Abstract

Hackers assaulted the website of the Philippines' elections commission to protest both the integrity of the upcoming presidential elections in addition to security concerns regarding the electronic voting. The website was hacked and defaced on Sunday, March 27th by AnonymousPH, and a few hours later was assaulted by another group of hackers - LulzSec Pilipinas – which hacked and dumped the database of COMELEC voter's polls (see Figure 1).

The attackers questioned the security measures taken by COMELEC to secure votes and voters' data for the upcoming May 9th national elections. In addition to the defacement, they published the poll database. The commission responded by promising that the election website will be hosted somewhere else and have its own set of security features which are of a higher quality.

Beyond the general concern to election voting systems, this event demonstrates the power hackers have. It has the potential to lead to psychological bias of voters, reduce election participation rates, undermine governing party's support, and more.

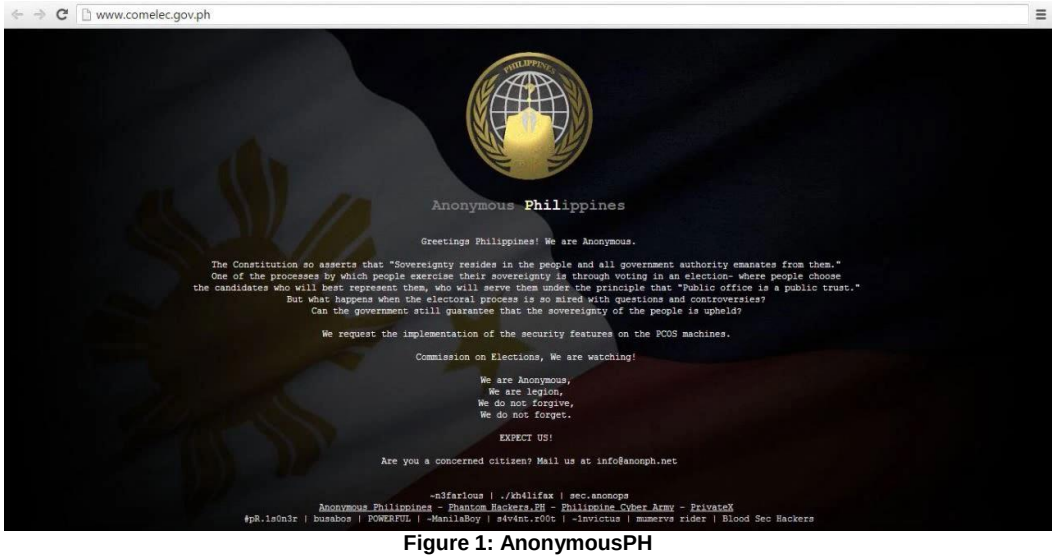


Figure 1: AnonymousPH

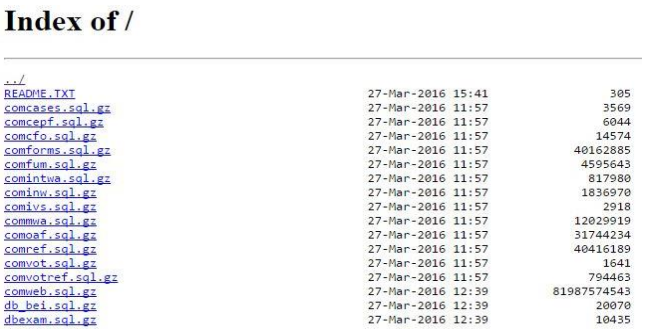
Background

1. The hackers questioned both the integrity of the upcoming elections as well as the security measures taken in order to protect voters' private information. They demanded legitimate election results and threatened to remain vigilant in watching how COMELEC will be running the elections.[i]

2. They specifically referred to securing the PCOS (Precinct Count Optical Scan) machines.

3. These attacks followed a court ruling requiring the polling body to activate the voter verification audit trail so that they can produce voter receipts on the May 9th election day.

4. Following the defacement by AnonymousPH, the hacktivist group LulzSec Pilipinas hacked and dumped COMELEC's database on their website, LulzSecPinas.ml. This leak included several databases including an 81Gb file (see Figure 2).



Index of /

../		
README.TXT	27-Mar-2016 15:41	305
comcases.sql.gz	27-Mar-2016 11:57	3569
comcepf.sql.gz	27-Mar-2016 11:57	6044
comcfo.sql.gz	27-Mar-2016 11:57	14574
comforms.sql.gz	27-Mar-2016 11:57	40162885
comfum.sql.gz	27-Mar-2016 11:57	4595643
comintwa.sql.gz	27-Mar-2016 11:57	817980
cominw.sql.gz	27-Mar-2016 11:57	1836970
comivs.sql.gz	27-Mar-2016 11:57	2918
commwa.sql.gz	27-Mar-2016 11:57	12029919
comoaf.sql.gz	27-Mar-2016 11:57	31744234
comref.sql.gz	27-Mar-2016 11:57	40416189
comvot.sql.gz	27-Mar-2016 11:57	1641
comvotref.sql.gz	27-Mar-2016 11:57	794463
comweb.sql.gz	27-Mar-2016 12:39	81987574543
db_bei.sql.gz	27-Mar-2016 12:39	20070
dbexam.sql.gz	27-Mar-2016 12:39	10435

Figure 2: Database leak on LulzSecPinas.ml

COMELEC spokesman James Jimenez stated the database leaked on social media sites was available for public use and no sensitive information was stolen. [ii] COMELEC indicated their IT department and web team is working to restore the database and searching for any malware the attackers may have left behind.

Figure 3: LulzSec Pinas Facebook page

Figure 4: AnonymousPH references attack

Reasons for Concern

These attacks appear to have one main purpose: to spread fear that the polling systems that will be in the upcoming presidential elections are just as insecure as the COMELEC website. It could potentially influence the election's results.

Defacements and data dumps can cause reputation loss along with financial, and in this case, political damage. Over the last year, hacktivists have increased activity around social and political issues. Given the amount of media attention these attacks attract; they serve as fodder for cyber-attacks. Protests and political uproars have now taken to the digital world where hacktivists work to spread their message through defacements, SQL injection and denial of service attacks.

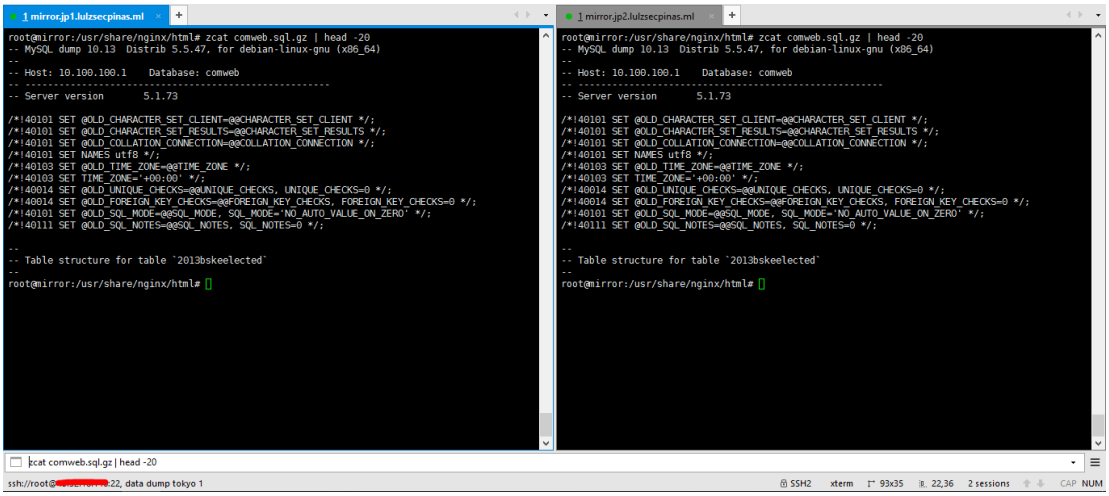


Figure 5: Database leaked via LulzSec Pinas

Video

- https://youtu.be/cTJjMTnEJdE

Attackers

- https://twitter.com/AnonymousPH_
- https://www.facebook.com/LulzSecPinas/

Organizations Under a Cyber Threat Should Consider

Effective DDoS protection elements:

- A hybrid solution that combines on premise detection and mitigation with cloud-based protection for volumetric attacks. It provides quick detection, immediate mitigation and prevents internet pipe saturation.
- Solution must distinguish between legitimate and malicious traffic, protect the SLA and block the attack.
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.

Effective Web Application protection elements (against web intrusions, defacement and data leakage):

- IP-agnostic device fingerprinting – Having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time
- Automatic and real time generation of policies to protect from Zero-day, unknown attacks
- Shortest time from deployment to a full coverage of OWASP Top-10

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

http://www.mb.com.ph/comelec-website-hacked-by-anonymous-group-but-spokesman-assures-poll-results-will-be-secure/

[ii] http://newsinfo.inquirer.net/776683/comelec-shrugs-off-hacking