Cybercrime Digest

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

16-30 June 2016

Source: Department of Justice, Republic of Philippines

Date: 29 June 2016

DOJ conducts cybercrime trainings with Council of Europe and Philippine Judicial Academy

"The Department of Justice Office of Cybercrime (OOC) conducted simultaneous cybercrime trainings on 15-22 June 2016 in Philippine Judicial Academy (PHILJA) Training Center, Tagaytay City, for law enforcers, prosecutors, public attorneys, and judges. This is in line with the Global Action against Cybercrime (GLACY) project in partnership with the Council of Europe (COE). The specialized trainings focused on cyber-incident responses, cybercrime investigation, handling of electronic evidence, and international cooperation." READ MORE

Source: The Fiji Times

Date: 29 June 2016

Fight against cybercrime in Fiji

"Communications Minister Aiyaz Sayed-Khaiyum says Fiji cannot let its cyber defences down and cannot go it alone in the fight to protect the information and privacy of the Fijian people. He made the comment while discussing technological advances in cyber security and Fiji's role in combating cyber crime in the Pacific with Jayantha Fernando, the program director and legal adviser of Sri Lanka's Information and Communications Technology Agency. Mr Sayed-Khaiyum said the Government hoped to improve its processes and laws relating to cyber crime prevention, specifically the Budapest Cybercrime Convention which it hoped to ratify." READ MORE

Source: Le Monde Informatique

Date: 29 June 2016

L'ANSSI avertit des risques de sabotage dans les SI de l'industrie en France

"Les entreprises françaises n'ont jamais été aussi vulnérables. Des agents dormants infiltrés dans les systèmes informatiques menacent, surtout dans l'industrie, selon l'ANSSI." READ MORE

Source: Capital Business

Date: 27 June 2016

Kenya loses Sh2bn in cyber crime annually

"This is despite the formation of Kenya National Computer Incident Response Team Coordination Centre launched in 2012 and the development of the national cyber security strategy in 2014. According to the report, Kenya is among other developing markets being targeted for cyber crimes, which is despite the notion that cyber attackers only target developed markets. "Contrary to the perception that cyber breaches are a problem unique to the large multinational companies based in developed markets, East African organisations are fast becoming a target for attacks with local subsidiaries particularly attractive as the 'cyber' route into these multinationals," said the report." READ MORE

RELATED ARTICLES

Here's how hackers hit African organisations, Fin24 Tech, 28 June 2016

Source: SoftPedia

Date: 27 June 2016

Underground market selling details of compromised servers in 173 countries

"An underground marketplace has been found to be selling information of more than 70,600 compromised servers in both government and private networks, located across 173 countries including Singapore, China, Malaysia, and Australia. Available for sale from US$6 each, access to these servers was being hawked at a cyber black market called xDedic, which appeared to be operated by a Russian-speaking group, according to Kaspersky Lab. Researchers from the cybersecurity vendor had received a tipoff from a European ISP in March 2016 about the marketplace and both companies jointly investigated the underground operations." READ MORE

Source: Security Affairs

Date: 27 June 2016

Another victim of SWIFT attackers, they steal $10 million from a Ukrainian bank

"Unknown hackers have stolen $10 million from an unnamed Ukrainian bank through SWIFT loophole. The news was spread by the Kyiv branch of ISACA, the Information Systems Audit and Control Association, that confirmed the fraudulent activity was carried on through the SWIFT international banking system that manages money transfers between financial institutions worldwide." READ MORE

Source: HelpNet Security

Date: 23 June 2016

154 million US voter records exposed, revealing gun ownership, Facebook profiles, and more

"MacKeeper security researcher Chris Vickery has discovered yet another database containing voter profiles of US citizens, accessible to anyone who stumbled upon it or knew where to look. This one contains records on 154 million voters, which include their name, address, phone number, age, gender, marital status, estimated income, political party, congressional and state senate district affiliation." READ MORE

Source: SC Magazine

Date: 28 June 2016

Russia's Duma approves bill requiring decryption backdoors

"Russia's lower house of parliament approved sweeping anti-terrorism legislation that requires companies to decrypt any message sent by users. The surveillance laws would enlist messaging apps, social networks, and other services in providing the Federal Security Service (FSB), the successor to the KGB, with access to all communications within Russia upon request." READ MORE

Source: Security Week

Date: 23 June 2016

Botnet of 3 Million Twitter Accounts Remains Undetected for Years

"Not all the Twitter accounts have created by humans, and researchers recently caught wind of no less than 3 million such accounts that were all created on the same day two years ago, but which are still active today. […] The 3 million accounts botnet is responsible for a total of 2.6 billion tweets (including retweets), with a daily activity of 500 million tweets. […] This amount of tweets is enough to handle on world top any hashtag for 8 years permanently."" READ MORE

Source: ZDNet

Date: 15 June 2016

A Massive Botnet of CCTV Cameras Involved in Ferocious DDoS Attacks

"A botnet of over 25,000 bots lies at the heart of recent DDoS attacks that are ferociously targeting business around the world. More exactly, we're talking about massive Layer 7 DDoS attacks that are overwhelming Web servers, occupying their resources and eventually crashing websites. […] Taiwan accounted for a quarter of all compromised IPs, followed by the US, Indonesia, Mexico, and Malaysia. In total, the compromised CCTV systems were located in 105 countries." READ MORE

Source: ComputerWeekly

Date: 23 June 2016

New cyber security law in the offing for Singapore

"Singapore's minister for communications and information Yaacob Ibrahim told lawmakers that the country needs updated cyber laws, and that a new Cyber Security Bill will be tabled in Parliament in 2017. He said the proposed bill will ensure that operators take proactive steps to secure critical information infrastructure, as well as report incidents." READ MORE

Source: Free Malaysia Today

Date: 28 June 2016

Malaysia: Need for special unit to tackle Dark Web

"The Government has been urged to establish a dedicated cybercrime unit to tackle the Dark Web. Akhbar Satar of the Institute of Crime and Criminology at Help University said this was necessary in view of the dangers posed by people using the World Wide Web for nefarious purposes. The most recent case of such abuse involved Briton Richard Huckle, who was jailed for life after admitting to 71 charges of sexual abuse against children in Malaysia. He had used the Dark Web to post more than 20,000 pictures of children as young as six months old being sexually abused from 2006 to 2014." READ MORE

Source: The Standard

Date: 24 June 2016

Philippine Police nab 20 in Bulacan on 'sextortion' charges

"The Philippine National Police Anti-Cybercrime Group arrested 20 persons for cybercrime charges during an operations in San Jose del Monte City, Bulacan, PNP-ACG director, Senior Superintendent Guillermo Lorenzo T. Eleazar said Thursday. Eleazar said that before midnight Wednesday the cybercops raided a cybersex den in San Jose del Monte City, Bulacan where they arrested 20 persons, 13 of them males accused of recording the sex act of their victims and threatening to send the video to their target's families if their extortion demand is unheeded." READ MORE

Source: IT Web

Date: 23 June 2016

DNS attacks on the increase, concern for South African firms

"[…] As the number of connected devices and the volume of data continues growing exponentially, businesses and consumers are now totally reliant on the Internet. The challenges of securing our networks becomes bigger and more complex; and the potential threats become increasingly alarming." READ MORE

Source: Bank Info Security

Date: 20 June 2016

$55 Million in Digital Currency Stolen from Investment Fund

"An experimental investment fund based on the digital currency ether, which runs on the ethereum platform, has been hacked, with about $55 million worth of the currency stolen, according to news reports. Founders of the $150 million fund, known as the Decentralized Autonomous Organization, have shut it down in the wake of the June 17 hack and are planning for its unwinding, the Wall Street Journal reports. The attackers stole about 3.6 million ether coins, valued at about $55 million, and moved it to another account, the newspaper reports." READ MORE

Latest reports

- ENISA, Personal Data Breach Notification Tool, 17 June 2016
- S. Shackelford, Human Rights and Cybersecurity Due Diligence: A Comparative Study, 16 June 2016
- Kaspersky, Ransomware 2014-2016, 22 June 2016
- EMC, Global Data Protection Index 2016, June 2016
- Venice Commission, Opinion on Turkey Regulation of Publications on the Internet and Combating Crimes Committed by Means of such Publication, 15 June 2016

Upcoming events

- 12 – 14 July, 2016, Canterbury, United Kingdom – Final meeting of the EC funded project on the efficiency of 24/7 points of contact, EAP II

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime