# Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-31 March 2016

*Source: Agence de Presse Africaine (APA)*

*Date: 31 March 2016*

## Nigeria loses over $450m annually to cyber crimes

"As technology becomes increasingly pervasive and our dependency on it grows, our economic losses will grow exponentially unless pre-emptive measures are taken to mitigate and eliminate the capacity of cybercriminals to take advantage of our environment." READ MORE

---

*Source: Washington Post Writers Group*

*Date: 22 March 2016*

## The biggest cyber heist ever?

"It's a big story that has stayed beneath the radar of most American media. Somehow, cyber criminals stole $81 million from Bangladesh's central bank (its Federal Reserve). The theft surely qualifies as one of the biggest cyber heists ever[…] The money moved from Bangladesh's account at the Federal Reserve Bank of New York to private accounts in the Philippines, from which it was channeled to other accounts, including those of some gambling operations and a casino." READ MORE

RELATED ARTICLES

Bangladesh Bank 'prepares' to sue NY Federal Reserve Bank over funds heist News 24, 24 March

Bangladesh Asks New York Fed, Philippines to Help Retrieve Stolen Money, Gadgets360, 28 March 2016

Bangladeshi Investigators to arrive in Sri Lanka to Probe an Intl. Cyber Crime, Hiru, 22 March 2016

---

*Source: Bloomberg*

*Date: 29 March 2016*

## Feds Drop Apple Case After Gaining Access to Terrorist's iPhone

"The U.S. said it has successfully gained access to the data on the iPhone used by a man in a San Bernardino, Calif., terrorism attack and no longer needs Apple's assistance, marking an end to a legal clash that was poised to redraw boundaries between personal privacy and national security in the mobile Internet age." READ MORE

---

*Source: Le Point*

*Date: 26 March 2016*

## Quand Daech prendra le contrôle d'une centrale nucléaire

"La prise de contrôle d'une centrale nucléaire par des mouvements djihadistes pourrait devenir une réalité « avant cinq ans », a admis samedi le coordinateur de l'Union européenne pour la lutte contre le terrorisme alors que la sécurité des sites nucléaires belges est pointée du doigt." READ MORE

---

*Source: Cytegic*

*Date: 23 March 2016*

## Brussels Attacks likely to Bring Cyber Aftermath

"Following the terror attacks in Brussels on March 22nd, done by ISIS-affiliated terrorists, there is a heightened threat level in Belgium and Western Europe on the cyber front as well. Belgium is forecasted to experience cyber-attacks against high-profile websites and targets such as government and media." READ MORE

*Source: TelesurTV*

*Date: 24 March 2016*

## Caribbean Nations sign off on Cyber Crime Action Plan

"Priority areas in the action plan include training, legislation, technical capacity and law enforcement. Caribbean countries have signed off on a plan of action to strengthen regional co-operation and help governments address cyber security vulnerabilities. It follows a five-day meeting in Saint Lucia that brought together legislators, cyber security experts and international law enforcement bodies such as Interpol." A member of the Cybercrime Convention Committee (T-CY) of the Council of Europe presented the benefits of the Budapest Convention for the Caribbean region. READ MORE

*Source: The Japan News*

*Date: 25 March 2016*

## 18 Million Stolen Credentials Found in Japan

"The IDs and passwords of about 18 million Internet users have been found on a computer server set up by a Tokyo company, which was found in November to have allegedly provided its relay server to parties in China for illegal access, the Metropolitan Police Department announced Friday" READ MORE

*Source: Krebs On Security*

*Date: 24 March 2016*

## 1.5 Million Verizon Customer Records Found for Sale on Dark Web

"Earlier this week, a prominent member of a closely guarded underground cybercrime forum posted a new thread advertising the sale of a database containing the contact information on some 1.5 million customers of Verizon Enterprise. The seller priced the entire package at $100,000, but also offered to sell it off in chunks of 100,000 records for $10,000 apiece." READ MORE

*Source: The Register*

*Date: 24 March 2016*

## Water treatment plant hacked, chemical mix changed for tap supplies

"Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, we're told. […] The utility in question is referred to using a pseudonym, Kemuri Water Company, and its location is not revealed. A "hacktivist" group with ties to Syria compromised Kemuri Water Company's computers after exploiting unpatched web vulnerabilities in its internet-facing customer payment portal, it is reported." READ MORE

*Source: Daily Mirror Sri Lanka*

*Date: 24 March 2016*

## APCERT conducts cyber drill on evolving threat and financial fraud

"The Asia Pacific Computer Emergency Response Team (APCERT) today has successfully completed its annual drill to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies. For the fifth time, APCERT involved the participation of members from the Organisation of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT) in this annual drill. The theme of the APCERT Drill 2016 was *An Evolving Cyber Threat and Financial Fraud.*" READ MORE

*Source: GDataSoftware*

*Date: 24 March 2016*

## Ransomware Petya encrypts hard drives

"The new ransomware which has been dubbed Petya (after the notification it shows to the user) is the first of its kind to encrypt entire hard drives. […] This malware campaign is obviously aiming at companies. In an email application which is sent to the HR department, a Dropbox download link is referenced where allegedly a 'job application portfolio' can be downloaded." READ MORE

*Source: WeLiveSecurity*

*Date: 23 March 2016*

## New self-protecting USB trojan able to avoid detection

"A unique data-stealing trojan has been spotted on USB devices in the wild – and it is different from typical data-stealing malware. Each instance of this trojan relies on the particular USB device on which it is installed and it leaves no evidence on the compromised system. Moreover, it uses a very special mechanism to protect itself from being reproduced or copied, which makes it even harder to detect." READ MORE

*Source: Mashable*

*Date: 23 March 2016*

## Facebook is testing a feature that alerts you if someone is impersonating your account

"The social network is testing a new feature that will automatically alert you if it detects another user is impersonating your account by using your name and profile photo." READ MORE

*Source: NAN – News Agency of Nigeria*

*Date: 21 March 2016*

## Conference to combat world cybercrime opens in Mauritius

"Mauritian Acting-Attorney General, Nandcoomar Bodha, on Monday said that the response to the huge volume of constant hacking and online fraud is the sharing of experiences and intelligence, common policy and determination.

He said while speaking at the second International Workshop on Adaptation and Update of the Electronic Evidence Guide, through the development of the Standard Operating Procedures for Digital Forensics." The event was organised under the GLACY project on Global Action on Cybercrime of the Council of Europe and the European Union. READ MORE

*Source: PressAfrik*

*Date: 17 March 2016*

## Après l'attaque terroriste en Côte d'Ivoire: le Sénégal annonce une plateforme de lutte contre la cybercriminalité

"Les événements récents témoignent que la situation dans le continent demeure plus que jamais préoccupante à la lumière des nombreuses crises qui constituent le quotidien des Etats. Les organisations djihadistes se servent d'internet et des réseaux sociaux comme de puissants vecteurs de propagande et surtout de recrutement " READ MORE

## Latest reports

- ENISA, Strategies for incident response and cyber crisis cooperation, 24 March 2016
- Symantec, Financial Threats 2015, 23 March 2016

## Upcoming events

- 31 March-3 April 2016, Colombo, Sri Lanka - Training of trainers, Introductory course on Cybercrime and Electronic Evidence for the Judiciary
- 5-6 April 2016, Colombo, Sri Lanka - Introductory Training on Cybercrime and Electronic Evidence for Prosecutors
- 4-5 April 2016, Kyiv, Ukraine - Third Meeting on Improving International Cooperation on Cybercrime in the Eastern Partnership region
- 6-7 April 2016, Kyiv, Ukraine - Criminal Justice Access to Evidence Conference
- 11-13 April 2016, Johannesburg, South Africa - International Workshop on Judicial Training Curricula Integration
- 11-14 April 2016, Rabat, Morocco - First Responders Course for the Gendarmerie
- 15 April 2016, Rabat, Morocco - Workshop on training strategies for law enforcement and magistrates

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

**www.coe.int/cybercrime**

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE