

The background is a dark, deep blue space filled with a complex network of glowing, ethereal blue lines that swirl and connect various points. Scattered throughout this network are numerous white and light blue numbers, including 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9, some of which appear to be floating or drifting. The overall effect is one of high-tech digital connectivity and data flow.

COMELEAK

FROM HACKING TO LEAKING TO BEHIND
BARS?

SEMPRIX

XY

GODFLUX

DISCLAIMER

THIS PRESENTATION IS INTENDED FOR EDUCATIONAL PURPOSES ONLY AND DO NOT REPLACE INDEPENDENT PROFESSIONAL JUDGMENT. STATEMENTS OF FACT AND OPINIONS EXPRESSED ARE THOSE OF THE PARTICIPANTS INDIVIDUALLY AND, UNLESS EXPRESSLY STATED TO THE CONTRARY, ARE NOT THE OPINION OR POSITION OF ROOTCON, ITS COSPONSORS, OR ITS COMMITTEES. ROOTCON DOES NOT ENDORSE OR APPROVE, AND ASSUMES NO RESPONSIBILITY FOR, THE CONTENT, ACCURACY OR COMPLETENESS OF THE INFORMATION PRESENTED. ATTENDEES SHOULD NOTE THAT SESSIONS ARE AUDIO-RECORDED AND MAY BE PUBLISHED IN VARIOUS MEDIA, INCLUDING PRINT, AUDIO AND VIDEO FORMATS WITHOUT FURTHER NOTICE.

THE OPINIONS EXPRESSED HEREIN ARE OUR OWN PERSONAL OPINIONS AND DO NOT REPRESENT OUR EMPLOYER'S VIEW IN ANY WAY.

BACKGROUND OF THIS TALK

WEEKS BEFORE THE PHILIPPINE ELECTION A GROUP OF HACKERS MADE THEIR WAY INSIDE THE COMELEC'S WEBSITE AND LEAKED MASSIVE VOTERS DATA TO THE PUBLIC, IT WAS THEN TAGGED AS THE **WORST PUBLIC DATA BREACH IN THE PHILIPPINES.**

HISTORY || ORIGIN

DATA BREACHES HAVE GAINED WIDESPREAD ATTENTION AS BUSINESSES OF ALL SIZES BECOME INCREASINGLY RELIANT ON DIGITAL DATA, CLOUD COMPUTING, AND WORKFORCE MOBILITY. WITH SENSITIVE BUSINESS DATA STORED ON LOCAL MACHINES, ON ENTERPRISE DATABASES, AND ON CLOUD SERVERS, BREACHING A COMPANY'S DATA HAS BECOME AS SIMPLE – OR AS COMPLEX – AS GAINING ACCESS TO RESTRICTED NETWORKS.

SOURCE: [HTTPS://DIGITALGUARDIAN.COM/BLOG/HISTORY-DATA-BREACHES](https://digitalguardian.com/blog/history-data-breaches)



ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

[See Your Matches »](#)

Over **37,765,000** anonymous members!



0 YEARS 5 MONTHS 26 DAYS
OR 5 MONTHS 26 DAYS
OR 25 WEEKS 4 DAYS

OR **179** DAYS AGO



MARCH 27, 2016
DEFACEMENT DAY



Anonymous Philippines

Greetings Philippines! We are Anonymous.

The Constitution so asserts that "Sovereignty resides in the people and all government authority emanates from them."
One of the processes by which people exercise their sovereignty is through voting in an election- where people choose the candidates who will best represent them, who will serve them under the principle that "Public office is a public trust."

But what happens when the electoral process is so mired with questions and controversies?

Can the government still guarantee that the sovereignty of the people is upheld?

We request the implementation of the security features on the PCOS machines.

Commission on Elections, We are watching!

We are Anonymous,
We are legion,
We do not forgive,
We do not forget.

EXPECT US!

Are you a concerned citizen? Mail us at info@anonph.net

~n3farlous | ./kh4lifax | sec.anonops

Anonymous Philippines - Phantom Hackers.PH - Philippine Cyber Army - PrivateX

#pR.1s0n3r | busabos | POWERFUL | ~ManilaBoy | s4v4nt.r00t | ~Invictus | mumervs rider | Blood Sec Hackers



BEFORE DEFACEMENT

VIDEO

WHOOOPS..

**“WE REQUEST THE IMPLEMENTATION OF THE
SECURITY FEATURES OF THE PCOS MACHINES”**

- ANONYMOUS PHILIPPINES

HOURS LATER..

THE LEAK

**Lulzsec Pilipinas**
22 hrs · 🌐

A great lol to Commission on Elections, here's your whoooooole database.
Update: Added 3rd db mirrors.

Mirror 1: [REDACTED]
Mirror 2: [REDACTED]
Mirror 3: [REDACTED]

**LulzSec Pinas**
We are LulzSec Pinas, now you know. Db leaks and other shits. Leaks leaks leaks. Hello Comelec !
LULZSECPINAS.ML



WHAT'S IN IT?

THE DATA COPIED APPEARS TO CONTAIN INFORMATION ON THE **NAMES, DATES OF BIRTH, GENDER, CIVIL STATUS, ADDRESSES, PRECINCT NUMBERS, BIRTHPLACES** AND **DISABILITIES** (THESE DATA ITEMS ARE NOT MANDATORY FOR ENTRY DURING APPLICATION SO NOT NECESSARILY SAME NUMBER OF RECORDS HAVE THESE ENTRIES). IT ALSO INCLUDES **VOTER IDENTIFICATION NUMBERS, VOTER REGISTRATION RECORD NUMBERS, REGISTRATION DATES**, AND THE REASONS FOR DELETIONS AND DEACTIVATIONS OF VOTER RECORDS.

SOURCE: [HTTP://WWW.COMELEC.GOV.PH/?R=CYBERSECURITY](http://www.comelec.gov.ph/?R=CYBERSECURITY)

THE GOOD NEWS.. DATA IS ENCRYPTED

THE BAD NEWS,.. DECRYPTION KEYS WERE
LEAKED?

THE SILVER LINING... DUE IN PART TO THE MEDIA
ROLLERCOASTER – THE MASSES WERE MADE
AWARE OF THE IMPORTANCE OF SECURITY.



4h

hello .@govph,

why are you seeding the .@COMELEC data leak?

IP	Client	Flags	%
cpe-104-162-106-224.nyc.res.rr.com [uTP]	qBittorrent v3.3.4	D P	0.6
cpe-66-27-221-170.hawaii.res.rr.com	Shareaza 2.7.9.0	d	1.6
112.201.210.121.pldt.net [uTP]	µTorrent 3.4.5	d P	1.1
205.56.85.115.dsl.service.eastern-tele.com [uTP]	Torch 45.0.0.10802	d P	0.9
mail.malacanang.gov.ph	Deluge 1.3.12	d	2.4
97e08b2c.skybroadband.com [uTP]	Vuze 5.7.1.0	d P	1.0
237.112.156.175.unknown.m1.com.sg	µTorrent 3.4	d	7.0



114



104



Follow

@govph @COMELEC the govt,
while obtaining a copy for themselves,
contributes to the sharing, making it more
accessible

SOURCE: [HTTP://WWW.INTERAKSYON.COM/INFOTECH/ENTIRE-COMELEC-DATABASE-AVAILABLE-VIA-TORRENT-MALACANANG-SEEDING-IT](http://www.interaksyon.com/infotech/entire-comelec-database-available-via-torrent-malacanang-seeding-it)

APRIL 20, 2016



THE SUSPECT WAS ARRESTED ON WEDNESDAY EVENING, IN HIS HOUSE IN SAMPALOC, MANILA.

SOURCE: [HTTP://WWW.RAPPLER.COM/NATION/POLITICS/ELECTIONS/2016/130252-SUSPECTED-HACKER-COMELEC-WEBSITE-NABBED](http://www.rappler.com/nation/politics/elections/2016/130252-suspected-hacker-comelec-website-nabbed)



DEFACING THE COMELEC WEBSITE WAS MEANT **“TO GIVE VOICE TO THE VOICELESS,”** PAUL BITENG TOLD THE INQUIRER IN AN INTERVIEW. BUT THE **DATA LEAK** WAS **NOT** PART OF **THE PLAN**, HE ADDED.

SOURCE: [HTTP://TECHNOLOGY.INQUIRER.NET/47763/BOREDOM-MADE-ME-DO-IT-SAYS-COMELEC-HACKER](http://technology.inquirer.net/47763/boredom-made-me-do-it-says-comelec-hacker)

Anonymous PH Hacker Could Face Up To 60 Years In Jail

His bail has also been set at P600,000

By **Andrei Medina**
Apr 28, 2016

f Shares

Tweet

0 Comments

The individual who [allegedly hacked](#) the [Commission on Elections](#) (Comelec) website is facing a maximum sentence of **up to 60 years in jail**, if proven guilty of violating the Cybercrime Prevention Act.



If so, **Paul Biteng**, who is only 23 years old and has already been dubbed a "master hacker" by the National Bureau of Investigation, might be walking out of jail by the time he's in [his eighties](#).

MOST POPULAR



1
Bea Benedicto Is One Of The Main Reasons You Should Buy FHM's September 2016 Issue



2
Maria Ozawa Cries Foul Over 'Bastos' Immigration Staff



3
Louise Delos Reyes Is Currently Our Favorite Beach Babe

Total notifications: **144** of which **46** single ip and **98** mass defacements

Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

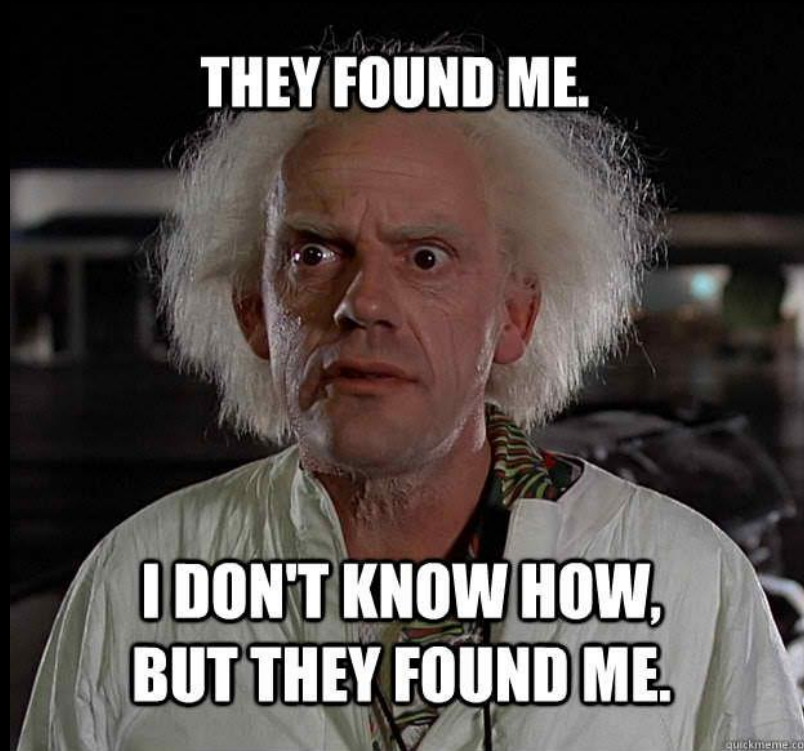
L - IP address location

★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2016/03/14	kh4lifax					★ dipologcity.gov.ph/about.php	Linux	mirror
2016/03/14	kh4lifax					★ kidlat.pagasa.dost.gov.ph/abou...	Linux	mirror
2015/08/10	kh4lifax			R		www.wi-tribe.ph/hacked.txt	Linux	mirror
2015/07/17	kh4lifax		M			★ caraga.csc.gov.ph/kh.txt	Unknown	mirror
2015/07/17	kh4lifax					★ web.csc.gov.ph/kh.txt	Unknown	mirror
2015/07/15	kh4lifax	H				cryptors.org	Linux	mirror
2015/05/28	kh4lifax					starcinemamovies.abs-cbn.com/k...	Linux	mirror
2015/04/07	kh4lifax					klhunters.my/main/news.php?new...	Linux	mirror
2015/03/12	kh4lifax		M	R		pinoyitsolution.com/x.txt	Linux	mirror
2015/03/09	kh4lifax		M	R		ungeorgia.ge/x.html	Linux	mirror
2015/02/27	kh4lifax		M	R		www.isuzuphil.com/x.htm	Linux	mirror
2015/02/27	kh4lifax	H	M			www.mallcomindia.com	Linux	mirror
2015/02/27	kh4lifax	H	M			koratcity.in	Linux	mirror
2015/02/27	kh4lifax	H	M			abzab.com	Linux	mirror
2015/02/27	kh4lifax	H				heartlandworld.com	Linux	mirror
2014/02/13	kh4lifax	H				singaporeartbridge.com	F5 Big-IP	mirror
2014/02/13	kh4lifax	H	M	R		www.pacitaabad.com	F5 Big-IP	mirror
2013/12/09	kh4lifax					www.penshoppe.com/kh4lifax.php	Linux	mirror
2013/08/16	Kh4lifax					www.headhuntermanila.com/hhmla...	Win 2008	mirror
2013/08/06	Kh4lifax		M			puptaguig.net/kh4lifax.php	F5 Big-IP	mirror
2013/07/26	Kh4lifax	H				www.belships-tj.com.cn	Win 2003	mirror
2013/07/24	kh4lifax	H				peacetravel.cn	Linux	mirror
2013/07/24	Kh4lifax	H	M			www.dow.org.tw	Win 2003	mirror
2013/07/24	kh4lifax	H				powerloops.ph	Linux	mirror
2013/07/17	Kh4lifax	H				machine.extension.fcu.edu.tw	Linux	mirror

1 2 3 4 5 6

SOURCE: [HTTP://WWW.ZONE-H.ORG/ARCHIVE/NOTIFIER=KH4LIFAX/PAGE=1](http://www.zone-h.org/archive/notifier=kh4lifax/page=1)



THEY FOUND ME.

**I DON'T KNOW HOW,
BUT THEY FOUND ME.**

quickmeme.com

THEN SOMETHING CAME UP

Philippines, we have your data :b

Fill two or more fields

First name

Last name

Maternal name

BENIGNO SIMEON III AQUINO COJUANGCO

Birth

Year of birth	Month of birth	Day of birth	Birth province	Birth city
1960	02	08	NATIONAL CAPITAL REGION - MANILA	

Body

Basic

Sex	Weight	Height	Marks
M			

Fingerprints

Finger info	Finger topo	Matching finger	Quality
PPN,N,N,PPN,N,N	02E1FE3FFF2D014F04BDF87FFB2014F___034801ABFF59014F03D0FF19FF13013E___	I	117,82___128,92___

Relatives

Civil status	Spouse name
--------------	-------------

COMELEC SPOKESPERSON JAMES JIMENEZ ISSUED A STATEMENT VIA TWITTER ON THURSDAY, ADVISING THE PUBLIC NOT TO USE THE SITE AS IT CAN BE USED BY THE HACKERS TO STEAL INFORMATION AND FURTHER EXPOSE THEM TO IDENTITY THEFT.

691,200 SECONDS

11,520 MINUTES

192 HOURS

8 DAYS

1 WEEK AND 1 DAY

2.19% OF 2016

APRIL 28, 2016



COMMISSION ON ELECTIONS (COMELEC) CHAIRMAN ANDRES BAUTISTA ON FRIDAY (APRIL 29) NAMED JONEL DE ASIS AS THE ALLEGED SECOND COMELEC WEBSITE HACKER.

SOURCE: [HTTP://CNNPHILIPPINES.COM/NEWS/2016/04/29/COMELEC-HACKER-DATA-LEAK.HTML](http://cnnphilippines.com/news/2016/04/29/COMELEC-HACKER-DATA-LEAK.html)

THEY REPORTEDLY HAD NO INTENTION OF SELLING THE INFORMATION TO ANY POLITICAL PARTY OR INTERESTED PERSONALITIES.

“WE ONLY WANTED TO PROVE THAT IT IS EASY TO HACK THE COMELEC WEBSITE,” SAID DE ASIS.

SOURCE: [HTTP://WWW.PHILSTAR.COM/HEADLINES/2016/04/30/1578281/2ND-COMELEC-HACKER-NABBED](http://www.philstar.com/headlines/2016/04/30/1578281/2nd-comelec-hacker-nabbed)

MENDEZ SAID THAT THE NBI-CCD CONTINUES TO WORK ON THE CASE.

“WE ARE WARNING THE PUBLIC **WHO** WERE ABLE TO **OBTAIN THE HACKED DATA NOT TO USE IT** BECAUSE CERTAINLY **WE WOULD BE ABLE TO IDENTIFY YOU SOONER OR LATER.**”

NBI-CCD CHIEF ROLAND AGUTO SAID THAT THEY ARE STILL LOOKING FOR THE **THIRD HACKER**, WHO IS BELIEVED TO BE STILL IN MANILA.

SOURCE: [HTTP://WWW.PHILSTAR.COM/HEADLINES/2016/04/30/1578281/2ND-COMELEC-HACKER-NABBED](http://www.philstar.com/headlines/2016/04/30/1578281/2nd-comelec-hacker-nabbed)

#FREEPaulBITENG



Free Paul Biteng

May 2 · 🌐

👍 Like Page

Cause? [#FreePaulBiteng](#) needs help! www.freepaulbiteng.info



👍❤️👹 3K

75 Comments 2.6K Shares



👍 Like

💬 Comment

➦ Share

#FREEPaulBITENG



Donate



“ Paul Biteng has been in custody since April 20, 2016, for alleged defacement and leakage of voter's information from the COMELEC website in which the latter was strongly denied by him.

Your smallest form of help and donation will matter a lot to Paul.

Paul, we will be with you in everything and awaiting of your return. Keep smiling, we hope this will all be over soon. You will be free to live your life with your beautiful family and we will be here to celebrate all of your accomplishments. Keep the faith our dearest friend.

VULNERABILITIES?

WHY NOBODY NOTICED?

HOW DID THEY GOT CAUGHT?

ALLEGED HACKERS ARE THE FIRST
AND LAST TO GET IN RIGHT?

PUBLIC DATA?

PRIVACY?

IMPLICATIONS?

OTHER NOTABLE ELECTION BREACH

**FBI SAYS FOREIGN HACKERS
PENETRATED STATE ELECTION
SYSTEMS; ARIZONA AND ILLINOIS –
YAHOO.COM**

Q&A - PANEL DISCUSSION

THANKS!!!