Google Project Zero

Kabeer Ahmed	SE-19028
Haris Aqeel	SE-19034
Daniyal Aamir	SE-19049

1. REPORT OBJECTIVES

The objectives of this report are:

- To examine the various features of the Google's Project Zero, including the motivation behind it, its objectives, its working, and the role it plays in enhancing the overall security of the open Internet wit the help of a case study.
- To discuss about "Zero-day Vulnerabilities", how they become serious security threats for potential users, and the risks associated with them.
- To outline some of the important statistical facts, and the contributions this project made to the society.

2. INTRODUCTION

Google Project Zero was announced in 2014. It was a group of security researchers, practitioners, and experts, which are appointed by google to study the untraced (previously unknown) vulnerabilities (also called as "zero day" vulnerabilities) in the applications which reside on the Internet. This is not limited to Google products only, but also covers much of the Internet. The goal of project zero is to make the open Internet safe, private, and secure.

2.1. Objectives of Project Zero

The objectives of Google Project Zero are:

- To identify much of the loopholes in the various products that make use of the Internet such as operating systems, hardware devices, application software etc.
- To minimize the security loopholes of the Internet.
- To atleast spread awareness among the users about the potential security risks that continue to exist, or which were not fixed by the developer.
- To enhance learning, research, and creativity by publically documenting how security flaws can be exploited in practice.

2.2. Case Study

In this information age, the use of technology and the Internet is rapidly increasing. There are so many applications which people from diverse age groups use regularly including online banking, online purchases, education, entertainment, gaming, social media etc. Even businesses have now become dependent on these applications. But this is also a ground reality that the greater the use of the Internet, the greater are the security concerns.

For example, if you want to order some food, you will probably unlock our phone first, which is running using the services provided by the operating system. Then you will also get connected to the Internet, which is a service you get from the ISP. Then you will log in to the food ordering application through a third-party authentication service such as OAuth. Once you are logged in, you will search for items through the application and make an order. If you are making an online payment, then it is also obvious that you will use another service for that. Hence, in order to make use of one application, several other services came into play, with there own respective loopholes and vulnerabilities, which increases the number of opportunities for attackers to enter into the system and exploit lots of the confidential and valuable information. However, the first victims of these attacks are the users themselves, so in the exchange of the trust which they are putting on an application, they expect security, privacy, and safety. Therefore, any application which fails to fulfill its promise of preserving the security is considered useless. Based on the same ideology, Google initiated a project in 2014, known as the project zero, which aims to improve the overall security of the Internet by minimizing the loopholes of the applications that reside on the Internet.

2.3. Working

The researchers of Project Zero study the security of the systems such as applications, operating systems, hardware, etc. that make the use of Internet, by looking at the source code, or performing security testing. If they come with any zero-day vulnerability, then it is reported to the developer or vender of the application it resides in, and asked to fix within a provided notice period. If the reported list of issues are not fixed within the timeframe, then being a responsible individual in the society, Google posts the details of the security loophole in its official Project Zero blog to atleast spread its awareness among the users.

Github: https://github.com/googleprojectzero

3. ZERO DAY VULNERABILITIES

A zero-day vulnerability, commonly referred to as a 0-day, is one that has not yet been discovered by the program manufacturer or those in charge of its security. Hackers may take advantage of this weakness to harm networks, data, and programs. A vulnerability that has not yet been found or fixed is referred to as “zero-day”, and an attack or exploit that takes use of that vulnerability is known as a “zero-day exploit” or “zero-day attack”. Because they can be exploited before they are even found or fixed, these kinds of vulnerabilities are highly risky.

3.1. Zero-Day Attack

Let’s break down the zero-day vulnerability and see how it leads to an attack:

- Your developers create an application, but they do not know that the code contains a vulnerability.
- An attacker comes to know about the vulnerability before developers could find it or get time to patch it.
- This attacker writes malicious code and executes attack while the vulnerability is still open.
- After exploit, either customers recognize data leak/identity theft or the developer traces down exploitation.

A cyberattack known as a “Zero-Day Attack” makes use of undiscovered software flaws. Because the flaws they take advantage of have not yet been identified, these assaults are particularly challenging to identify using conventional cybersecurity techniques. Attackers who focus on identifying these weaknesses invest a lot of time and money in honing their talents. To stay ahead of future assaults, it is crucial to employ more sophisticated techniques for identifying and fixing Zero-Day vulnerabilities. Protecting against these threats requires the use of advanced detection and patching procedures.

3.2. Risks Associated with Zero-Day Vulnerabilities

Zero-day vulnerabilities pose a higher risk to users for the following reasons:

- Cybercriminals race to exploit these vulnerabilities to cash in on their schemes
- Vulnerable systems are exposed until a patch is issued by the vendor.
- They are difficult to identify and defend against because neither the vendor nor the general public are aware of them.
- Attackers may take advantage of them before they are found and fixed, increasing the likelihood that a successful attack will take place.
- They can frequently be used to exploit "safe" systems and get beyond conventional security precautions.
- They may result in negative outcomes like identity theft and data breaches.
- They pose a serious threat to both persons and organisations because they can be used to conduct sophisticated and targeted attacks.
- Even after they are launched, they may go undetected, making it challenging to identify their source and stop the attack.
- They may be employed to introduce malware, build backdoors, and obtain illegal access to private data.

3.3. Zero-Day Protection

Zero-day protection refers to the steps taken to protect against zero-day exploits, which are software flaws that the vendor has not yet identified or fixed. Because the public is unaware of these attacks, they can be extremely challenging to identify and defend against. They may go undetected even after they have been launched and can be effective against systems that are regarded as “safe”. It is crucial to apply advanced security measures as well as safe computing practices and common sense to keep watchful against potential attacks in order to protect against zero-day exploits.

4. FACTS AND STATISTICS

Google Zero recently released valuable statistics on security vulnerabilities they have found in the past several years that are important to know.

According to the report, there is a positive change in the number of days to get security issues fixed by vendors. In 2021, it took an average of 52 days to fix security vulnerabilities reported from Project Zero which is a significant acceleration from an average of about 80 days 3 years ago.

On the other hand, there are unsolved issues that are concerning. Based on the report between 2019 and 2021, Google Zero reported 376 issues to vendors under their standard 90-day deadline. 351 (93.4%) of these bugs have been fixed, while 14 (3.7%) have been marked as WontFix by the vendors. The majority of vulnerabilities are clustered around a few vendors:

a. 96 bugs (26%) were reported to Microsoft,

b. 85 (23%) to Apple,

c. 60 (16%) to Google.

5. CONTRIBUTIONS IN REAL WORLD SCENARIOS

Google Project Zero has already been playing an important role in enhancing the security of the Internet. Below are outlined some of the important contributions made by the Google Project Zero to the society in the past few years:

1. On 30 September 2014, Google detected a security flaw within Windows 8.1's system call "NtApphelpCacheControl", which allows a normal user to gain administrative access. Microsoft was notified of the problem immediately but did not fix the problem within 90 days, which meant information about the bug was made publicly available on 29 December 2014. Releasing the bug to the public elicited a response from Microsoft that they are working on the problem.

2. On 9 March 2015, Google Project Zero's blog posted a guest post that disclosed how a previously known hardware flaw in commonly deployed DRAM called Row Hammer could be exploited to escalate privileges for local users. This post spawned a large quantity of follow-up research both in the academic and hardware community.

3. On 19 February 2017, Google discovered a flaw within Cloudflare's reverse proxies, which caused their edge servers to run past the end of a buffer and return memory that contained private information such as HTTP cookies, authentication tokens, HTTP POST bodies, and other sensitive data. Some of this data was cached by search engines. A member of the Project Zero team referred to this flaw as Cloudbleed.

4. On 27 March 2017, Tavis Ormandy of Project Zero discovered a vulnerability in the popular password manager LastPass. On 31 March 2017, LastPass announced they had fixed the problem.

5. Project Zero was involved in discovering the Meltdown and Spectre vulnerabilities affecting many modern CPUs, which were discovered in mid-2017 and disclosed in early January 2018. The issue was discovered by Jann Horn independently from the other researchers who reported the security flaw and was scheduled to be published on 9 January 2018 before moving the date up because of growing speculation.

6. CONCLUSION

In conclusion, Google Project Zero has been highly successful in identifying vulnerabilities in software and systems. Their team of experts uses a combination of manual and automated techniques to find and report security issues, which have led to many patches and fixes being released by major technology companies. This has greatly improved the overall security of the internet. Additionally, Project Zero serves as a valuable learning resource for the security community, providing detailed information and analysis of discovered vulnerabilities, as well as sharing techniques and tools used by their team. Overall, Google Project Zero has made a significant impact in the field of computer security and continues to be a vital player in the ongoing effort to make the internet a safer place.