# Backdoor Attacks

**Vinoshan Thevananthan**
*Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka*
*it20238780@my.sliit.lk*

## ABSTRACT

This study mainly focuses on the Backdoor vulnerability. This study thoroughly describes, what is a backdoor vulnerability, how it works, examples of backdoor attacks, how hackers/malicious actors try to exploit it, what can hackers/malicious actors do with a backdoor, and the best practices or ways to protect from backdoor attacks. At the end of this paper, there will be ten frequently asked questions about backdoor attacks.

***Keywords – Backdoor, Hackers, Android, Open Ports, Exploits, Payloads, Rootkits, Naive Users, Malware, Prevention***

## INTRODUCTION

Backdoors in legitimate applications allow attackers to gain access to users' personal information and launch remote assaults without having to download malicious files to the target device. Some passive backdoor behaviors, on the other hand, are quite dangerous. They resemble typical behaviors and are difficult to spot. Android users and the majority of harmful behavior detecting systems. A backdoor is a security feature that allows an unauthorized user to access your device without your knowledge or consent. Backdoors can be added to the system in two distinct ways (Martens, 2022):

- Hardware/ Firmware: Any physical alteration allows for remote access to the device.
- Software: Malware files that mask their traces, so the operating system doesn't realize someone else is using the system.

Most of the backdoors are being installed in the devices or built with the application/ software by the developers or technical support team for any remote tech support, but there are instances where the backdoors are being installed in the devices by the malicious actors/ hackers or by the invasive government as with the motive of gaining root access to the devices, networks, or any software applications or to steal user information and data or install malware with the motive of ransom.

Long story, in short, we can say that any malware that allows hackers or any malicious actors to gain to the device can be considered the backdoors, this includes rootkits, trojans, spyware, and cryptojackers, worms, keyloggers, spyware.

# HOW DO BACKDOOR ATTACKS WORK?

For successful exploitation of the backdoor, the hacker/ malicious actor should gain the access to the device as the first step. This can be done by the hackers/ malicious actor using physical access or by a malware attack or by exploiting system or software vulnerability. Hackers/ malicious actors mainly focus on the system/software vulnerability that is inbuilt within them. Some of the common vulnerabilities that come as the target of the hackers or malicious actors are:

- **Open network Ports**: Open ports are an easy entry point for the malicious actors or hackers in-order to exploit since these open ports may accept traffic from remote locations. If there are any unused open ports hackers / malicious actors may use those ports to install their backdoor for the attack since they won't be noticed by any intrusion detection.
- **Weak passwords**: Having weak or default or basic or guessable passwords without any password policies may help the hackers immediately gain access to the device or network.
- **Out-of-date software:** Hackers/ malicious actors may exploit the vulnerabilities that are found in the out-of-dated software and may use those vulnerabilities to install a backdoor in the device.
- **Weak firewalls:** Having firewalls that can't detect or monitor incoming outgoing traffic signals and block any malicious activity may lead to some serious issues since it will be easier for the hackers/ malicious actors to get into the system.
- **Hidden/ Legitimate backdoors:** These are the backdoors that are created or installed intentionally by the developers to provide tech support to the users, if there are any instances where those backdoors are not properly secured or implemented with the proper security it may allow the malicious actor/ hackers to gain access towards the system easily.
- **Naive Users**: This is the vulnerability that has been widely exploited by the hackers/ malicious actors since it is not technical just psychological. This vulnerability is depending on human error. If an end-user clicks on unknown links or malicious links or downloads any third-party software, it allows the hackers/ malicious actors to come into the network and install a backdoor.

Most hackers/ malicious actors direct their attacks towards the above-mentioned vulnerabilities to gain the access and installation of backdoors (it is more likely to target the software that interacts with the internet or with the same public network since it is easier to gain access). Else hackers/ malicious actors may use their own built malicious websites or ads which appear like a popup that scans the system's exploitable vulnerabilities and they might use those ways as an entryway to the systems.

As the next step of the entry, the hacker/ malicious actor may exploit those vulnerabilities and install the backdoor. The hacker/ malicious actor can use the system's backdoor to steal the data or create an interrupt in the system.

Backdoors can be varied according to their nature, and they are:

- **Trojans**: Trojans are malware that looks like a legitimate file, but they act like a legitimate file in-order to trick the users to gain access to the devices. Once the user allowed the trojan in the device, it will install itself on the device without the knowledge of the user and open a backdoor which allows the malicious actor or hacker to gain access to the device also it may allow installing other serious or next level malware or virus or any other harmful things on the device.
- **Rootkits**: Rootkits are advanced-level malware that may hide its activities and operations from the operating system to gain the system/ root-level privileges from the operating system. These rootkits make the path for the malicious actors or hackers to access the infected device remotely and do alterations, steal data, observe the user activities, or create interruption. These rootkits can be either software or physically altered chips.
- **Hardware Backdoors**: Malicious actors or hackers can gain access to a device using hardware backdoors, which are changed computer chips Phones, IoT devices such as thermostats and routers, and laptops. Hardware backdoors can be delivered with products (either by a rogue manufacturer or for a good cause), but they can also be manually inserted if a device is stolen.
- **Cryptographic Backdoors**: Using the cryptographic backdoors is a master key that can be used to decrypt the encrypted data which uses a specific protocol. These backdoors are used to decrypt the end-to-end secure conversations and also by manipulating the protocols it may grant access to the malicious actors or hackers to gain access to all encrypted data that is being shared.

## PAST BACKDOOR ATTACKS

Backdoor attacks are the most dangerous attack that can happen on a system since they can deal serious damage to system and user data. With the evolution of technology these attacks are also becoming more sophisticated and dealing more damage. Let's see some of the backdoor attacks that happened in real life.

- **DoublePulsar crypto-jacker**: In 2017, the US national security agency created malware named DoublePulsar, which was identified that it is being used in the monitoring of Windows PCs, and installation of cryptojacker on the computers with sufficient memory and CPU power. This installed cryptojacker stole the processing power of the infected computers to mine Bitcoin and also it has been identified that tens and thousands of those PCs are being used in a massive crypto-mining botnet.
- **Dual_EC (NSA cryptographic backdoor)**: Dual_EC is an encryption cryptographical protocol, which is used to encrypt user data. But it was created with a backdoor which is, high-level users with the secret key to decrypt. In 2013, Edward Snowden revealed that US NSA has possession of these keys and used this backdoor to decrypt and read all the communication done through the Dual_EC. Companies like Blackberry, RSA, Microsoft, and Cisco are some of the companies that used Dual_EC in products that have millions of users.

- **Poison Tap**: A serious backdoor malware that has been created by a hacker named Samy Kamkar, which allows any hackers/ malicious actors to access almost any websites which also including sites with 2FA authentication. This malware is one example of hardware path malware since this backdoor can be only installed in the system by plugging a Raspberry Pi computer into the victim's USB directly.
- **Mirai botnet**: In 2016, There was a massive DDoS attack on the U.S East coast where everyone is left with inaccessible internet. Mirai exploited unsecured IoT devices by checking the large parts of the internet for open Telnet ports and then attempting to log in using default passwords. It was able to amass a botnet army this way and did a massive DDoS attack.
- **ES file manager (CVE 2019-6447):** In Android, When the ES file manager is opened and the ES file browser in the background creates an open HTTP service on port 59777 at runtime which opens a backdoor that allows any malicious actors or hackers to access more than 10+ privacy-related data of the user and enable to download too. It also allows running any application on the mobile.
- **AdUps backdoor:** In 2016, it has been found out more than 700 million android phones in the U.S identified with a pre-installed backdoor malware under the AdUps software which automatically sends SMS messages, contacts, users' PIIs, logs, geolocation, and other private information to the AdUps every 72 hours. It has been also found that this backdoor is capable of remotely installing and updating applications of that smartphone. Vendors like ZTE, Huawei, and Blu are smartphone vendors identified with this backdoor. Though the motive was unclear whether this data is collected for advertising purposes or government surveillance.

## WHAT CAN CYBER-CRIMINALS DO WITH A BACKDOOR?

Backdoor attacks can be both serious and fun it depends on the motive of the malicious actor/ hacker. If it is fun-motivated, they might play tricks on the user like opening apps randomly hiding files on so on, but if the motive was in a harmful way it may adversely cost the user/ victim. With the backdoor access, the hackers / malicious attackers can perform malicious activities like DDoS attacks, sending and receiving files, messing with the system settings, stealing private information and data like contacts, images, videos, documents, geo-location, and so on.

In addition to these with the installation of the backdoor, hackers can remotely access the device and download and transfer the private data of the victim to a C&C server. Sometimes the use of a backdoor to take control of the victims' system and lock the user documents with a secret key and blackmail the victim for a handsome ransom.

As a real-life incident, we can take Edward Snowden and the U.S NSA incident. He has revealed that U.S National Security Authority has forced the backdoors into many electronic communication devices and even in a widespread cryptographic protocol like Dual_EC and eavesdropping on conversations, accessing cameras, and microphones without users' knowledge. Further, it revealed that they have even gathered users' data remotely.

# BEST PRACTICES TO PROTECT AGAINST BACKDOOR ATTACKS

Backdoors often stay hidden under any software or they will stay without anyone or anything's attention due to this it is impossible to track and get them. Backdoors cannot be identified easily by using task manager as we do for other attacks like trojan, viruses, and so on. Though it cannot be 100% eradicated, it can be prevented by following some basic steps.

- **Anti-Virus Software:** The system should be installed with any antivirus software which can identify a wide range of malware like trojans, viruses, spyware, crypto-jackers, and rootkits. The anti-virus should be capable of identifying this malware before they infect the system and get rid of them as soon as possible. If the antivirus is enabled with the features like Wi-Fi Monitoring, Web protection, and privacy breach detection (microphone, camera) it will be much better for preventing backdoor
- **Being cautious using the Internet:** When downloading files to the system, that file must be double-checked. Downloading any software other than the open-source software for free there is a high chance it may have attached with any backdoor. Downloading from official authorized sites may reduce the high risk of backdoor, there is many pirate sites' software with backdoors enabled. Good common sense while browsing might eradicate many issues.
- **Using of Advanced Firewall:** Firewalls are the basic protection that any system can get against backdoor but still, some backdoor attacks can bypass the basic firewalls so implementation of the advanced firewall may come in handy. That firewall should be able to filter the incoming and outgoing traffic in the network also it should not allow any external devices sending data to the network remotely which are unfamiliar to the network. Having a physically installed firewall can also be an advantage.
- **Password Manager:** Password managers will store the login information of the websites and other apps in 256-bit AES encryption in a secure manner which may help you to login into those sites and apps automatically without re-entering the passwords. The password manager is locked behind a master key which only the user might know sometimes that master key also can be protected using the 2FA authentication as well as in addition to numerical and letter, the master key can be biometric of the user which is not replicable. So, in an event of a backdoor attack, it will be harder for the attacker to gain the encrypted passwords of the user.
- **Up to date on the Security updates and vulnerabilities:** Due to the huge development in the technology world and cyber world day to day, there are many vulnerabilities identified and many exploit6s created. So, it is necessary to stay updated about the vulnerabilities and their patches. Keeping the OS updated and applications patched and updated will help to protect the system against attacks. Dark-web monitoring can also help to warn if any data of ours is breached and leaked.

# QUESTIONS ABOUT BACKDOOR ATTACKS

? **What is a backdoor?**
- A backdoor is any method that hackers/ malicious actors can use to gain access to a victim's system without his/ her knowledge.

? **Name two distinct ways that the backdoor can be added/ installed into the system?**
- Hardware/ firmware - Any physical alteration allows for remote access to the device.
- Software: Malware files that mask their traces, so the operating system does not realize someone else is using the system.

? **Name the malware which allows any malicious actors/ hackers to install a backdoor to the system?**
- Rootkits
- Trojans
- Spyware
- Keyloggers
- Crypto-jacker
- Worms
- Ransomware

? **What are the common vulnerabilities that hackers/ malicious actors might like to exploit to install a backdoor?**
- Open Ports
- Weak passwords
- Out-of-date software
- Weak firewalls

? **Name some past events related to backdoor attacks?**
- DoublePulsar Crypto-jacker – 2017
- Dual_EC cryptographic backdoor – 2013
- PoisonTap
- ES file manager – 2019
- AdUps - 2016
- Mirai Botnet – 2016

? **What is meant by hardware backdoor?**
- Malicious actors or hackers can gain access to a device using hardware backdoors, which are changed computer chips Phones, IoT devices such as thermostats and routers, and laptops. Hardware backdoors can be delivered with products (either by a rogue manufacturer or for a good cause), but they can also be manually inserted if a device is stolen.

- **What do hackers/ malicious actors do with the backdoor?**
  - It depends on the motive of the attacker if his/ her motive was fun then he or she might play pranks or tricks on these friends or family like opening random apps pop upping banners whereas the intention is malicious with the sophisticated nature of the backdoor it may vary. DDoS, Data theft, Ransom, and eavesdropping by accessing cameras and microphones are some of the malicious intentions examples

- **How to protect the system from backdoor attacks?**
  - Anti-virus
  - Using the internet with caution
  - Using advanced firewall
  - Using password manager
  - Stay updated on security updates.

- **What are the features that should be available in the Anti-virus software to protect against backdoor attacks?**
  - The anti-virus software that is selected to protect from the backdoor attack should have features like identification of a wide range of new and old malware including trojans, viruses, keyloggers, spyware, and rootkit. In addition to this, the anti-virus software must have Wi-Fi monitoring, a good firewall system, web protection, and privacy monitoring of the microphone and camera.

- **How can an advanced firewall protect the system from a backdoor attack?**
  - Firewalls are the basic protection that any system can get against backdoor but still, some backdoor attacks can bypass the basic firewalls so implementation of the advanced firewall may come in handy. That firewall should be able to filter the incoming and outgoing new and old traffic in the network also it should not allow any external devices sending data to the network remotely which are unfamiliar to the network. Having a physically installed firewall can also be an advantage. If the advanced firewall is stepped with the above features if an intruder or malware tries to enter the network the firewall will block it and destroy it so, that the intruder can't access the network and install a backdoor.

# CONCLUSION

With the vast development of the technology, it is clear that the cyber threats in the industry are also day to day developing just like that. Cyber threats can't be eradicated but they can be avoided by using the common intelligence.

Attacks like Backdoor leads to a serious data leakage and a ransom threat. Backdoors are hidden and they are harder to find, the harder they are to find, the more danger they are. These backdoors attacks are mostly done again the system by the attackers due the human error or due to the outdated components in the system. Having vulnerabilities like weak password, open unnoticed ports, being naïve are some vulnerabilities that has been exploited to install the backdoor.

By having a proper security practices the backdoors attacks against the system can be protected. Using anti-virus software, using advanced firewall, password manager, staying up to date with the security news are some of the ways.

As per the Saying "PREVENTION IS BETTER THAN THE CURE"

# REFERENCES

[1] Aimin Zhang, Y. H. (2016). CrashFuzzer: Detecting Input Processing Related.

[2] Alejandro Argudo, G. L. (2017). Privacy Vulnerability Analysis for Android Applications.

[3] Ebin Thoppil, S. S. (2020). Android Device Hacking : TheFatRat and.

[4] Giorgio Severi, J. M. (2021). Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers.

[5] Junsung Cho, G. C. (2017). Open Sesame! Design and Implementation of.

[6] Martens, B. (2022). *What Is a Backdoor & How to Prevent Backdoor Attacks (2022)*. Retrieved from Safety Detectives: https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/#Attacks-Work

[7] XuweiXia, C. Q. (2016). Android Security Overview: A Systematic Survey.

[8] Yao Yao, L. Z. (2018). Real-time Detection of Passive Backdoor Behaviors .

[9] Yunhan Jack Jia, Q. A. (2017). Open Doors for Bob and Mallory: Open Port Usage in.

[10]Zheran Fang, W. H. (2014). Permission based Android security: Issues.

# AUTHOR PROFILE

**Thevananthan Vinoshan** currently following BSc (Hons) in Information Technology specializing in Cyber security at the Sri Lanka Institute of Information Technology. His current interest is in the vulnerability pen testing and current research interests include cyber security threats, deep learning, wearable security, the Internet of Things, big data, and biometrics