Unexplored Warfare of 21st Century

Esha Chadha, Kartik Verma, Monika Arora

Abstract: The world has gone through huge technological-advancement in recent years. With the increased usage of technology, there is a rise in cybercrime too. Advanced methods are being used to commit cybercrime in recent times. One of the recent methods being used is malware. Malware, also known as malicious software, is a software that can damage the system it is installed in it. Malware is a software that is used to compromise a computer, steal data and cause harm to a computer. Few types of malware are viruses, worms, ransomware, spyware, adware etc. Another tool that's been used by black hat hackers is called Spyware. Spyware is a software that infects a device and steals all the personal information available on that device. Spyware, if once installed in a device like mobile phone allows the hacker to completely clone the attacker's device as spyware then access each and every information that's stored in the phone. Spyware is also capable of accessing the camera and microphone of the targets phone. One such spyware is Pegasus. Pegasus made by an Israeli group, can hack into any person's system by just clicking on a link or worse by just receiving a call from a random number. Pegasus can jailbreak into devices and access their messages, camera, microphone, applications and much more.

Keywords: Malware, Spyware, Pegasus, Chrysaor.

1. Introduction

In the 21st century, it is almost impossible to even imagine life without technology. Everything from mobile phones to cars everything has embedded systems and computers installed in it which allows the devices to function smartly and fast. These computers are often misunderstood as "smart" whereas the truth is these computers are very dumb as they just follow a set of instructions. These instructions often have few bugs in them which are consequently exploited. These exploitation leads to instability and huge losses to people. In a world where everything is on the internet, Cybercrime is very common.

In order to prevent these cyber-attacks an individual need to understand Cyber Security and hence they also need to understand Cyber Kill Chain that allows us to break down a cyber-attack in 7 steps. If an individual is aware about these steps then he/she can prevent their devices from getting compromised.

In this paper, individuals will be informed about one of the most sophisticated cyber-attacks of all time, Pegasus. Individual will also become aware about several topics like Malware, its types and many more.

2. About Malware

Malware is an abbreviation of the term malicious software. Malware is a software or code that is designed and aimed to seize and harm devices. Malware cannot harm the hardware of a device. It can encrypt, modify and delete the device data. It can also spy on the device activity without permission.[1]

2.1. Types of Malware

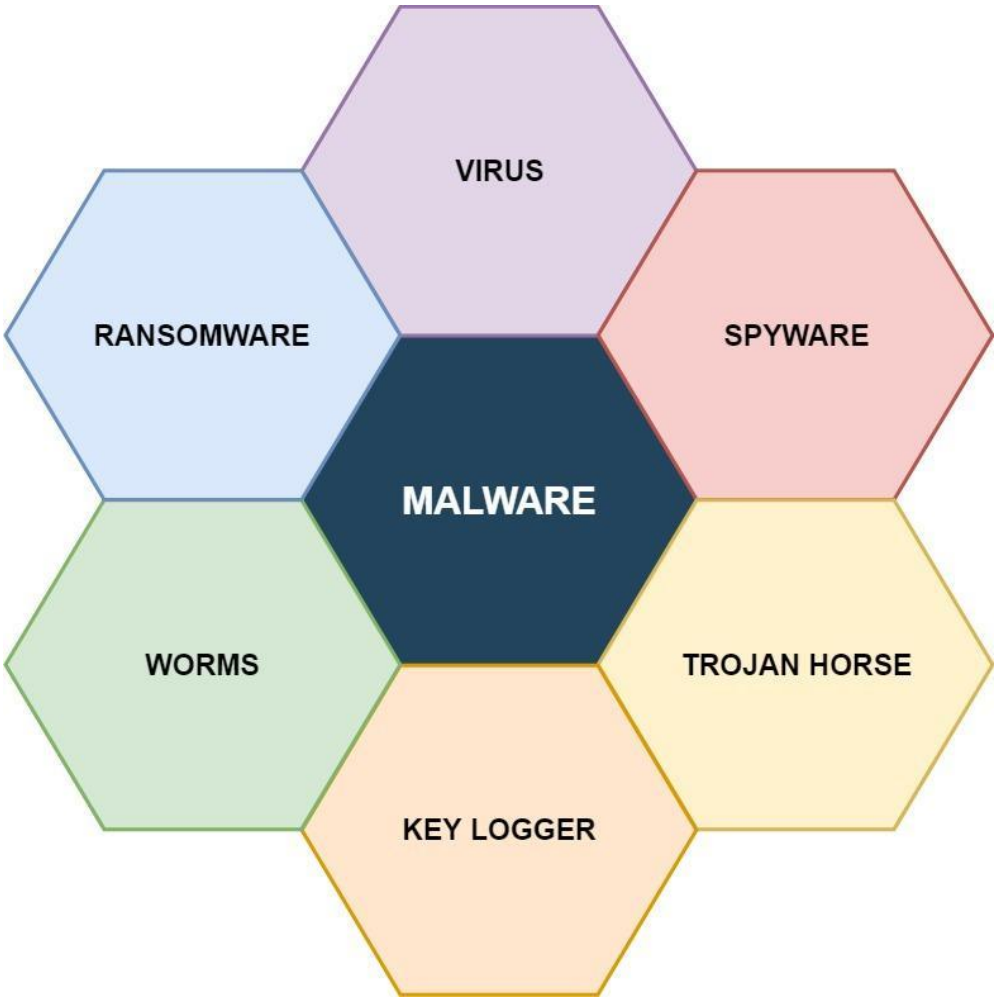

Figure 1. Types of Malware

Table 1. Types of Malware **[2][3]**

Sno	Malware Name	Description	Transmitted Through	Effects	Types
1.	Virus	Viruses are attached to a code/program. Users need to execute the program for the virus to work.	Self-replicates and spreads to other computers.	Slows host computer performance, Data loss, Computer Crashes.	Multipartite Virus Macro Virus Polymorphic Code Boot Sector Virus
2.	Worms	Unlike viruses, worms can spread independently. It is programmed to spread to uninfected devices	Spread through computer networks	Uses up bandwidth of infected networks and overloads them	Email Worms IM Worms File-Sharing Network Worms IRC Worms
3.	Trojan Horse	Trojans give remote access of the affected device to a party	Binds to a document and seems like a useful program so that the user downloads it	Gives access to others of the infected device, damage files, Obtain personal details	Backdoor Exploit Rootkit
4.	Spyware	Spywares are programmed to track activities of a user and obtain sensitive information	Spyware is installed when user tries to download a software attached with a spyware	Ad pop ups Device gets slower Changes in victim's browser	Adware System Monitors
5.	Ransomware	Encrypts user data. A ransom is asked by the attackers before the data can be decrypted	Embedded in downloadable files	Loss of important data, device is down till ransom is not paid	Locker Ransomware Crypto Ransomware
6.	Keylogger	Keylogger is used to record every key pressed by the user.	Attached in malicious programs or emails, Embedded in vulnerable webpage scripts	Obtains personal information like credentials and economic information	Software Keyloggers Hardware Keyloggers

3. Pegasus And Chrysaor

Spyware, as mentioned above, is a malicious software application or a type malware that is responsible for collecting information about an individual (sometimes an organization) without their consent. This information is then shared with other individuals or parties in order to earn some profit. Pegasus and Chrysaor are a few recent examples of a spyware that can hack any iOS and Android device respectively and steal all of its data.

3.1. History of Pegasus And Chrysaor

Pegasus was first discovered by Ahmed Mansoor, a human rights activist in the UAE on 10 August 2016. Mansoor received a link as SMS text message on his iPhone which was "supposed" to redirect him to a page that would provide him with the information about individual torture in UAE jails. Mansoor instead of clicking on the link sent it to Citizen Lab, an organization based at the University of Toronto.
Citizen Lab collaborating with Lookout produced evidence-based research. The researchers detected that the link had a malicious code embedded into it which would have compromised Mansoor's data on his iPhone.

After a few days, Lookout identified the malware as a spyware named Pegasus which was a surveillance software produced by the Israel-based NSO Group, which sells it to government for investigating crime and terrorism.

Also, in 2018, an Amnesty International staff member received a suspicious WhatsApp message that included a link that, if clicked, would have installed Pegasus on the employee’s mobile device.

Recently, in May of 2019, Pegasus was being installed on around 1400 mobile devices across the globe. 20 of these mobile phones belonged to famous politicians, lawyers and human rights activists of India like Anand Teltumbde and Nihalsing Rathod. Pegasus, in this case was installed by using WhatsApp an application that has around 1.5 billion active users around the globe making it the most popular mobile messaging app.

3.2. Working of Pegasus And Chrysaor

According to NSO, Pegasus spyware is being installed onto devices by carriers(vectors) classified in two types namely one-click vector and zero click vector. The two vectors are explained below :-

a. One-click vector:

Just like in the case of a phishing attack, the attacker disguised as a trustworthy source sends a website URL via text message, email or on social media like WhatsApp. In general, this link would open a malicious website called Anonymizer which is responsible for communicating with operator's servers.

The server then scans the victim's device and checks whether Pegasus could run its malicious code for that particular model. If for any reason Pegasus isn't able to run the code then the link redirects to an actual website in order to avoid raising suspicions.

In case of iOS devices like iPhone, when the victim clicks on the link then the malware secretly carries out a zero-day exploit. It's very difficult for the user to identify whether his/her device has been compromised as they cannot tell whether something has occurred or not, in some cases just after clicking the link the browser closes.

- *Zero-Day exploits:*

It refers to the bugs present on a software that no one even the creator is aware of. These bugs are very hard to track and hence if an attacker exploits these bugs then it could be dreadful. This kind of exploit is called zero-day exploits.

These exploits subsequently result in jailbreaking it remotely so that Pegasus could be installed which allows Pegasus to access control servers and hence execute the operator's commands. After Pegasus is installed it doesn't install the malicious versions of all the applications present in the mobile, instead it compromises all the apps that were already present in the mobile and capture all of its data. Pegasus contains a malicious code which spies on everything that the user does on his/her device.

In IOS if Pegasus fails to implement the zero-day exploits and hence fails to jailbreak the system then the attack would fail. In case of Android devices, Chrysaor doesn't require any zero-day vulnerabilities to jailbreak and hence install the malware, this is the main difference between Chrysaor on Android and Pegasus on IOS. Here it uses another technique called Framaroot.

- *Framaroot:*

It is a rooting technique that allows the user to easily root its device with a click and also unroot it easily. In case of Android devices if the process of rooting doesn't work then, Chrysaor would still ask for permission to access and withdraw data. If at any given instance Chrysaor finds itself in danger of getting exploited then it has the ability to delete and remove itself, hence leaving no trace behind. It has been successful to hide itself for three years. Majority of Android mobiles are out of danger as Chrysaor wasn't distributed at such a large scale.

b. Zero click vector:

This process was carried out to install spyware on a user's device via WhatsApp.This is worse than one-click vector as in this case the user doesn't even have to click or open the link sent by

an attacker. One click function often uses push messages which automatically loads links without the user even clicking on it.

In the case of WhatsApp, the attacker exploited a bug in its call function. This allowed the attacker to send data packets containing spyware code via a phone call to the target by simply using his/her phone number. In this case, the Pegasus was being installed on the victim's device by simply receiving an incoming call. Pegasus was being installed in the device even if the call was unattended. This incoming call carried data packets along with the spyware code which immediately opened a small backdoor for its installation while the phone rang. There are many kinds of spyware code for instance, spyware code called Ganges is responsible for installing Pegasus on a device using networks like Hathways, Bharti Airtel, MTNL and spyware code called Pricklypear is used to install Pegasus in devices in US.

The exploit impacted WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen (which is used by Samsung devices) prior to v2.18.15.[4]

3.3. Fixing of Pegasus And Chrysaor

After the failed attempt of hacking Ahmed Mansoor's mobile, Apple only after 10 days came with an update to its IOS version 9.3.5 in which the zero-day bug was been fixed and hence jailbreaking was being prevented. Also, the previous bugs such as:

1. CVE-2016-4655: Information leak in Kernel – A kernel base mapping vulnerability that leaks information to the attacker allowing them to calculate the kernel's location in memory. [5]

2. CVE-2016-4656: Kernel Memory corruption leads to Jailbreak – 32- and 64-bit iOS kernel-level vulnerabilities that allow the attacker to secretly jailbreak the device and install surveillance software - details in reference.[6]

3. CVE-2016-4657: Memory corruption in the Webkit – A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.[7]

Chrysaor was a spyware that was mainly targeted at users using android version 4.3 Jelly Bean or earlier.

3.4. Effects of Pegasus And Chrysaor

Pegasus and Chrysaor are spyware which are responsible for "spying" on victim's activity. This spyware also is responsible for stealing data from the victim. All this data can easily allow the attacker to easily clone the victim's device.

These spyware easily allow the attacker to access everything on victims device like :-

1. Microphone recording
2. Email
3. SMS
4. Location tracking
5. Network details
6. Device settings
7. Browsing history
8. Contact details
9. Social networks
10. Phone calls
11. Calendar records
12. Files retrieval
13. Instant messaging
14. Photos and screenshots

3.5. Prevention from Pegasus And Chrysaor

In order to prevent Chrysaor from installing on your device, you should :-

- Always verify the links that have been sent to you are secure to open.
- Unknown links should not be clicked.
- Do not use your primary devices to open an unknown link. Use a device which you only use to view files instead.
- Use non-default browsers like Mozilla Firefox for the phone as Pegasus is supposed to target default browsers like Google Chrome for Android and Safari for iPhone.

In order to prevent Pegasus from installing on your device, you should :-

- Do not give your phone to others.
- While crossing borders make sure that your phone is switched off so that your device isn't compromised.
- Never open links sent by unknown sources.
- Turn off push SMS on your device.
- Avoid jailbreaking your iPhone in order to prevent unwanted and unsigned software applications to be downloaded on your device.
- Always install the latest security patches on your device.
- WiFi and Bluetooth should be switched off when not in use.[8]
- Keep important data encrypted on your device.[9]
- Back up your data on a regular basis.
- Read terms and conditions of an application carefully before accepting them.

4. Implementation of Lockheed Martin Kill Chain

According to Lockheed Martin Kill Chain, any cyber-attack could be broken down into 7 main stages/phases. If an individual is able to remove any of the seven stages of this Kill chain then he/she keeps his/her device out of danger.

In this case, both Pegasus and Chrysaor can be broken down in these seven stages/phases. These were the steps taken by the attacker, in this case NSO Group in Israel to attack various countries making this cyber-attack one of the most sophisticated attacks of all time(Fig 2).

Fig. 2. Lockheed Martin Kill Chain

a. Pegasus Attack on WhatsApp

The attack on WhatsApp occurred because of a bug in the voice and video call function of WhatsApp. This bug was exploited. Pegasus could be installed in the victim's phone by just calling them on WhatsApp. The attack on WhatsApp can be broken down into seven stages and are explained below (Table 2).

Table 2. Pegasus Attack on WhatsApp by Kill chain

Sno.	Stage	Implementation
1.	Reconnaissance	This step involves methods of Social Engineering. In this an attacker looks for weakness in a software. NSO (Attacker) researched a lot on WhatsApp (Victim). This research led to the discovery of a number of exploits in various versions of WhatsApp. A bug was found in the call function of WhatsApp, this included both voice and video call. This bug was then exploited.
2.	Weaponization	This step involves the formation and creation of a Malicious application which leads to the formation of a malware, in this case the type of malware was a spyware. This spyware was called Pegasus.
3.	Delivery	This step involves the delivery of the malicious application that is Pegasus to the victim. In this case, Pegasus was distributed and delivered to the victim (WhatsApp users) by calling them. WhatsApp voice call works on the following ports: TCP: 4244, 5222, 5223, 5228, 5242 TCP/UDP: 59234, 50318 UDP: 3478, 45395
4.	Exploitation	This step involves the exploitation of a bug in order to execute a code on the victim's device. In the case of Pegasus, various data packets containing spyware codes were being sent to the targeted WhatsApp users by calling them on their numbers which were registered on WhatsApp. This spyware code was capable of jailbreaking the victim's device and hence downloading unsigned application as well by gaining root access.
5.	Installation	This step involves installation of a malware that is spyware on the victim's device. In this case, the Pegasus was being installed in the victim's device by simply receiving an incoming call. Pegasus was being installed in the device even if the call was unattended. The spyware code called Ganges, that has been sent to WhatsApp users opened a backdoor for its installation via internet provided by Hathways, Bharti Airtel, MTNL and more.
6.	Command and control	This step involves creating a channel between the attacker and victim which allows the attacker to connect to the victim's device over the internet. This is a very important stage as this stage further allows the attacker to give commands and hence control the victim's device from his/her own device.
7.	Action on objectives	This step involves gaining access over the victim's device. After Pegasus has been installed the victim has no idea about its existence. Hence, the attacker is easily able to access each and every piece of data available on the victim's device. This allows the attacker to gain access to photos, videos of the victim's device.

b. Pegasus Attack on iOS

A bug was found in a particular version of iOS. Pegasus was designed to jailbreak the device and install itself on it. The attack on iOS, can be broken down into seven stages and are explained below (Table 3).

Table 3. Pegasus attack on iOS by Kill Chain

Sno.	Stage	Implementation
1.	Reconnaissance	This step involves methods of Social Engineering. In this an attacker looks for weakness in a software. NSO (Attacker) researched a lot on iPhone (Victim). This research led to the discovery of a number of exploits in version before 9.3.5 of iPhone. A bug was found in a particular version of the iPhone. This bug was then exploited.
2.	Weaponization	This step involves the formation and creation of a Malicious application which leads to the formation of a malware, in this case the type of malware was a spyware. This spyware was called Pegasus.
3.	Delivery	This step involves the delivery of the malicious application that is Pegasus to the victim. In this case, Pegasus was distributed and delivered to the victim by sending them a malicious URL in a text message.
4.	Exploitation	This step involves the exploitation of a bug in order to execute a code on the victims device. In case of Pegasus, after the victim clicks on the malicious link, a malicious code is downloaded which would allow the victims device to jailbreak itself and hence download unsigned application Pegasus by gaining root access.
5.	Installation	This step involves installation of a malware that is spyware on the victim's device. In this case, the Pegasus was being installed in the victim's device by jailbreaking itself. In general, this link would open a malicious website called Anonymizer which is responsible for communicating with operator's servers. The server then scans the victim's device and checks whether Pegasus could run its malicious code for that particular model. If for any reason Pegasus isn't able to run the code then the link redirects to an actual website in order to avoid raising suspicions.
6.	Command and control	This step involves creating a channel between the attacker and victim which allows the attacker to connect to the victim's device over the internet. This is a very important stage as this stage further allows the attacker to give commands and hence control the victim's device from his/her own device.

7.	Action on objectives	This step involves gaining access over the victim's device. After Pegasus has been installed the victim has no idea about its existence. Hence, the attacker is easily able to access each and every piece of data available on the victim's device. This allows the attacker to gain access to photos, videos of the victim's device.

References

[1] https://www.avg.com/en/signal/what-is-malware

[2] https://www.lastline.com/blog/malware-types-and-classifications/

[3] https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

[4] https://en.wikipedia.org/wiki/Pegasus_(spyware)

[5] https://en.wikipedia.org/wiki/Pegasus_(spyware)

[6] https://en.wikipedia.org/wiki/Pegasus_(spyware)

[7] www.deccanherald.com/specials/pegasus-spyware-all-you-need-to-know-772667.html

[8]https://www.deccanherald.com/specials/pegasus-spyware-all-you-need-to-know-772667.html

[9] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html