

Cybercrime Digest

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

16-30 April 2016

Source: *International
Business Times*

Gundremmingen nuclear power plant in Bavaria shut due to computer malware

Date: 26 April 2016

"On the 30th anniversary of the Chernobyl disaster, a nuclear power plant in Bavaria has been the victim of a computer virus and shut down as a precaution. Malware hit the IT network that handles the fuel handling system at block B of the reactor in Gundremmingen, in the west of the region." [READ MORE](#)

Source: *ICE
Newsroom*

ICE participates in EUROPOL-led effort to identify victims of child abuse

Date: 20 April 2016

"For the past two weeks, victim identification specialists from U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) have been working with top experts from around the globe at Europol's headquarters in The Hague, to work unsolved cases in an effort to identify victims of child sexual abuse and exploitation." [READ MORE](#)

Source: *Reuters*

Bangladesh Bank hackers compromised SWIFT software

Date: 25 April 2016

"The attackers who stole \$81 million from the Bangladesh central bank probably hacked into software from the SWIFT financial platform that is at the heart of the global financial system, said security researchers at British defense contractor BAE Systems [...] The developments coming to light the unprecedented cyber-heist suggest that a lynchpin of the global financial system could be more vulnerable than previously understood because of weaknesses that enabled attackers to modify a SWIFT software program installed on bank servers." [READ MORE](#)

RELATED ARTICLES

[SWIFT bank network says aware of multiple cyber fraud incidents](#), Reuters, 26 April 2016

[SWIFT: Fraudulent messages sent over international bank transfer system](#) (The Guardian, 25 April 2016)

Source: *MacKeeper*

93 Million Mexican Voter Records Leaked Online

Date: 22 April 2016

"Authorities in Mexico have launched an investigation after a researcher discovered a publicly accessible database containing the personal details of tens of millions of Mexican registered voters. MacKeeper researcher Chris Vickery reported on Friday that he discovered an unprotected database on an AWS server containing 93.4 million records associated with Mexican voters. The records include names, addresses, dates of birth, occupations, voter registration IDs, and other information." [READ MORE](#)

Source: Reuters

Dutch police seize encrypted communication network with 19,000 users

Date: 23 April 2016

"Dutch police said on Friday they have arrested the owner of Ennetcom, a provider of encrypted communications for a network of 19,000 customers, on suspicion of using the business for organized crime and shut it down. Rotterdam judges ordered that Danny Manupassa, 36, be held for 14 days during an ongoing investigation. Prosecutors said he is suspected of money laundering and illegal weapons possession." [READ MORE](#)

Source:
Choozurmobile

Australian Government Initiates Strong Cyber Security Strategy

Date: 24 April 2016

"The Australian government is now running behind cyber crimes aggressively. Prime minister Malcolm Turnbull recently announced AU\$230 million worth for Cyber Security Strategy. Subsequent cyber crime defensive failure may have led to this decision, authorities reported. Prime minister also said – the use of such a capability is subject to stringent legal oversight and is consistent with our support for the international rules-based order and our obligations under international law." [READ MORE](#)

Source: IT Web
Africa

Warning of cybercrime crisis in Botswana

Date: 26 April 2016

"IT experts have advised companies in Botswana to strengthen their information security and warn that most businesses in the Southern African country fall way short of implementing the required level of cyber protection. Beza Belayneh, Cyber security Architect at the African Cyber Risk Institute, South African Centre for Information Security, says while Botswana's financial sector and foreign-owned companies have generally adopted a stringent approach to cyber security, most organisations in public and private sectors need to do a lot to internalise common practices of information security controls." [READ MORE](#)

Source: Focus News
Agency

Bulgarian President: Bulgaria target of intensive cyber attacks

Date: 14 April 2016

"During the 2015 local elections there were many attacks against the communication and information systems of different state institutions and organisations, which led to websites breakdown, denied access to services and other potential threats for illegal information leak. There were also attacks against Bulgarian banks, airports and other elements of the critical infrastructure. Leak of large amount of personal data of Bulgarian and foreign nationals has been ascertained." [READ MORE](#)

Source: Technociate

Online banking and plastic card-related fraud in India increases 35 percent

Date: 23 April 2016

"The incidence of ATM, credit, debit card and net banking-related fraud has gone up by more than 35 percent between 2012-13 and 2015-16 in India, according to country's federal bank Reserve Bank of India (RBI). According to RBI data, 8,765 cases were reported by banks in 2012-13 and the corresponding figures for subsequent three years were 9,500 (2013-14), 13,083 (2014-15) and 11,997 (in the first nine months of 2015-16) respectively." [READ MORE](#)

Source: Sen360

Pour lutter contre la cybercriminalité : Le Pr Abdoulah Cissé invite nos forces de sécurité à se mieux former et coopérer avec la justice

Date: 24 April 2016

Senegal – "Le professeur Abdoulah Cissé, avocat à la cour, a invité, ce vendredi, les forces de sécurité à se former, s'équiper et coopérer également afin de mieux lutter contre la cybercriminalité. C'était à l'occasion des journées culturelles des élèves de la 42ème promotion de l'école de police et 30ème promotion de l'Administration pénitentiaire." [READ MORE](#)

Source: Le Figaro

Les Français davantage exposés à la cybercriminalité

Date: 12 April 2016

« Pour la première fois depuis cinq ans, la France fait partie des dix pays où la cybercriminalité est la plus active, les trois premières places étant occupées par la Chine, les États-Unis et l'Inde. » [READ MORE](#)

Source: Forbes

Hacker Offers Millions of Naughty America Accounts For A Mere \$300

Date: 14 April 2016

"Stolen databases containing emails and passwords of 3.8 million porn users, which a hacker claims to have taken from the owner of the Naughty America porno production house, [...] are for sale at just 0.7048 Bitcoin, worth approximately \$300. [...] The databases for sale on Tor-based dark market The Real Deal come not just from NaughtyAmerica.com, but affiliated groups including gay porn site Suite703 and related forums, according to the seller, who also offered access to the server they claimed to have hacked into." [READ MORE](#)

Source: Microsoft

Keeping secrecy the exception, not the rule: An issue for both consumers and businesses

Date: 14 April 2016

"This morning we filed a new lawsuit in federal court against the United States government to stand up for what we believe are our customers' constitutional and fundamental rights – rights that help protect privacy and promote free expression. This is not a decision we made lightly, and hence we wanted to share information on this step and why we are taking it." [READ MORE](#)

Source: *The Star Online*

FBI chief sees better cyber cooperation from China

Date: 27 April 2016

"FBI Director James Comey said he has seen some improvement in cooperation from China in fighting cybercrime following last year's bilateral agreement on the issue. Chinese authorities "seem to have an agreed upon framework for what is nation-state action appropriate, that is intelligence collection, and what is theft," Comey told a cybersecurity event in Washington, when asked about international cooperation on cybercrime." [READ MORE](#)

Latest reports

- Verizon, [2016 Data Breach Investigation Report](#), [Related materials](#), 26 April 2016
- Norse, [Real-time map of attacks](#), 2016
- FireEye, [Follow the Money: dissecting the operations of the cyber crime group FIN6](#), April 2016
- Imperva, [The Secret Behind CryptoWall's Success](#), April 2016
- Ponemon Institute, [The State of Cybersecurity in Healthcare Organizations in 2016](#), April 2016

Upcoming events

- 2 – 3 May – Johannesburg, Pretoria, South Africa, Advisory mission and workshop on reporting systems and public / private cooperation, [GLACY Project](#)
- 2 – 4 May – Dakar, Senegal, Advanced judicial training, [GLACY Project](#)
- 5 – 6 May, 2016, Sarajevo, Bosnia and Herzegovina – Country visit for meeting the relevant stakeholders and collecting the necessary information for the situation report, [iPROCEEDS Project](#)
- 9 – 10 May, 2016, Tirana, Albania – Country visit for meeting the relevant stakeholders and collecting the necessary information for the situation report, [iPROCEEDS Project](#)
- 9 – 11 May – Dakar, Senegal, Conference on international cooperation in cybercrime and electronic evidence involving 15 west African states, [GLACY Project](#)
- 10 – 12 May, 2016, Minsk, Belarus – Country assessment visit on Public/Private Cooperation, [EAP III Project](#)
- 10 – 12 May, Tirana, Albania – IPA Western Balkans Security Governance Programming Meeting, [iPROCEEDS Project](#)

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