



You Should Be Worried About NADRAGate

Briefing Paper
June 2017

© 2017, CommandEleven. All rights reserved.

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

REPORT AUTHORS

"You should worry about NADRAGate, here's why" was researched, compiled and written by **Rafay Baloch**, Senior Analyst.

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.

BACKGROUND

There have been multiple reports leaked from various credible sources about NSA & GCHQ hacking into Pakistan's critical infrastructure. One of the first reports that was made public was in [June 2015 published by Intercept which highlighted GCHQ's infiltrating PTCL's Core Routers and hence allowing them not only intercept every single user's traffic but it also had abilities to re-route the traffic to their passive collection systems.](#)

This report was followed up by another roughly one year back, which pointed out that [NSA had gained access to Pakistan's National Telecommunications Corporation \(NTC\) using Malware known as "SECOND DATE"](#)

Part of this was confirmed in October 2016, when a group known as "**Shadow Brokers**" leaked list of hosts that were compromised as a part of NSA's operation, The leaks also reveal a step by step guide on how [NSA compromised Mobilink's network including the CDR Servers \(Call Data Records\) in 2006. \[3\]](#)

From the evidence obtained, it is very clear that NSA & GCHQ both have had significant amount of interest in hijacking Pakistan's critical infrastructure.

OUR ANALYSIS

As per various leaks, Edward Snowden reveals a couple of NSA's deadliest weapons, most notable being Quantum-Insert attacks in order to carry out targeted attacks. The hijacking of Pakistan's ISP provides a great aid in Quantum-Insert attacks. [As per one of the leaked documents](#) confirms this attack was being utilized in order to infect a target located in Miran Shah. We have posted a detailed technical analysis of Quantum-Insert attacks [here](#).

(TS//SI//NF) DGO Enables Endpoint Implants via QUANTUMTHEORY
By [[REDACTED]] on 2011-09-26 1548

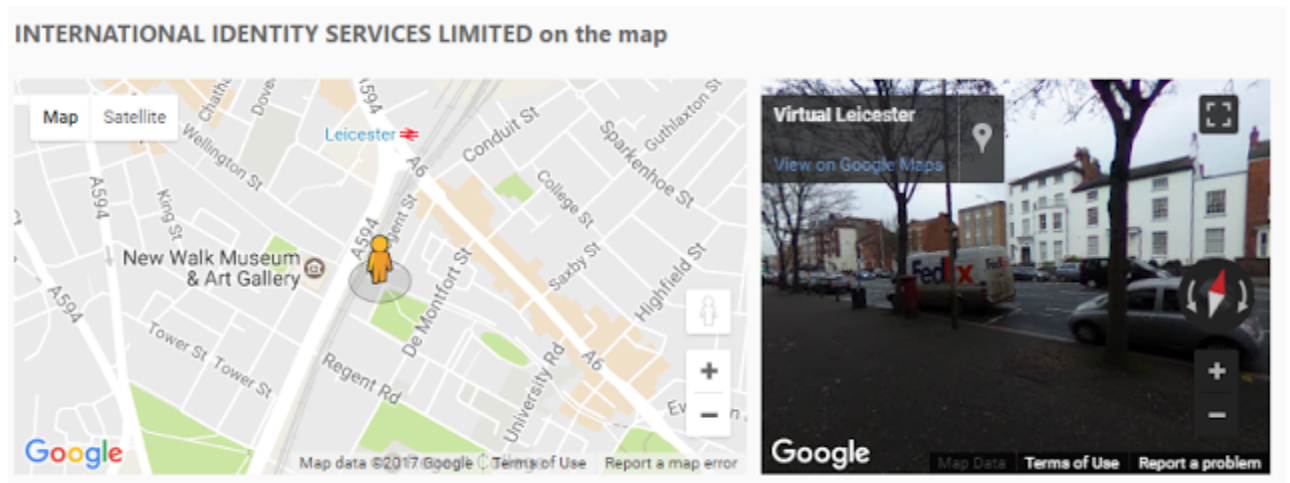
(TS//SI//NF) In another example of the emerging collaboration between the Endpoint and Midpoint missions, the QUANTUM team had another marked success during the week of 12 September 2011. TAO's R&T analysts identified an opportunity to use QUANTUMINSERT to exploit a Pri-1 CT target, Badruddin Haqqani, the senior leader in the Haqqani network located in the Miran Shah in Pakistan's tribal area. Badruddin's importance has recently come under closer scrutiny by U.S. Government policymakers due to his involvement in the attack on coalition forces in Afghanistan with a large truck-borne IED.

(TS//SI//NF) QUANTUMINSERT is meant to briefly hijack connections between a specific target and a web connection in order to redirect the target to a TAO server (FOXACID) for implantation. To implement this, SIGDEV analysts worked with SSO's DANCINGOASIS (DGO) collection management to put four specific signal case notations on cover. Using the tips from the collection from DANCINGOASIS, 47 shots from QUANTUMINSERT were taken resulting in 22 FOXCONTACTs, including nine from this specific target. This meant nine opportunities to implant the target. One of these was successful, resulting in the VALIDATOR implant being installed on the target computer. This allows TAO to formulate and execute plans for further exploitation of the target's computer.

INTRODUCTION & ANALYSIS




In [a recently leaked cable by WikiLeaks](#), it was highlighted that in 2009, then Prime Minister Yousaf Raza Gilani and Interior Minister Rehman Malik went to US Embassy and offered access to NADRA's database. It was later highlighted that this was accomplished by setting up a cover company known as "**International Identity Service Limited**" based in UK since it's easier to conduct attacks being an insider.

As per the data we gathered from a deep search, it is revealed that the company was incorporated on **9 July 2009** and had a registered office address, which comes in harmony with the dates when Prime Minister and Interior Minister visited the US Embassy. The registered office address of the company as the records "**Owg, 2nd Floor, 94 New Walk, Leicester, LE1 7EA**". The company was dissolved on **November 18 2014**.



There is couple of [information that can be found about company's staff](#):

A CommandEleven Briefing Paper

Company staff		
 James Martin McNally Date of birth: March 1950 Age: 67 years old Nationality: British Role: Director	Appointed: 01 July 2012 Occupation: Director	Address: Floor, 94 New Walk, Leicester, LE1 7EA, England Residence: United Kingdom
<small>Latest update: 3 June 2017</small>		
 Simon Robert Brodie Date of birth: September 1954 Age: 63 years old Nationality: British Role: Director	Appointed: 09 July 2009 Occupation: Management Consultant	Address: Devonshire House, Low Road, Barrowby, Lincolnshire, NG32 1DB Residence: England
<small>Latest update: 3 June 2017</small>		
 Jonathan Hall Date of birth: March 1964 Age: 53 years old Nationality: British Role: Director	Appointed: 09 July 2009 Occupation: Company Director	Address: 55 Trent Valley Road, Lichfield, WS13 6EZ Residence: England
<small>Latest update: 3 June 2017</small>		

We actually dug deeper into Simon Robert Brodie, one of the directors of the company and found the following work history:

Work History			
Company name	Role	From	To
Healthcare Learning Ltd	director	1 February 2002	1 December 2012
Handbag.com Limited	director	16 August 1999	18 March 2005
Sports Results Solutions Limited	director	3 December 2014	current
Siuk Consultancy Ltd	director	11 October 2011	current
International Identity Services Limited	director	9 July 2009	current
The Belvoir Hunt Limited	director	27 January 2004	current
Futures Perfect Limited	director	7 February 2003	current
Hlc Group Limited	director	22 May 2001	current

It can be safely assumed that the role of consultant company would not only be limited to ex-filtrating data from NADRA's database, but they would also have planted backdoors into the systems, so that they would have the updated copy of the database.

It also be safely assumed that NSA/GCHQ's penetration into NADRA's database would not be READ-ONLY, however they would have done their best to gain highest privileges into order to INSERT, UPDATE and DELETE records.

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.

For instance, in order to register a SIM, the devices used by telecom operators take the fingerprint, convert it into NADRA's acceptable format and send the request to NADRA's web service, if the fingerprint is accepted, the SIM is issued.

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.

PRIVACY & WHY THIS MATTERS?

A very common argument that I keep hearing is "**I am not a criminal, I have nothing to hide, why should I have afraid of?**" Even if you have nothing to hide and you are not a criminal, your online identity can be hacked and you can turn into a criminal. Assume, if your Facebook account gets hacked and your status is flooded with messages sponsoring and supporting terrorism, it will be extremely difficult for you to repudiate and it requires a complete forensic investigation in order to prove that you are not guilty. The case of Mashal Khan is evident, where his identity was impersonated and a narrative was build that he has committed blasphemy.

Privacy is not only our democratic right; however, it is considered as a fundamental Human right in 1948 United Nations Universal Declaration of human rights.

RECOMMENDATIONS

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

- Principally, no access to NADRA's 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.
- 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.

REFERENCES

- 1) <https://firstlook.org/theintercept/2015/06/22/gchq-reverse-engineering-warrants/>
- 2) <https://www.documentcloud.org/documents/3031638-Select-Slides-FINAL-PMR-4-24-13-Redacted.html>
- 3) <https://github.com/x0rz/EQGRP/blob/33810162273edda807363237ef7e7c5ece3e4100/Linux/doc/old/etc/user.mission.sicklestar.COMMON>
- 4) <https://www.documentcloud.org/documents/3031642-SSO-News-Excerpt-Redacted.html>
- 5) https://wikileaks.org/plusd/cables/09ISLAMABAD1642_a.html
- 6) <https://www.companieslist.co.uk/06956966-international-identity-services-limited>

ABOUT THE AUTHOR

Rafay Baloch is a prominent cybersecurity researcher from Pakistan. His work has been noted by Forbes, BBC, Wall Street Journal and Black Hat Asia.

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.