EasyChair Preprint

№ 5257

NADRA Database Hack In Context Of Cyber Kill Chain and Overview of Pakistan's Cyber Security

Muhammad Abrar Khan

March 31, 2021

NADRA Database Hack In Context Of Cyber Kill Chain and Overview of Pakistan's Cyber Security

Muhammad Abrar Khan

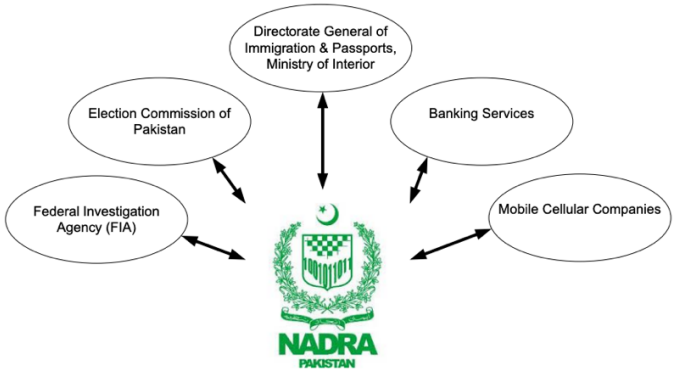
Masters Information Security
Military College of Signals, NUST, Pakistan
mkhan.msis-19mcs@student.nust.edu.pk

Abstract— **NADRA (National Database and Registration Authority) is a centralized national ID database of Pakistan. Recently National Database and Registration Authority (NADRA) Database got hacked and the personal data of millions of Pakistani nationals was compromised. This attack has become the biggest scandal in the history of cyber-attacks in Pakistan. This paper aims to explain this attack in the context of Cyber Kill Chain (CKC) which is a framework that explains the categorization of steps included in a cyber-attack. Fortunately, in this attack, all of the fingerprints and information stolen were retrieved. However, this gave a point to ponder that we really need to enhance our security measures and have good defense mechanisms. This paper also discusses our current cyber awareness level as a country.**

Keywords— **Cyber Kill Chain, Cyber-Attack, Cyber Awareness, NADRA, Pakistan Cyber Security**

I. INTRODUCTION

NADRA (National Database and Registration Authority) is a centralized national ID database of Pakistan, which is shared among banks, passport offices, Election Commission Departments, Mobile networks and FBI (Federal Bureau of Investigation) etc. NADRA is the only organization which registers and stores the information about the population. Due to this, NADRA is the goal target for cyber terrorism to block or sabotage its essential services, hack human confidential information and use them for their illegal purposes.



II. CYBER ATTACK ON NADRA DATABASE

Recently National Database and Registration Authority (NADRA) Database got hacked and the personal data of millions of Pakistani nationals was made insecure. The data included personal information such as Name, CNIC, Addresses and fingerprints. The cyber- attack was launched by criminal hackers from Pakistan who stole finger prints and then used them to make artificial rubber finger prints so that they can mask these fake fingerprints as legitimate ones. The scope of such attack is enormous as it imposes direct threat on all government institutions and banks and agencies etc. The hackers used these fingerprints illegally for phone hacking, fraud related to bank, facilitating terrorism, selling SIM cards and various other criminal activities. This attack has become the biggest scandal in the history of cyber-attacks in Pakistan. On the response, the police conducted a raid at a house in Karachi from they recovered thousands of fingerprints and they were all stored on a single laptop which the hackers were using.

III. CYBER KILL CHAIN

Cyber Kill Chain (CKC) is a framework which explains the categorization of steps included in a cyber-attack. Each step has a different contribution in the attempt of that cyber-attack. In this framework, a total of 7 steps are included. Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Actions on Objectives.

The attack methodology of this attack is not revealed for general public information. However, the investigators are of the view that the hackers followed the following attack route.

A. ***Reconnaissance***

This is the first step of Cyber Kill Chain. This step involves information gathering about the target. In this

phase hackers look for every bit of information, do vulnerability assessment, look for profiles. In this attack, the criminal hackers first looked for all the personal social media profiles associated with NADRA, like their staff, management and developed their profile. After that they studied the website of NADRA and carried out vulnerability assessment on it. There are tools available online which can tell you all the details related to a website, like on which Operating system it is being hosted. The hackers also did deep inspection of the website and found out its subdomains and vulnerabilities such as SQL Injection.

*B. **Weaponization***

This is the second step of Cyber Kill Chain. In this step the attacker generates or chooses the attack vector which he has decided to bring into play from all the information gathered in the first step. In this step the attacker can make his own custom malware to infect the website or choose to go with any of the traditional attacks available such as SQL Injection, Buffer Overflows or Cross-site Scripting XSS. In NADRA's attack the weapon was malware such as SQL Injection and Malicious scripting.

*C. **Delivery***

This is the third step of Cyber Kill Chain. In this step the attacker makes his first move to officially launch the attack. There can be numerous ways to deliver the weapon in the infected system. It can be through a USB flash or directly by attacking with a malicious script on the network. It can be also achieved through social engineering using techniques such as phishing, voice over phishing etc. In NADRA's attack the delivery was through malicious scripting on the site exploiting vulnerabilities such as SQL injection and custom script execution.

*D. **Exploitation***

This is the fourth step of Cyber Kill Chain. In this step the attacker exploits the target as he wished when he delivered his weapon successfully. In this step the attacker through his weapon gains unauthorized access to the machine and now he is able to do whatever he wants. Once access is gained, the attacker will do all sorts of malicious activity like stealing confidential information or deface the website. In NADRA's attack the criminal hackers gained unauthorized access through scripting and they were able to collect personal data of millions of Pakistani nationals.

*E. **Installation***

This is the Fifth Step of Cyber Kill Chain. In this step the attackers install their malware inside the victim's machine or server and launch their malicious script which can be sending confidential data to the attacker's server. In NADRA's attack the installation part was to send all the personal information like name, cnic, addresses and fingerprints of users to the local machine of the hackers located in Karachi.

*F. **Command and Control***

This is the sixth Step of Cyber Kill Chain. In this step the attacker fully gains authority over the victim as he gains not only the access but also gets all the privileges. In this case the attacker can either deface the website and disrupt the service but that would let the organization know that their website is hacked. The other way is that the attacker installs a backdoor in the target website in order to gain unauthorized access any time in the future. In this way the owner or the organization never know that the website is compromised. In NADRA'S attack the hackers installed a backdoor and they did not let the authorities know that their website is compromised. It was very late known when investigators noted suspicious activity on the dark web markets.

*G. **Actions on Objectives***

This is the last step of Cyber kill Chain. In this step the attacker does all the necessary work required after the attack. This can include hiding footprints and erasing logs. Also maintaining how much data is transferred to the attacker's machine and how much is left. All the necessary tasks carried out after the main exploitation and wrapping up the attack comes under the actions on objectives step. In NADRA's cyber-attack the criminals just created copies of the data stored on the server being under the hood and once completed then disconnect their connection with the website server.

IV. CONSEQUENCES OF THE ATTACK

This was one of the major cyber-attacks launched in Pakistan. It has a massive affect because many government institutions are associated with NADRA and if NADRA's data is compromised, then it can have disastrous effects on the overall national security of Pakistan. Fortunately, in this attack, all of the fingerprints were stolen were retrieved and thankfully no records were leaked. However, this gave a point to ponder that we really need enhance our security measures and have good

defense mechanisms. Cyber safety is one of the major concerns for every organization in this age of digitization. The volume of cyber-attacks is growing at a rapid rate.

V. PAKISTAN'S CYBER SECURITY

Pakistan is ranked one of the least cyber secure countries with the following measures.

- 25 percent of the mobile phones are infected with malware in the form of games downloaded by children and third-party applications for entertainment.
- One of the worst prepared countries in case of a cyber-attack as the nation itself has not even a single Cyber Security Incident Response Team (CSIRT).
- 70% of the population is untrained on how to ensure security of their data on their digital devices

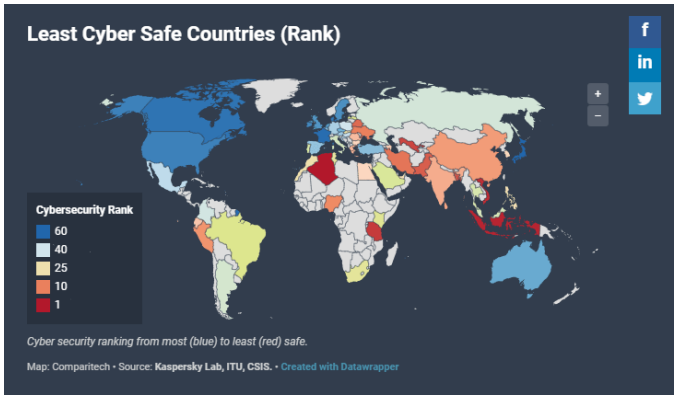


Fig. 1 Least Cyber Safe Countries [2]

Each data breach does not only cause economical loss but also time loss, resource usability loss and most importantly the loss of data. Data is important to every user, whether you are a student or being a corporate. Right now, 18,000+ Cases are pending in FIA for cyber-harassment, hacking, leak of personal pictures and cyberextortion. Unfortunately, current cyber policies are unable to recover the damage caused.

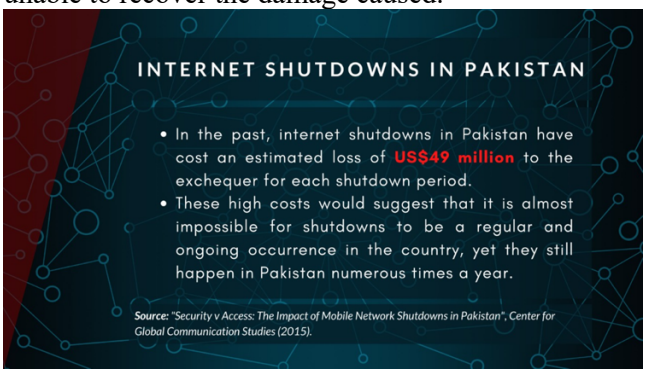


Fig. 2 Economical effects of a cyber-attack in Pakistan [3]

VI. CONCLUSION

Apart from having a few specialized researchers in this field, we are lagging behind from the world in the field of cyber security and digital forensics. In the present, we are going through summit of technological advancement in the field of computer science. It doesn't matter from which sector you belong; we all use smartphones and plenty of gadgets for our daily use. It's high time for individuals of Pakistan to identify the importance of the data they possess and its safeguarding measures.

VII. REFERENCES

[1] https://insiderpaper.com/nadra-database-hacked-pakistan/
[2] Kaspersky Lab, ITU, CSIS
[3] Awan, Jawad & Memon, Shahzad. (2016). Threats of Cyber Security and Challenges for Pakistan.
[4] "Security v Access: The impact of Mobile network Shutdowns in Pakistan" Center for Global Communication Studies (2015)