Running head: Journal Specs for courses with Dr. Chris Veltsos

Journal Specs

Tram Nguyen

[Apache fixes actively exploited zero-day vulnerability, patch now 3](#_Toc89138144)

[Samsung apologises for Russian app download error 3](#_Toc89138145)

[Railroads say they don't need cybersecurity mandates 4](#_Toc89138146)

[Sunderland University IT systems down in possible cyber attack 4](#_Toc89138147)

[iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security 5](#_Toc89138148)

[US warns that Chinese government is using 'wide variety' of methods, some illegal, to steal trade secrets 6](#_Toc89138149)

[Ransomware Gangs Earned $590 Million in H1 2021 6](#_Toc89138150)

[Cheap and free cybersecurity training: 8 ways to build skills without breaking the bank 7](#_Toc89138151)

[Cyber-attack hits UK internet phone providers 8](#_Toc89138152)

[Database firm Clearview AI told to remove photos taken in Australia 8](#_Toc89138153)

[Widespread Vulnerability Identified in Phones and Bluetooth Devices 9](#_Toc89138154)

[Apple digital ID scheme comes with conditions and costs 9](#_Toc89138155)

[All Versions of Windows Are Vulnerable to a New Zero-Day Exploit 10](#_Toc89138156)

[References 11](#_Toc89138157)

Tram Nguyen

CIS 450

Journal Specs – Second Round

# **Apache fixes actively exploited zero-day vulnerability, patch now**

10/6 | Apache fixes actively exploited zero-day vulnerability, patch now| [link](https://www.bleepingcomputer.com/news/security/apache-fixes-actively-exploited-zero-day-vulnerability-patch-now/)| October 5, 2021|Bill Toulas

**Quick Summary:** The CVE-2021-41773 (zero-day vulnerability) and CVE-2021041524 (DoS) vulnerabilities are fixed in the new version – 2.4.50 of Apache Server.

**Key quotes:** “The actively exploited zero-day vulnerability is tracked as CVE-2021-41773 and it enables actors to map URLs to files outside the expected document root by launching a path traversal attack.”

“The vulnerability was discovered and reported to Apache by security researcher Ash Daulton and the cPanel Security Team on September 29, 2021. Being an actively exploited flaw, the fix for it came pretty quickly.”

“The second vulnerability is CVE-2021-41524, a null pointer dereference detected during HTTP/2 request processing. This flaw allows an attacker to perform a denial of service (DoS) attack on the server.”

**Reflection:** However, a new attack vector was discovered against the Apache http server, which is still unpatched, allowing file access from areas outside the site root directory of websites. In essence, the new issue ([CVE-2021-42013](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42013)) is same as the earlier vulnerability (CVE-2021-41773) at 2.4.49, with the sole variation being characters in encoding.

In the last version, it allowed something like “curl http://host/img-sys/.%2e/%2e%2e/etc/passwd” that is the content of /etc/passwd. Although the 2.4.50 version fixed the issue reported correctly, it did not close the issue completely. As the picture below, it allowed characters like “%%32%65” to be decode to “%2e” and decoded unreserved characters twice:

/cgi-bin/%%32%65%2%65/bin/sh

* Normalize: /cgi-bin/%2e%2e/bin/sh
* Decode: /cgi-bin/../bin/sh

Then, the access was granted and given to CGI (common gateway interface) handler for execution. (Updated: Apache Software Foundation releases version 2.4.51 that fixes those vulnerabilities.)

[Text

Description automatically generated](https://twitter.com/roman_soft/status/1446252280597078024?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1446252280597078024%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fblog.desdelinux.net%2Fvi%2FtC3ACm-thE1BAA5y-mE1BB99t-lE1BB97-hE1BB95ng-trong-apache-mC3A1y-chE1BBA7-http%2F)

# **Samsung apologises for Russian app download error**

10/8 | Samsung apologises for Russian app download error| [link](https://www.bbc.co.uk/news/technology-58843162)| October 8, 2021| Jane Wakefield

**Quick Summary:** Samsung has issued an apology for a software update delivered to UK users that stated Russian government-mandated applications had been installed.

**Key Quote:** “After the installation had completed, he noticed the wording which read: "As part of the implementation of the requirements of the decree of the government of the Russian Federation No 1867 of 18/11/2020, the download of mandatory applications has been added. Some of these apps will only be installed if the device is reset to factory settings."”

“It offered an insight into how Samsung was dealing with the Russian law.”

“Russia has tightened its rules on the internet in recent years, including requiring search engines to delete some results and calling on messaging services to share encryption keys”

**Reflection:** This article reminds me of my friend who is studying abroad in Russia. So, I asked him about that, and he shared that he just bought a new iPhone this July. When he activated the phone for the first time, it asked him to install apps (around 16) that Russian developed. Some of the applications Apple provided using the Mir payment system that competitor to Visa and Mastercard. In addition, some software is from Yandex – a Russian search engine like Google. However, different from Samsung, Apple allowed him to choose not to install those apps if he did not really want, he said.

These applications are required to pre-install not only on phones but also on Smart TVs, laptops, and tablets. The law about pre-installation of Russian software on devices was signed by President Vladimir Putin in December 2019. So, I wonder if this country is trying to increase the influence of government-controlled on the Internet like the way China does in several years.

# **Railroads say they don't need cybersecurity mandates**

10/12 | Railroads say they don't need cybersecurity mandates| [link](https://www.washingtonpost.com/politics/2021/10/07/railroads-say-they-dont-need-cybersecurity-mandates/) | October 7, 2021| Aaron Schaffer

**Quick Summary:** The Bide n government intends to put new cybersecurity rules on railways and rail transportation networks, but these regulations are a shock, and a major railroad organization is opposing the idea.

**Key quotes:** “The new mandates on “higher-risk’’ railroad and rail transit systems represent an expansion of the government’s regulatory push beyond the country’s pipelines”

“Hackers have targeted transit operators around the country.”

“There’s “no better example of how the cybersecurity threat can impact our lives than in the transportation sector and how people commute, see one another, engage with one another,” ”

**Reflection:** I had never heard about railroad systems that can be attacked by hackers. So, when I saw this article, I felt like whoa it was interesting to get to know more, and after that, I decided to search for other articles or news related to rail systems and hackers or ransomware. And then, I found out the news that said the Ministry of Transportation website was collapsed by hackers on July 10. Computer systems of employees of the Ministry of Roads and Urban Development had been attacked, making the portal of the Ministry and the affiliate sites were inaccessible.

I think rail systems are attacked is extremely dangerous. There are billions of people using trains or metros to move around every day. Although trains are fast, convenient, and comfortable, it is also a target of cyber-attacks. Rail services may be severely interrupted, and customer data may be taken, resulting in significant economic harm. Even the safety of people is endangered.

# **Sunderland University IT systems down in possible cyber attack**

10/13| Sunderland University IT systems down in possible cyber-attack| [link](https://www.bbc.com/news/uk-england-tyne-58895850)| October 13, 2021

**Quick Summary:** Sunderland University is collaborating with the police and other organizations to resolve the situation. The institution treated system security very seriously. Moreover, Sunderland University canceled all online lectures while their website was being serviced.

**Key Quotes:** “Sunderland University has been hit by "extensive IT disruption" which has "all the hallmarks of a cyber-attack".”

“Sunderland University has been hit by "extensive IT disruption" which has "all the hallmarks of a cyber-attack".”

**Reflection:** This article reminds to one experience that happened on this September. I got the mail from IT solution that said there was a very realistic looking malware scam called “Shlayer” affecting many students using Apple/Mac computers. Although I did not use Mac computer, this mail was helpful. Its content included how Shlayer malware looked, how to prevent this malware, and what this malware did. Moreover, if students wondered whether they did have malware on their machines or had malware and wanted help removing it, IT solutions could help them by calling, chatting, or meeting face to face.

Malware has been very tricky and dangerous, so we need to know how to react when attack happens or prevent the malwares. For example, Shlayer uses “Adobe Flash Player update” to add a malicious extension to Safari web browser and secretly collects users’ data. Thus, users should be careful when clicking any updates that are not from Apple or App Store especially from Adobe Flashing Player (it has been discontinued). Beside it, users should update computer’s software and application frequently and scan regularly to check for and stop malware.

# **iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security**

10/18| iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security| [link](https://www.forbes.com/sites/daveywinder/2021/10/18/iphone-13-pro-hacked-chinese-hackers-suddenly-break-ios-1502-security/?sh=2e045b341fe6&fbclid=IwAR3EyxmqpjQjLy8GrdIPjmhWbt0fTLf7ZDe6z_qYf8rmOUjvZRSpgVyVqpw) | October 18, 2021| Davey Winder

**Quick Summary:** The Kunlun Lab team attacked the iPhone 13 Pro by utilizing RCE (remote code execution) in about 15 seconds. Team Pangu was also able to compromise the iPhone 13 Pro by activating a one-click link that circumvented Safari’s security safeguards. However, Apple will release new versions to patch security vulnerabilities.

**Key quotes:** “Kunlun Lab wasn't the only team to hack the iPhone 13 Pro, though. Team Pangu, which has a history of Apple device jailbreaking, cemented its reputation in this regard by claiming the top $300,000 cash reward for remotely jailbreaking a fully patched iPhone 13 Pro running iOS 15.”

“The not so good news is that there have been reports in the past of Chinese state actors using some of these exploits for espionage or surveillance purposes before patches can be released.”

**Reflection:** When reading that article, I looked for more information about “remote code execution” and knew that attack relies on a vulnerability in the system to remotely access the victim’s computer or computer network. So, the hacker could execute malicious code or malware on the victim’s device without having direct contact with the device.

While I see this title, there are two questions that popped up in my mind. Why can hackers easily break security iOS 15.0.2 in just 15 seconds while Apple – a company for many years has tried the image that its native ecosystem is more secure than others thanks to many features such as it is a closed-source, or a propriety use of Apple-owned hardware? Another is android phones are safer than iPhones. After researching for a while, I realized that the main barrier against cybercrime is us.

Most attacks that occur daily, take place using social network, such as phishing. Thanks to doing labs on CIS 450, I know that my caution is key when it comes to protecting my data. I always check the legitimacy of my email senders, and make sure I don’t give my private or access data on sites that do not have the required SSL certificates. I avoid the temptation to use a public Wi-Fi network without encrypting my connection privately. I think these actions can make a significant difference in protecting me from any future attacks.

# **US warns that Chinese government is using 'wide variety' of methods, some illegal, to steal trade secrets**

10/23/2021 | US warns that Chinese government is using 'wide variety' of methods, some illegal, to steal trade secrets | [link](https://www.cyberscoop.com/china-ai-quantum-national-security/) | Oct 22, 2021 | AJ Vicens

**Quick summary**: The Chinese government intends to become the worldwide leader in A.I technology within the next decade, and that threat is especially dangerous to US national security. Therefore, the U.S recommended businesses to take precautions to protect and be careful with phishing efforts. However, the U.S is “very hooked” on Taiwan’s company for quantum computing processors. (Vicens, 2021)

**Key quotes:** “its “well-resourced and comprehensive strategy,” which employs “a wide variety of legal, quasi-legal, and illegal methods” in pursuit of both technology transfers and intelligence gathering, the notice warned.”

“This information transfer takes place in the shadows—through traditional intelligence activities, intellectual property theft, co-opted insiders, front companies”

“U.S. is “heavily dependent on a single company in Taiwan for producing its leading-edge chips, and has significant dependence on China for mature node logic chips.” Disruptions to that supply chain risk both economic and security issues”

**Reflection:** I heard that China intended to become a world leader in artificial intelligence (AI) by 2030, with the goal of creating estimate over $100 billion economy from the news broadcasted on tv. Indeed, I can feel like China’s high-tech corporations are increasing their investments in AI technology. For example, Baidu has AI research lab in Silicon Valley and is exploring areas like driverless car technology. Meanwhile, Alibaba is focusing mainly on applying AI in areas from shopping to healthcare. (Kharpal, 2017). However, in my opinion, the transformation that Internet and new technologies creates affects human society whoever wins the race for A.I. The most obvious example is that some jobs can be totally replaced by technology (e.g.: accountant), resulting in employees losing their jobs or having their earning reduced.

# **Ransomware Gangs Earned $590 Million in H1 2021**

10/25/2021 | Ransomware Gangs Earned $590 Million in H1 2021| [link](https://cyware.com/news/ransomware-gangs-earned-590-million-in-h1-2021-1b5964a1/) | Oct 24, 2021| Cyware Alerts

**Quick Summary:** Ransomware has been one of the most significant cybercrime risks for cryptocurrencies. The groups behind this attack are said to be REvil, DarkSide, Conti, Phobos, and Avaddon. To prevent centralization, ransomware attackers ask for payments in bitcoin, using distinct bitcoin addresses, and they hide their money through centralized exchanges.

**Key quotes:** “Almost $5.2 billion worth of outgoing Bitcoin transactions have been observed by FinCEN. This amount is possibly linked to the top 10 most reported ransomware strains.”

“Bad actors mainly use foreign centralized exchanges to deposit their illegally earned money. Non-compliant centralized exchanges are believed to be a major component in the layering process of money laundering.”

“The practice of chain hopping is followed to obfuscate the origin of the funds. Chain hopping refers to converting one CVC to another at least once before transferring the funds to a different platform.”

**Reflection:** I don’t know about Bitcoin much, but I have a chance to see how my uncle makes bitcoin transactions. So, I can tell the reason why Bitcoin or other anonymous cryptocurrencies cause a ransomware boom. Bitcoins works differently from typical currencies. There is no central bank to manage it and the payment is convenient and fast. The hackers can simply look at the public blockchain to see if and when the victim has paid. Moreover, it is very difficult to trace and know who the hacker is or criminal or who the normal user is because the payment is anonymous.

A common question when dealing with ransomware problems is should the victim pay a ransom to get the data back when infected with ransomware? My opinion is “should not” because it only encourages hackers to create more ransomware. In addition to paying the ransom, there are also some tools dedicated to decrypting files locked by ransomware although the recovery may not be successful completely. When I search with key “decrypt file tools” on Google, I can see a lot of helpful tools such as Alcatraz Locker, BadBlock, AES\_NI, BTCWare, EncrypTile, Apocalypse, CryptoMix, …

However, prevention is better than cure. Do not install software or give it administrative rights unless we know exactly what it is and what it does. We can use a USB or external hard drive to store the new or updated files.

# **Cheap and free cybersecurity training: 8 ways to build skills without breaking the bank**

10/27/2021 | Cheap and free cybersecurity training: 8 ways to build skills without breaking the bank

|[link](https://www.csoonline.com/article/3340819/cheap-or-free-cybersecurity-training-resources.html) |Oct 26, 2021| Josh Fruhlinger

Quick Summary: Internal training is a good choice for any organization that would like to boost up their employees’ cybersecurity skills instead of other high-cost ways. Companies might save training expenditure by utilizing internal resource and match senior and younger personnel in order to assist teach knowledge across generations. Other low-cost training can be online course, learning from the experience of others or from the vendors.

Key quotes: “… less formal ways in which employees at companies with fewer resources can help keep each other's skills up to date.”

“There are plenty of free and low-cost resources out there, and several sites and courses came up repeatedly with the experts we spoke to”

Reflection: Indeed, internal training gives a lot of benefits to organizations. Besides these effects, the companies no longer must spend more money to hire people with talents equivalent to their own employees. The employees in the companies after the internal training process will also become more engaged and loyal, helping businesses in retaining employees.

I agree the online course is a good way too. For example, this summer, I wanted to learn more about how to build the website so I decided to register for one online course – [Codecademy](https://www.codecademy.com/?g_network=g&g_device=c&g_adid=528849219079&g_keyword=codecademy&g_acctid=243-039-7011&g_adtype=search&g_adgroupid=70946090375&g_keywordid=kwd-41065460761&g_campaign=US_Brand_Exact&g_campaignid=1955172604&utm_id=t_kwd-41065460761:ag_70946090375:cp_1955172604:n_g:d_c&utm_term=codecademy&utm_campaign=US_Brand_Exact&utm_source=google&utm_medium=paid-search&utm_content=528849219079&hsa_acc=2430397011&hsa_cam=1955172604&hsa_grp=70946090375&hsa_ad=528849219079&hsa_src=g&hsa_tgt=kwd-41065460761&hsa_kw=codecademy&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAiAnO2MBhApEiwA8q0HYXR1s_VPgSti20TTcJhf-y0tUdpmr7DBBHQ5dZdNeAK2KyzKIUVWlxoCoYAQAvD_BwE). It was free but if you want to do more practice exercises or do more projects in courses, you can buy the annual plan costed around $100. After three months, I see codecademy as a great way to learn a programming language. It explains every step and then it asks you to do exercises by yourself to see how you understand. You can test your code there without the necessity of downloading any extra software. It also has cyber courses. Two other cyber security courses online I find with highly recommendations are Udemy, Coursera.

# **Cyber-attack hits UK internet phone providers – Tram Nguyen**

11/1/2021 | Cyber-attack hits UK internet phone providers| [link](https://www.bbc.com/news/technology-59053876)| October 26, 2021|

**Quick Summary:** A DDoS attack has targeted various UK-based suppliers of voice over internet protocol (VoIP) services in recent weeks.

**Key quote:** “Ransom threats have been made to numerous providers and an overall threat has been made to the entire industry.”

“By exploiting weaknesses in VoIP, this wave of attacks is actually a clever twist on the traditional DDoS approach.”

“Ransomware is more usual for criminals extorting money at present.”

**Reflection:** Thanks to CIS 350 course I took at the last semester, I can know three common types of DDoS (distributed denial-of-service) are protocol attacks, application layer attacks, and volumetric attacks. So, in this article, DDoS uses the protocol attack. It takes advantage of the 3 TCP handshakes processes – SYN, SYN-ACK, ACK. The attack sends an SYN request to the server and is responded with an SYN-ACK packet but does not send the ACK packet back. This causes the server resources to be used up waiting for the ACK packet to be sent.

The ways to avoid the attack are the same as I said in the “Ransomware Gangs Earned $590 Million in H1 2021” article above. In addition, for DDoS attacks, you should check your network traffic often. This way can help you detect small DDoS attacks that hackers often use to test the network before an actual attack. If you can determine the addresses of the computers performing the attack, it is possible to create an access management list in the firewall to block these IPs. And Wireshark is a good choice for analyzing network traffic.

# **Database firm Clearview AI told to remove photos taken in Australia**

11/4 |Database firm Clearview AI told to remove photos taken in Australia| [link](https://mnscu-my.sharepoint.com/personal/rz9644xr_go_minnstate_edu/Documents/Assignment%203%20-%20CIS%20350.docx)| BBC News

**Quick Summary:** Clearview AI has violated Australia's privacy rules by allowing police enforcement to scan its database of faces.

**Key Quotes:** “The OAIC found the firm's breaches of the Australian Privacy Act included:

* collecting sensitive information without consent
* collecting personal information by unfair means
* not notifying individuals of the collection of personal information
* not ensuring that personal information it disclosed was accurate”

**Reflection:** One thing I am astounded when knowing who CEO of Clearview AI is. Hoan Ton-That has Vietnamese and Australian blood. His father's family was derived from Vietnam's Royalty. I am so more surprised to know about his achievement. Mr. Ton-That was top solo contestant in Australia’s Informatics Olympias as a student. Being a Vietnamese, I am quite proud and impressed by his talent.

However, as a user of social networks, I also do not want my images or videos to be used without my consent even if they are used to help whatever cause. The collection of this sensitive information is an unreasonable and unfair invasion of privacy. If personal photographs are widely searchable on the Internet, this can cause significant harm to individuals, extremely sensitive populations such as children and abuse victims. Although Mr. Ton-That objects to the Australian ruling and claims his company’s product is an important tool for justice and it only collects public data, a person who has nothing to hide still feels uncomfortable with facial recognition since it violates their right to privacy.

# **Widespread Vulnerability Identified in Phones and Bluetooth Devices**

11/8| Widespread Vulnerability Identified in Phones and Bluetooth Devices| [link](https://spectrum.ieee.org/bluetooth-security#toggle-gdpr)| November 4 2021| Michelle Hampson

**Quick Summary:** Research teams uncovered a flaw in Bluetooth devices that enable an approximate 40% of phones to be uniquely identified. It also means an attacker only needs to seek out the fingerprints of many devices used by the target to trace it down. Givehchian's team is looking at security methods that would make it impossible for an attacker to distinguish the device's unique identifier. Furthermore, near the end of this article, the author updates that this issue only impacts short-range devices.

**Key Quotes:** “Unfortunately, this also means that an adversary can also find out where we are at all times by simply listening to the Bluetooth transmissions from our personal devices.”

“A device that is distinguishable among thousands of other devices can be tracked effectively across wireless conditions if it has a distinct enough identity.”

**Reflection:** I never thought Bluetooth could be attacked, so this article was interesting for me. I searched more information about how to Bluetooth could be compromised. I found out five different Bluetooth hacks and vulnerabilities, and how to prevent them. However, their commons are that hacker paired with Bluetooth device without victim’s consent, and the attack only work if the device had Bluetooth turned on. While vulnerability was exploited, hacker would steal or compromise victim personal or sensitive information. There are 4 safety tips I collect after researching. Firstly, do not turn on Bluetooth function when not needed, do not accept pair requests from unfamiliar devices, make sure always have the lasted system software, and ensure that our purchased device has suitable security features.

Furthermore, with low-cost Bluetooth devices, there are frequently no security measures in place when designing these products. As a result, these products are compromised easily by hackers. It will be considerably more perilous for devices that use Bluetooth to unlock automatically. A smart lock that unlocks your front door as soon as you step onto the porch is fascinating and futuristic, but it also makes it easily accessible. That causes me concern if someone steals my phone, and that person will suddenly be able to enter my house without knowing the passcode.

# **Apple digital ID scheme comes with conditions and costs**

11/16| Apple digital ID scheme comes with conditions and costs| [link](https://www.bbc.com/news/technology-59292649)| November 15, 2021| BBC News

**Quick Summary:** Apple has a partnership with states to issue digital IDs to license holders. State authorities are required to publicize the feature, but Apple has final say over the advertising material. In addition, states have "given Apple a frightening degree of influence" by allowing it to manage its technological systems at expense of the taxpayer.

**Key Quotes:** “State bodies must employ or allocate people and resources to support the project "on a timeline to be determined by Apple" and, if Apple requests, "designate" project managers to answer Apple's questions”

“The digital ID must be "proactively" offered to every new license holder or renewal at no extra cost to the person applying”

“When Apple announced the first details of its ID scheme, it emphasised the encryption and other security features, stressing neither the company nor state officials could know "when or where" users showed IDs.”

**Reflection:** In my opinion, Apple allows users have or not be charged to renew digital IDs of their driver licenses in the Wallet app that makes Apple’s product more important and sells better than competing brands. In addition, this article also mentions the digital Covid password that has caused strong public opposition in many countries. Personally, I believe that personal information privacy should be the foundation of vaccine or other certification development. It must ensure users are protected from data exploitation, manipulation, and privacy violations of personal data. Besides it, the unknown duration of vaccine-induced immunity, as well as the danger of the emergence of new SARS-Cov-2 variations with the potential to escape the vaccine’s protective effect, raise concerns about the length of the vaccine certificate. Whether or not the holder of the certification is immune to virus strains that are currently infected.

# **All Versions of Windows Are Vulnerable to a New Zero-Day Exploit**

11/24| All Versions of Windows Are Vulnerable to a New Zero-Day Exploit| [link](https://www.pcmag.com/news/all-versions-of-windows-are-vulnerable-to-a-new-zero-day-exploit)| November 24, 2021 |Matthew Humphries| threat post

**Quick Summary:** A security analyst discovered a new weakness in Windows Operating system that might allow the user to get elevated access. The Microsoft update for CVE-2021-41379 was still not done consistently, allowing an attacker to circumvent group policy, and run code as an admin.

**Key Quotes:** “The original vulnerability allowed a user with a limited account to escalate their privileges and delete targeted files on a system. This new vulnerability looks to be more serious, though.”

“The knock-on effect being that an attacker can replace any executable file on the system with an MSI file and can run code as an administrator.”

“The only action users can take is to wait for Microsoft to release another security patch because of the complexity of the vulnerability, and "any attempt to patch the binary directly will break windows installer."”

**Reflection:** After reading this article, I know the new thing – the zero-day attack. Zero-day vulnerabilities are the term for unknown and unresolved software or hardware vulnerability. Hackers can take advantage of this vulnerability to attack and infiltrate the computer systems of businesses and organizations to steal or change data. Normally, after discovering a 0-day vulnerability, the product supplier will release a security patch for this vulnerability to make users better secure. However, users rarely update the new version of the software immediately. That makes zero-day known as very dangerous that can cause serious damage to businesses and users.

According to the video "What are zero-day attacks?" I saw on YouTube, three popular cyber-attacks include online browsers, email attachments, especially if the user downloads and accesses the attachment, and file formats – Word Documents, Excel, Pdfs, or Flash. As a result, there are some precautions I take to avoid assaults. I maintain my program update with the most recent new versions and releases; I also install the most recent security fixes, which solve vulnerabilities that were detected in prior versions. Another thing I do is downloading antivirus software to assist block and avoid any attacks. I use an IDS (Intrusion Detection System) to defend my system from both known and unknown attackers. It may not always detect threats, but it will alert you to questionable hacker activity.

# References

*Apple digital ID scheme comes with conditions and costs*. (2021, November 15). Retrieved from BBC News: https://www.bbc.com/news/technology-59292649

*Cyber-attack hits UK internet phone providers*. (2021, October 26). Retrieved from BBC News: https://www.bbc.com/news/technology-59053876

*Database firm Clearview AI told to remove photos taken in Australia*. (2021, November 3). Retrieved from BBC News: https://www.bbc.com/news/technology-59149236

*FBI Raids Chinese Point-of-Sale Giant PAX Technology*. (2021, October 26). Retrieved from Krebs on Security: https://krebsonsecurity.com/2021/10/fbi-raids-chinese-point-of-sale-giant-pax-technology/

Fruhlinger, J. (2021, October 26). *Cheap and free cybersecurity training: 8 ways to build skills without breaking the bank*. Retrieved from CSO: https://www.csoonline.com/article/3340819/cheap-or-free-cybersecurity-training-resources.html

Hampson, M. (2021, November 4). *Widespread Vulnerability Identified in Phones and Bluetooth Devices* . Retrieved from IEEE Spectrum: https://spectrum.ieee.org/bluetooth-security#toggle-gdpr

Humphries, M. (2021, November 24). *All Versions of Windows Are Vulnerable to a New Zero-Day Exploit*. Retrieved from PCMag: https://www.pcmag.com/news/all-versions-of-windows-are-vulnerable-to-a-new-zero-day-exploit

Kharpal, A. (2017, July 21). *China wants to be a $150 billion world leader in AI in less than 15 years*. Retrieved from CNBC: https://www.cnbc.com/2017/07/21/china-ai-world-leader-by-2030.html

*Ransomware Gangs Earned $590 Million in H1 2021*. (2021, October 24). Retrieved from Cyware Alerts - Hacker News: https://cyware.com/news/ransomware-gangs-earned-590-million-in-h1-2021-1b5964a1/

Schaffer, A. (2021, October 7). *Railroads say they don't need cybersecurity mandates*. Retrieved from The Washington Post: https://www.washingtonpost.com/politics/2021/10/07/railroads-say-they-dont-need-cybersecurity-mandates/

*Sunderland University IT systems down in possible cyber attack*. (2021, October 13). Retrieved from BBC News: https://www.bbc.com/news/uk-england-tyne-58895850

Toulas, B. (2021, October 5). *Apache fixes actively exploited zero-day vulnerability, patch now*. Retrieved from Bleeding Computer: https://www.bleepingcomputer.com/news/security/apache-fixes-actively-exploited-zero-day-vulnerability-patch-now/

Vicens, A. (2021, October 22). *US warns that Chinese government is using 'wide variety' of methods, some illegal, to steal trade secrets*. Retrieved from CyberScoop: https://www.cyberscoop.com/china-ai-quantum-national-security/

Wakefield, J. (2021, October 8). *Samsung apologises for Russian app download error*. Retrieved from BBC News: https://www.bbc.com/news/technology-58843162

Winder, D. (2021, October 18). *iPhone 13 Pro Hacked: Chinese Hackers Suddenly Break iOS 15.0.2 Security*. Retrieved from Forbes: https://www.forbes.com/sites/daveywinder/2021/10/18/iphone-13-pro-hacked-chinese-hackers-suddenly-break-ios-1502-security/?sh=2e045b341fe6&fbclid=IwAR3EyxmqpjQjLy8GrdIPjmhWbt0fTLf7ZDe6z\_qYf8rmOUjvZRSpgVyVqpw