CommandEleven on NADRAGate

Briefing Paper
June 2017

commandeleven
SECURING YOUR SIX

For more information about receiving this, or other CommandEleven analysis documents, please visit http://www.commandeleven.com/.

ABOUT COMMANDELEVEN

CommandEleven is a research organization focused on Pakistan's national security aspects and enhancing global understanding and collaboration opportunities for the nation.

Founded in 2015, CommandEleven provides situational awareness to facilitate a better understanding of the key dynamics that effect Pakistan from a national security perspective, especially in relation to terrorism, insurgencies and extremism.

CommandEleven seeks to inform and guide public policy and decision makers in government, business and military through a rigorous program of publications, conferences, digital medias, policy briefings and recommendations.

Visit http://commandeleven.com for more information or contact info@commandeleven.com.

NADRAGate is one of the most important national security issues to face Pakistan ever. For the first time, the entire database of the citizenry could potentially be in the hands of foreign governments for screening, profiling and other identity related activities.

The essence of this conversation is the WikiLeaks cable – https://wikileaks.org/plusd/cables/09ISLAMABAD1642_a.html – which establishes an irrefutable chain of evidence to an act disastrous to public and national interests.

Before we get into the details of the evidence, we need to establish certain precedents:

1. The entire conversation is centered on the sale, access, intelligence given to the United States' Department of Homeland Security, National Security Agency, by in 2009 between the then Interior Minister of Pakistan, Rehman Malik, the President of Pakistan, Asif Zardari, and the Prime Minister of Pakistan Yousaf Raza Gilani.
2. The facts of the memo are not in dispute because they are CONFIDENTIAL US FEDERAL DOCUMENTS that we were never meant to see. They are available because of Edward Snowden.

It is our duty, much like other think tanks and media organizations, to highlight and educate the Pakistani public to potential dangers to our national security and their personal security. The analysis that we have provided takes the precedents into account and leverages the best resources at our disposal to understand the technical data and provide an understanding for the Pakistani population of what has happened, the implications and the recommendations forward.

We strongly stand behind the integrity of NADRA, as an organization, as this crime was committed against them and the people of Pakistan, but the politicians elected to safeguard them from the same.

COMMANDELEVEN'S BACKGROUND

In the analysis posted on our website – https://www.commandeleven.com/regions/pak-ind-afg/you-should-be-worried-about-nadragate-heres-why/ – from Rafay Baloch, CommandEleven Analyst and internationally respected Cyber Security Specialist, we establish the following:

1. In June 2015, The Intercept published a report disclosing that GCHQ had hacked PTCL's Core Routers, allowing them to intercept every single user's traffic, but also re-route the traffic to their systems.
2. 2016 – another report details how the NSA had gained access to Pakistan's National Telecommunications Corporation (NTC) using Malware called SECOND DATE.
    a. Confirmed with a group called Shadow Brokers leaked a list of compromised hosts from the NSA operation, including a step by step guide on how NSA compromised Mobilink's network including the CDR (Call Data Records) servers in 2006.
3. We further establish that a Quantum-Insert attack was carried out on a target in Miranshah, as per another leaked document. Snowden's own statements confirm that the NSA uses this method regularly.
4. We establish that, as per the highlighted memo in 2009, Gilani and Malik went to the US Embassy and offered access to NADRA's database.
5. This was done through a cover company called – International Identity Service Limited – based in the UK
6. Incorporated on 9th July, 2009, dissolved 18th November, 2014

7. We suggested that the consultant company access would not have been limited to just pulling data, but most likely have planted backdoors to obtain updated copies of the database.
8. We also suggest that the NSA/GCHQ penetration into NADRA would not be Read-Only, but would have gained Insert, Update, Delete records as well.

PISCES

In today's Daily Pakistan – https://en.dailypakistan.com.pk/opinion/nadragate-the-terrifying-cable-that-should-not-be-ignored/ – Waqas Ahmed explains in great detail the access that was given to passenger information during the Musharraf government.

Under the cable, DHS wanted to provide GoP a tool that would connect an API to the NADRA database for the purpose of analysis, providing an alert system if a suspected terrorist was travelling in or out of Pakistan. They gave us the technology free with the condition that they would be able to access our data. They would be able to access the data about EVERYONE travelling through Pakistan's airports.

PISCES was created by Booz Allen Hamilton, NSA contractors and the former employers of Edward Snowden.

IMPLICATIONS

NADRA is currently the most critical database holding public record, it contains everything from your CNIC, family tree, driving license, passport, biometric data to DNA record and voters record. NADRA's database values are utilized to perform identity verification while registering a SIM or opening a bank account, NADRA utilizes web-service which only exposes subset of a data that is required for verifying an identity.

In this case, however, it is clear from the leaks that the entire database was subject to theft.

This can lead to serious implications and consequences:

- Biometrics is technically described as Type-3 Authentication (Something that you are) which is based upon physical characteristic of a person. Currently, fingerprints are the most commonly used form of biometric authentication. In cases, where fingerprints are stolen, it effectively means that any form of authentication, where your fingerprints are utilized, can be compromised as they already in their possession.
- The worst part is that, in case your passwords get compromised, it's very easy for you to change the passwords and control the damage. If your fingerprints are compromised, there is nothing much you can do about it.
- Your stolen fingerprints can easily be used in order to issue a SIM on your behalf, without your knowledge, which then can be used to impersonate you and commit crimes.
- Stolen data from NADRA can be utilized to conduct social engineering attacks against an individual.
- Those who come from our western border, Chaman, also require a biometric verification. Assuming that NSA has WRITE access to NADRA's database, they can add a new record to the database. This can allow someone to effectively cross Chaman border by impersonating an identity and the biometric verification will happily accept it.

RECOMMENDATIONS

In the light of above events, we give the following recommendations to the government:

- Principally, no access to NADRA's database should not be given to anyone, and, even if a certain portion of database is exposed via web service, it should be limited and should follow the "principle of least".
- Under present circumstances, we strongly discourage electronic voting until the government, election commission and intelligence services have taken adequate security measures.
- The government should take the privacy of their citizens seriously.
    - The regulatory branch should impose penalties on any form of private data leaked, as a result of breach. In event of any breach and incident, the senior management should be held accountable if proper due care and due diligence is not carried by them.
- Under present circumstances, it is strongly recommended to setup a state-owned **Cyber Security Unit**.
    - The Cyber Security Unit's primary responsibility would be protecting the confidentiality, integrity and availability of critical internet infrastructure. The Cyber Security Unit would also be responsible for providing security advisory to all the critical sectors empowering country's economy and hosting user's critical data.
- We recommend a third-party independent security sweep of the entire NADRA database and network to determine if there are any backdoors and/or continued leaks.
- We recommend a fully empowered JIT to investigate and prosecute those involved to the fullest extent of the law.

About CommandEleven

CommandEleven is a research organization focused on Pakistan's national security aspects and enhancing global understanding and collaboration opportunities for the nation.

Founded in 2015, CommandEleven provides situational awareness to facilitate a better understanding of the key dynamics that effect Pakistan from a national security perspective, especially in relation to terrorism, insurgencies and extremism.

CommandEleven seeks to inform and guide public policy and decision makers in government, business and military through a rigorous program of publications, conferences, digital medias, policy briefings and recommendations.

Visit http://commandeleven.com for more information or contact info@commandeleven.com.