costs for all assets in your inventory. During an average asset’s life, there are many opportunities for added costs, like maintenance, capital, and disposal costs. Calculating lifecycle costs makes your asset inventory accurate and actionable.
3. **Tracking** -  The third step is tracking via an asset management tool. Your goal is to continuously monitor IT assets through their lifecycle keeping a close eye on things like contract, license, and warranty expiration. Tracking also helps you stay ahead of the fourth step, maintenance.
4. **Maintenance** - Maintenance involves asset repair, upgrade, and replacement. All maintenance activities should be tracked in an ITAM tool so that the data can be used to understand the overall performance of the asset.
5. **Financial Planning** - The fifth and final step is financial planning. With an accurate picture of your IT assets, their lifecycle stage, and their costs, you can effectively plan for the future. One goal of financial planning is to determine the budget needed to maintain or improve the “levels of service” your team provides for your most important assets. An asset that was successfully managed with a high level of service, like a service desk and dedicated team, will need that level of service going forward. Assets that underperformed may need a higher level of service in the future, which will cost more.
6. **Cyber Security Asset Management:**

Cybersecurity asset management (CSAM) is the process created to continuously discover, inventory, monitor, manage and track an organization's assets to determine what those assets do and identify and automatically remediate any gaps in its cybersecurity protections. CSAM is a subset of IT asset management.

**Why is cybersecurity asset management important?**

CSAM aims to provide the complete, real-time visibility security operations ([SecOps](https://www.techtarget.com/searchsecurity/definition/SecOps)) teams need to optimize their resources and build and maintain a proactive, [risk-based security program](https://www.techtarget.com/searchsecurity/tip/5-ways-to-achieve-a-risk-based-security-strategy) that better safeguards their organizations and assets from security threats. CSAM also enables SecOps teams to more quickly respond to security incidents.

**How does cybersecurity asset management work?**

CSAM uses a variety of tools and processes to discover which assets are on a network and then investigate which security controls each asset uses and whether each asset is properly secured. CSAM can include, but is not limited to, device discovery and inventory, vulnerability management, network and security monitoring, risk analysis and assessment, [incident response](https://www.techtarget.com/searchsecurity/definition/incident-response) and policy enforcement. CSAM can also help maintain regulatory compliance.

CSAM uses the following three-step cycle:

1. **Asset discovery and inventory.** Tools scan the network and inventory each asset. The inventory includes details about the asset. For example, the inventory can include hardware or software version, manufacturer, software libraries, location, etc. -- as well as who has access to the asset, who owns it, internal policies and compliance regulations that apply to that asset, the risk level of the asset, software updates or patches for the asset, and more, depending on the organization's needs. CSAM also determines which security tools and policies are in place to protect the asset against internal and external security risks.
2. **Gap identification.** Once the asset inventory is complete, CSAM identities gaps in security coverage and recommends measures to put in place to remediate the gaps.
3. **Automated response.** CSAM uses automation techniques to fill gaps by deploying validated cybersecurity resources where needed. CSAM can also alert the SecOps teams of any necessary remediations that aren't automatically implemented.

After the cycle completes, it runs again. The process aims to mitigate all information security gaps given the available tools of an organization. CSAM tools can also inform SecOps teams of any remaining gaps, enabling teams to consider purchasing and deploying additional tools engineered to meet internal security policies and compliance regulations.

1. **Similarities and differences between IT and Cyber Security:**

* **Similarities:**

1. **Inventory Management** – Both involve identifying and tracking IT assets such as hardware, software, and data.
2. **Risk Management** – Both focus on minimizing risks associated with asset usage and security vulnerabilities.
3. **Compliance & Regulations** – Both ensure compliance with industry standards and regulations like GDPR, ISO 27001, and NIST.
4. **Lifecycle Management** – Both track assets from acquisition to disposal to maintain efficiency and security.
5. **Optimization & Cost Management** – Both aim to optimize asset usage and reduce unnecessary costs.

* **Differences:**

|  |  |  |
| --- | --- | --- |
| Feature | IT Asset Management (ITAM) | Cybersecurity Asset Management (CSAM) |
| |  | | --- | | Primary Focus | | Managing IT assets for efficiency, cost control, and lifecycle tracking. | Securing IT assets by identifying vulnerabilities and mitigating cyber threats. |
| |  | | --- | | Scope |  |  | | --- | |  |  |  | | --- | |  | | Covers procurement, maintenance, and disposal of hardware/software. | Focuses on security risks, threat detection, and compliance enforcement. |
| |  | | --- | | Objective |  |  | | --- | |  |  |  | | --- | |  | | Optimizes asset utilization and minimizes costs. | Protects assets from cyber threats and unauthorized access. |
| |  | | --- | | Tools Used |  |  | | --- | |  | | Asset inventory software, CMDB (Configuration Management Database), and ERP. | Vulnerability scanners, SIEM (Security Information and Event Management), and endpoint protection tools. |
| |  | | --- | | Risk Management |  |  | | --- | |  | | Manages financial and operational risks related to IT assets. | Manages security risks, including malware, data breaches, and cyberattacks. |
| |  | | --- | | End of Life Management |  |  | | --- | |  |  |  | | --- | |  | | Focuses on proper decommissioning and cost-efficient disposal. | Ensures secure disposal by removing sensitive data and preventing security threats. |

1. **Emerging trends in Cyber Security:**

Top 10 emerging cyber security trends are given below

1. **The Emergence of Automotive Cybersecurity Threats**

Modern vehicles have sophisticated software, offering seamless connectivity and advanced features such as cruise control, engine timing, and driver assistance systems. However, this reliance on automation and connectivity also exposes vehicles to potential hacking risks. Utilizing technologies like Bluetooth and WiFi for communication, hackers can exploit vulnerabilities to gain vehicle control or even eavesdrop on conversations through built-in microphones. With the increasing adoption of automated vehicles, these threats are expected to escalate, necessitating stringent cybersecurity measures, particularly for self-driving or autonomous vehicles.

**2. Mobile Devices: A Growing Target for Cyber Attacks**

The proliferation of mobile devices has made them lucrative targets for cybercriminals, with a notable increase in malware and attacks targeting mobile banking and personal data. The extensive use of smartphones for various activities, including financial transactions and communication, amplifies the risks associated with potential breaches. Mobile security becomes a focal point as cybersecurity threats evolve, with anticipated trends indicating a rise in smartphone-specific viruses and malware.

**3.Cloud Security Challenges and Solutions**

As organizations rely on cloud services, ensuring robust security measures becomes paramount for data storage and operations. While cloud providers implement robust security protocols, vulnerabilities may still arise due to user-end errors, malicious software, or phishing attacks. Continuous monitoring and updates are essential to mitigate risks and safeguard confidential data stored in the cloud.

**4.Data Breaches: A Persistent Concern**

[Data breaches](https://www.simplilearn.com/how-to-prevent-data-breaches-article) remain a significant concern for individuals and organizations worldwide, with even minor software flaws posing potential vulnerabilities. Regulatory frameworks like the GDPR and CCPA aim to enhance data protection and privacy rights, underscoring the importance of stringent security measures. Ensuring compliance with these regulations and implementing proactive security measures are essential to mitigating the risks associated with data breaches.

**5. IoT Security in the Era of 5G**

The proliferation of 5G networks ushers in a new era of interconnectedness, particularly with the Internet of Things (IoT). While offering unprecedented connectivity, this also exposes IoT devices to vulnerabilities from external threats and software bugs. The nascent nature of 5G architecture necessitates extensive research to identify and address potential security loopholes. Manufacturers must prioritize the development of robust hardware and software solutions to reduce the risk of data breaches and network attacks.

**6. Embracing Automation for Enhanced Cybersecurity**

Automation plays a pivotal role in managing the ever-expanding volume of data and streamlining security processes. In the face of demanding workloads, automation offers valuable support to security professionals, enabling swift and efficient responses to emerging threats. Integrating security measures into agile development processes ensures the creation of more secure software solutions, particularly for large and complex applications.

**7. Targeted Ransomware Attacks**

Targeted ransomware attacks pose a significant threat to industries reliant on specific software systems, with potentially devastating consequences. Recent incidents, such as the WannaCry attack on healthcare institutions, underscore the importance of robust cybersecurity measures. Organizations must remain vigilant against ransomware threats and implement proactive strategies to mitigate risks effectively.

**8. Escalating State-Sponsored Cyber Warfare**

The escalating tensions between global powers fuel state-sponsored cyber warfare, with cyberattacks increasingly targeting critical infrastructure and sensitive data. High-profile events, including elections, are vulnerable to cyber threats, necessitating heightened security measures. Expectations for 2025 include a surge in data breaches and state-sponsored actors' exploitation of political and industrial secrets.

**9. Mitigating Insider Threats Through Awareness**

Mistakes made by individuals continue to play a significant role in data breaches, especially regarding insider threats within organizations. To address this risk, it's vital to enhance awareness and provide thorough training programs for employees. By empowering staff to recognize and address potential vulnerabilities, companies can foster a strong culture of cybersecurity awareness. This approach is essential to safeguard sensitive data and effectively minimize the impact of insider threats.

**10. Addressing Cybersecurity Challenges in Remote Work Environments**

The transition to remote work during the pandemic presents fresh cybersecurity hurdles as employees navigate less secure network setups. Organizations must emphasize the implementation of strong security protocols, such as multi-factor authentication and secure VPNs, to shield remote workers from cyber threats effectively.

1. **Case Study on WannaCry ransomware attack:**

**What was the WannaCry ransomware attack?**

The WannaCry [ransomware](https://www.cloudflare.com/learning/security/ransomware/what-is-ransomware/)\* attack was a major security incident that impacted organizations all over the world. On May 12, 2017, the WannaCry ransomware worm spread to more than 200,000 computers in over 150 countries. Notable victims included FedEx, Honda, Nissan, and the UK's National Health Service (NHS), the latter of which was forced to divert some of its ambulances to alternate hospitals.

Within hours of the attack, WannaCry was temporarily neutralized. A security researcher discovered a "kill switch" that essentially turned off the [malware](https://www.cloudflare.com/learning/ddos/glossary/malware/). However, many affected computers remained encrypted and unusable until the victims paid the ransom or were able to reverse the encryption.

WannaCry spread by using a vulnerability exploit called "EternalBlue." The US National Security Agency (NSA) had developed this exploit, presumably for their own use, but it was stolen and released to the public by a group called the Shadow Brokers after the NSA was itself compromised. EternalBlue only worked on older, unpatched versions of Microsoft Windows, but there were more than enough machines running such versions to enable WannaCry's rapid spread.

\**Ransomware is malicious software that locks up files and data via*[*encryption*](https://www.cloudflare.com/learning/ssl/what-is-encryption/)*and holds them for ransom.*

**What is a worm?**

In the security field, a worm is a malicious software program that automatically spreads itself to multiple computers in a network. A worm uses operating system vulnerabilities to jump from computer to computer, installing copies of itself on each computer.

Think of a worm as being like a thief who walks around an office park checking for unlocked doors. Once the thief finds one, imagine that he can create a duplicate of himself that remains inside the unlocked office, and both versions continue their search for unlocked doors.

Most worms do not contain ransomware. Ransomware typically spreads through malicious emails, credential compromise, botnets, or highly targeted vulnerability exploits ([Ryuk](https://www.cloudflare.com/learning/security/ransomware/ryuk-ransomware/) is one example of the latter). WannaCry was unique in that it not only combined ransomware with a worm, but also used a particularly powerful worm-enabling vulnerability that had been created by the NSA.

**Who are the Shadow Brokers?**

The Shadow Brokers are a group of attackers who began leaking malware tools and [zero-day exploits](https://www.cloudflare.com/learning/security/threats/zero-day-exploit/) to the public in 2016. They are suspected of having acquired a number of exploits developed by the NSA, possibly due to an [insider attack](https://www.cloudflare.com/learning/access-management/what-is-an-insider-threat/) at the agency. On April 14, 2017, the Shadow Brokers leaked the EternalBlue exploit that WannaCry would eventually use.

Microsoft issued a patch for EternalBlue on March 14, one month before the Shadow Brokers leaked it, but many computers remained unpatched at the time of the WannaCry attack.

**Who was responsible for the WannaCry ransomware attack?**

In late 2017, the US and the UK [announced](https://www.bbc.com/news/world-us-canada-42407488) that the government of North Korea was behind WannaCry. However, some security researchers [dispute](https://www.darkreading.com/attacks-breaches/three-years-after-wannacry-ransomware-accelerating-while-patching-still-problematic) this attribution. WannaCry may have been the work of the North Korea-based Lazarus Group, some argue, without coming directly from the government of North Korea. Others suggest that the authorship clues in the malware may have been planted there to cast blame on North Korea-based attackers, and that WannaCry may be from another region altogether.

**How was the WannaCry attack stopped?**

On the day of the attack, a security blogger and researcher named Marcus Hutchins began reverse-engineering the WannaCry source code. He discovered that WannaCry included an unusual function: before executing, it would query the [domain](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. This website did not exist.

So, he registered the domain. (It cost [$10.69](https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/).)

After Hutchins did so, copies of WannaCry continued to spread, but they stopped executing. Essentially, WannaCry turned itself off once it began getting a response from iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

**Why did this stop the attack?**

While the WannaCry authors' motivations cannot be known for certain, it is theorized that this domain query function was included in WannaCry so that the ransomware could check if it was inside a sandbox.

A sandbox is an anti-malware tool. It is a [virtual machine](https://www.cloudflare.com/learning/cloud/what-is-a-virtual-machine/) running separately from all other systems and networks. It provides a safe environment to execute untrusted files and see what they do.

A sandbox is not actually connected to the Internet. But sandboxes aim to imitate a real computer as closely as possible, so they may generate a fake response to a query directed at a given domain by the malware. As a result, one way that malware could check if it is inside a sandbox is by sending a query to a fake domain. If it gets a "real" response (generated by the sandbox), it can assume it is in a sandbox and shut itself down so that the sandbox does not detect it as malicious.

However, if the malware sends its test query to a hard-coded domain, then it can be tricked into thinking it is always in a sandbox if someone registers the domain. This could be what happened with WannaCry: copies of WannaCry across the world were tricked into thinking they were inside a sandbox and shut themselves down. (A better design from the perspective of the malware author would be to query a randomized domain that was different every time — that way, the odds of getting a response from the domain outside of a sandbox would be close to zero.)

Another possible explanation is that the copy of WannaCry that spread across the world was unfinished. The authors of WannaCry may have hard-coded that domain as a placeholder, intending to replace it with the address of their command-and-control (C&C) server before releasing the worm. Or they may have meant to register iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com themselves. ([DNS filtering](https://www.cloudflare.com/learning/access-management/what-is-dns-filtering/) or [URL filtering](https://www.cloudflare.com/learning/access-management/what-is-url-filtering/) perhaps could have stopped queries to that domain, but most organizations would not have been able to deploy this safety measure in time.)

Regardless of the reason, it was a stroke of luck that such a simple action could save computers and networks around the world from further infection.

**What happened to Marcus Hutchins?**

It turned out that before Hutchins began working and blogging as a security researcher, he had spent years frequenting malware forums on the dark web, [building and selling his own malware](https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/). A few months after the WannaCry incident, the FBI arrested Hutchins in Las Vegas, Nevada, for authoring Kronos, a strain of banking malware.

**Is WannaCry a threat today?**

The version of WannaCry that was released into the world in 2017 no longer functions, thanks to Hutchins' kill switch domain. Additionally, a patch has been available for the EternalBlue vulnerability that WannaCry exploited since March 2017.

However, WannaCry attacks continue to occur. As of March 2021, WannaCry was [still using](https://www.netsec.news/wannacry-ransomware-attacks-up-53-since-january-2021/) the EternalBlue vulnerability, meaning only extremely old, out-of-date Windows systems were at risk. Newer versions of WannaCry have removed the kill switch feature present in the original version. Updating operating systems and installing security updates immediately is highly recommended.

While the original version of WannaCry is no longer active, several key lessons can be learned from the May 2017 attack:

1. **Networks around the world are highly interconnected.** In the Internet age, this may go without saying, but many organizations still assume that their networks cannot be penetrated from the outside (like a [castle with a moat](https://www.cloudflare.com/learning/access-management/castle-and-moat-network-security/)). WannaCry showed that unless a network is air-gapped — meaning it is completely separate from all outside connections — external threats can likely still get in.
2. **Even patched vulnerabilities can be dangerous.** A vulnerability patch is only as effective as the number of systems that apply it. The EternalBlue patch was available for almost two months prior to the WannaCry attack, but it seems that few organizations had installed the patch. (Even by 2021, some had not yet installed it.)
3. **Many crucial organizations are vulnerable to cyber attack.** This continues to be the case; ransomware attacks have impacted hospitals, schools, fuel pipelines, and governments in recent years. In fact, ransomware groups such as Ryuk seem to target these organizations. In some instances, organizations may not have the funding, resources, or commitment to technological updates that they need to face attacks. The NHS in particular faced scrutiny for continuing to use Windows XP, a highly vulnerable operating system that Microsoft no longer supported, in the wake of the attack.
4. **Ransomware is a major threat.** [Cloudflare One](https://www.cloudflare.com/cloudflare-one/) is a Zero Trust platform that can help organizations combat this threat. A [Zero Trust security](https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/) approach assumes that all users and devices present threats. It regularly re-authenticates users and assesses device security, ensuring that any unsafe or unauthorized devices have their application and network access revoked immediately. This helps prevent the spread of ransomware.