Zero Click Attack

Ahmed Mohamed Nader Fayrouz Shaker
New Cairo academy, fifth settlement, Egypt, ahmedfayrouz533@gmail.com
Supervisor: Ahmed Magdy Mohamed
1- Electrical engineering department, Faculty of engineering, Suez Canal university, Egypt
2- Communication engineering department, New Cairo academy, Higher Institute of Engineering and Technology, New Cairo City, Egypt, Ahmed.m.1986@ieee.org

Abstract– Zero-click-attack is a new method that allows you to take control of devices and bypass security providers to get to the data servers for an organization or a group of people in the same area. This study aims to investigate and analyze how to do this attack, as well as the ways to protect the people and organizations from it. The research is based on a group of approaches that have previously been used to attack devices such as: evil twin attack, in addition to social engineering attacks and other ways to achieve the same thing, and also malware programs.

On the other side, the research examines how data providers can protect their users from such attacks, as well as the options available to ordinary users to avoid such attacks. There are two primary ways to carry out this attack; firstly, sending harmful payloads to a target's mobile phone over a cellular network by calling them or sending an empty SMS or MMS.

The Second method is to use social engineering to lure the target to an exploitations sites that will link the target's phone to many servers and send harmful messages or a malware application.

The results suggest that the attack may be performed to anyone who is unaware of how to secure his data, as well as data providers who are unfamiliar with how to improve their security defenses against such attacks which can be carried out in a variety of ways.

Keywords-- Zero-click-attack, Payloads, Malware programs, Evil twin attack, social engineering.

I. Introduction

We often hear about cyberattacks, cyber operations, and malware infections that target computer systems or smartphones. Attacks against civilian infrastructure facilities such as hospitals, water sanitation systems, and the energy sector similarly get a lot of it; these attacks lead to give someone the access to the sensitive data or control the machines.

In my research I will discuss a new way to do such these attacks by a method called "zero click attack", in addition I will discuss how we can avoid such this attack which can pass from mobile phone (Android or iOS) or machine running by (Linux, Unix or windows) to control all the devices connected to the network.

Zero click attack is a modern cyber-attack which can be done without clicking direct to run an .exe file or Linux tool or install a mobile application or any other action from the user, this attack aims to recording the user (victims) machine sessions and send it to the attacker, or it can give the attacker remote accesses to the user (victims) machines in addition this attack can give the attacker the ability to start doing a more harmful attacks to other victims by the first victim machine.

The scary part of a zero-click attack is that you may get infected even if you don't do anything. If a malicious actor targets you, you have nothing to combat against zero-click attacks. Depending on the exploit, an attacker may have full control over your machine or have listening capabilities of emails, iMessage's, WhatsApp messages, and voice messages. Your machine will be exploited without you knowing it, and this invisibility makes this threat highly dangerous and you may not even notice it if an attacker silently listens to your conversations.

II. When zero click attack can be done

A. When transmitting specially formed data to a victim's device via a wireless data transmission channel (GSM, LTE, Wi-Fi, Bluetooth, NFC, etc.).

B. The vulnerability could work when processing this data directly on the chip (baseband, Wi-Fi SoC, Bluetooth SoC, NFC SoC, etc.).

C. Or the data can go a little further, and the vulnerability will work when preprocessing the data on the target program (calls, SMS, MMS, instant messengers, email clients, etc.), which is responsible for preparing this data for the user. Next, the payload in the exploit performs certain actions for post-Exploitation.

III. How it can be done

This attack can be done by several ways according to the victim situation and the machine which will be hacked.

Case A. by using evil twin attack

An evil twin attack is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. The evil twin is the wireless LAN equivalent of the phishing scam [1]. Figure (A).

This type of attack uses the same BSSID and SSID in addition to block the victim connection to the access point and this will make the victim don't notice anything different.

The evil twin can be configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection and start do evil things comes under a Man in The Middle attack (MITM) in addition the attacker can send a custom payload to control the victim's machine.

This attack can be done by using:

1-airmon-ng for finding necessary info about the network.
2-airbase-ng to create its twin.
3-aireplay-ng to deauthenticate the client, and strong signal strength to make it connect to our network.
4-provide internet access to our client after he has connected to the fake wireless network.
5-monitor traffic from the victim, maybe hack into his computer using Metasploit.

Other way the fake AP can say the system is temporarily unavailable until obtaining the username and password for the ISP and the WI-FI password then compare it with the WPA2 handshake and if they are correct, it returns the victim to the original AP and the attacker connect to it and control the all devices in the network by sending harmful payloads.

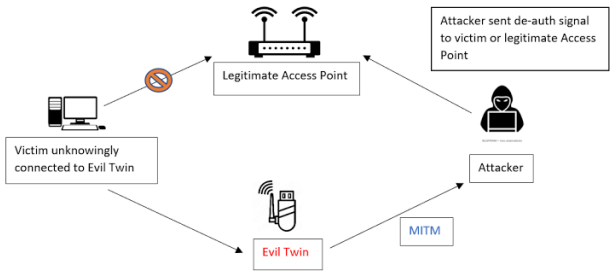


Figure (A): principle for evil twin attack

This attack can be done by using tools like: Linest, Fluxion, Airgeddon, EvilTwinFramework and etc.

Both ways can be done by using WIFI-pineapple device from Hak5.

CASE B. HACKING BY USING NETCAT OR ANY ALTERNATIVE TOOL

zero click attack can be done by using a tool works in many operating systems called a netcat.

Netcat is a great network utility for reading and writing to network connections using the TCP and UPD protocol.

Netcat is often referred to as the Swiss army knife in networking tools and most common use for Netcat when it comes to hacking is setting up reverse and bind shells, piping and redirecting network traffic, port listening, debugging programs and scripts and banner grabbing .

So, if the attacker wants to do a zero click attack it will send a generated file such (.pdf, .jpg, .doc and etc.) and it's contained malware trojan which will infect the machine by a payload to connect the victim machine to the netcat and then to attacker machine.

Other way to do such this attack for the mobile phones is to use the application bugs to run the malware when the victim get message contains it such: the malicious Pegasus code, and the recent CVE-2019-11932 in WhatsApp [2].

CVE-2019-11932 WhatsApp 2.19.216 Remote Code Execution:

1.set the listener Ip (nc -lvp 5555). Figure (B)
2. run ./exploit and save the content to .gif. Figure (D)
3. exploit.gif file and send it as Document with WhatsApp to another WhatsApp

Figure (B), (C): WhatsApp 2.19.216 Remote Code

CASE C. SIMJACKER

Researchers at Adaptive Mobile Security, a cyber telecommunications security organization, have revealed a new SIM card attack method that might operate on over 1 billion phones, and they claim it has already been used to track users by a surveillance firm [3].

The attack, dubbed Simjacker, entails sending a specially prepared SMS message to the victim phone. The SIM card (the universal integrated circuit card, or UICC) processes the message, which contains SIM Toolkit (STK) instructions, through the S@T Browser on the SIM [4].

An attacker could use this method to send a variety of STK commands to the targeted device, including to play a tone, send SMS messages, make phone calls, collect device information (location, IMEI, battery, language), launch a web browser, power off the card, request geographical location, and exfiltrate data.

These commands can be used to track a victim's location, send arbitrary messages on their behalf (even to premium-rate numbers for fraud), spy on users, transmit malware by ordering the device's web browser to visit a malicious website, and cause a denial-of-service (DoS) condition to all the machines which works in the same network.

The Simjacker can be done also by using calls. Figure (D), (C).

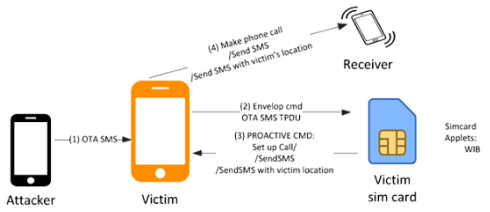


Figure (D), (E): Simjacker principle.

Case D. Attack the SIM Cards by the Basebands

The BTS (base station) was regarded as a trusted component of 2G (second generation) networks, out of reach of attackers. As a result, the phone will believe anyone acting as a BTS. This makes it possible to build a fake BTS and launch attacks over the air.

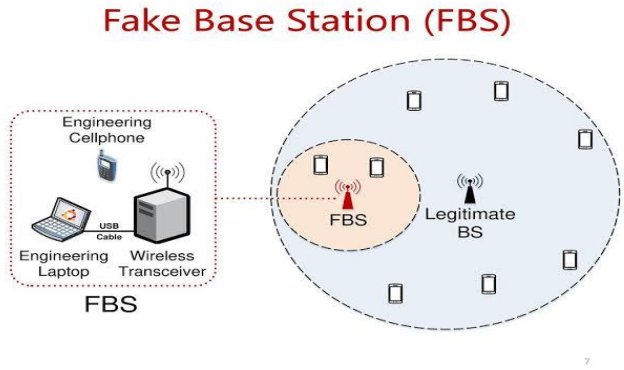
Only the base station authenticates the mobile phone, not the other way around. With the advent of SDR, it is evident that the BTS can no longer be trusted. It is now fairly inexpensive to set up a fake base station and attack mobile phones. Figure (E).

As a result, the strategy in 3G and newer networks has evolved. Generally, the mobile phone will authenticate the 3G or newer base station using keys from the SIM card. This reduces the number of attack surfaces on 3G and newer networks that require authentication bypass."

Because most new baseband supports 3G and 4G, and networks use new standards (which are given higher priority), the attacker needs additional techniques that allow downgrade the default connection method (up to 2G) in the client modem. Real life examples:

"A walk with Shannon Walkthrough of a pwn2own baseband exploit", Amat Cama (2018) [5].

"Exploitation of a Modern Smartphone Baseband", Marco Grassi, Muqing Liu, Tianyi Xie (2018) [6].



Case E. Methods for Zero Click Attack by Use Bluetooth

Bluebugging: Bluebugging is a type of a Bluetooth attack through which hackers can access a device and eavesdrop on phone calls, connect to the Internet, send and receive text messages and emails, and even make calls (while the owner is unaware of it). It is usually associated with older phone models.

Bluesnarfing: Hackers can perform a bluesnarfing attack on devices when they are within 90 meters. This is one of the most dangerous Bluetooth attacks because, even if your device is in a non-discoverable mode, hackers can attack it and gain access to all the personal information in your device. They can copy all the content on your device, including your pictures and videos, phone number, contact list, emails, and passwords. Figure (F).

However, the invisible mode makes it more difficult for hackers to figure out the model and name of your device. Examples in the real life:

"BLEEDINGBIT, (2018)" [7]

"CVE-2018-9555 and CVE-2019-2009 in the Android Bluetooth stack", (2018, 2019) [8]

Figure (F): Bluetooth attacks

IV. Threats of Zero-click Attack

Zero click attack is a scary attack because you need to be aware about something different running in your machine to know if you are infected or not. If any machine is infected by zero click payload it will put all around machines in dangers.

As we said before the attacker can attacks against civilian infrastructure facilities such as hospitals, water sanitation systems, and the energy sector and these attacks can start a cyber war between the countries.

Other scary side for the zero click attack is to infect modern military weapons which are networked such guided missiles, missile, and anti-missile systems, tanks, fighter jets, and more.

We can imagine that weapons systems contain security vulnerabilities similar to most other information systems, including serious ones. A malicious adversary taking over the control of deadly weapons capable of kinetic destruction may sound like a political fiction plot begging to be overhyped. But today, computerized weapons systems control the defense pillars of many countries. And though information on these systems is highly secretive, there is one thing we do know: While accessing such systems is not easy, they almost certainly contain vulnerabilities.

V. The methods to defend against zero click attack

As the result from my research, I get several methods to defend against the zero click attacks depends on the used machine and its operating system.

Firstly, the machines running by Microsoft windows the user can setup a anti malware to search for any harmful payloads. the user also should be aware for any data he downloads or get it from any one and how he can make his AP's BSSID hidden to avoid any attack can be done by it.

Secondly for machines works by using Linux or Unix operating system they can avoid this attack by ignored an untrusted tool which can be contains a harmful payload, in addition to what we said for the windows.

Thirdly for the wireless routers or access point the best way to avoid any attacks is to keep its BSSID hidden or use filtering methods and check the connected devices to the network every day.

Also, for the Bluetooth the user should stay in touch with the machine 's company which will notify him if there are any security problems.

Finally for sim card the user must use the modern methods such 5G ,4G and 3G which there are use new connection methods need authentication between the chip and the base station.

Conclusion

Zero click attack is a modern way that can give the criminal the ability to take control the infected machine without any notice, in addition to control all machines that are around the infected machine or working in the same area.

We can do this attack by several ways and my research discussed each way and its principle.

This attack is very harmful to any machine and we should protect our machine from it, also our army should use it as a weapon against any other army wants to start a cyber war.

References

[1] Evil Twin Tutorial, By Shashwat July 14, 2014.
https://www.kalitutorials.net/2014/07/evil-twin-tutorial.html?showComment=1406591245609#c5539483407421385761
[2] National Vulnerability Database CVE-2019-11932 Detail.
https://nvd.nist.gov/vuln/detail/CVE-2019-11932
[3] Adaptivemobile Security Simjacker Technical Paper.
https://simjacker.com/
[4] Simjacker: SIM Card Attack Used to Spy on Mobile Phone Users by Eduard Kovacs on September 12, 2019
https://www.securityweek.com/simjacker-sim-card-attack-used-spy-mobile-phone-users
[5] "A walk with Shannon Walkthrough of a pwn2own baseband exploit", Amat Cama (2018).
[6] Exploitation of A Modern Smartphone Baseband Marco Grassi, Muqing Liu, Tianyi Xie.
https://i.blackhat.com/us-18/Thu-August-9/us-18-Grassi-Exploitation-of-a-Modern-Smartphone-Baseband-wp.pdf
[7] BLEEDINGBIT: THE HIDDEN ATTACK ,SURFACE WITHIN BLE CHIPS
Ben Seri, Gregory Vishnepolsky and Dor Zusman
https://www.armis.com/research/bleedingbit/
[8] NATIONAL VULNERABILITY DATABASE CVE-2019-9506 Detail
https://nvd.nist.gov/vuln/detail/CVE-2019-9506