Cybercrime Digest

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

1-15 April 2016

Source: Associated Press

Date: 6 April 2016

Data of nearly 50 million Turks allegedly leaked online

"Hackers have posted a database online that seems to contain the personal information of nearly 50 million Turkish citizens in what is one of the largest public leaks of its kind. The Associated Press on Monday was able to partially verify the authenticity of the leak by running 10 non-public Turkish ID numbers against names contained in the dump. Eight were a match." READ MORE

Source: Bloomberg, 6 April 2016

German Police Arrest Key Suspect in Global Cybercrime Raids

"German police have arrested the main suspect in a ring of globally operating cyber criminals… The alleged ring sold software to conceal viruses, blackmail individuals and steal items such as passwords and banking data, prosecutors said in a statement. About 700 police raided 175 apartments and offices across Germany on Tuesday and also searched properties in the Netherlands, France and Canada. Among the items seized were computers as well as weapons and drugs."

READ MORE

Source: Security Week

Date: 8 April 2016

55 Million Exposed After Hack of Philippine Election Site

"A cyber-attack on the website of the Philippines Commission on Elections (Comelec) has resulted in personally identifiable information (PII) of roughly 55 million people being leaked online. While there are no exact details on the number of affected people, it appears that hackers managed to grab the entire voter database, which includes information on the 54.36 million registered voters for the 2016 elections in the Philippines. Information on voters abroad also leaked, along with other sensitive data." READ MORE

Source: SC Magazine

Date: 8 April 2016

Costa Rica investigating rigged elections by political hacker

"Jailed political hacker Andrés Sepúlveda admitted to running underhanded campaigns with the use of black propaganda and other tactics to influence many presidential elections across Latin America including Costa Rica, Mexico, Nicaragua, Colombia and more for almost a decade, from 2005-2013. For $12,000 (£8,500) a month, a customer of Sepúlveda could hire a crew that could hack smartphones, spoof and clone web pages, and send mass emails and texts. For $20,000 (£14K) a month, a more extensive package included a full range of digital interception, attack, decryption and defence." READ MORE

Source: Times of Malta

Date: 14 April 2016

Evidence in the cloud

"Security and privacy experts have long warned that cyber criminals would launch attacks on servers storing the data in cloud environments. Also, criminals are now known to be using the cloud infrastructure itself to get more capability out of their efforts to siphon money out of bank accounts across the globe. In other words, the same flexibility and freedom companies get from having their software and services hosted in the cloud is enabling criminals to conduct highly automated online banking scams." READ MORE

Source: FBI

Date: 4 April 2016

FBI Warns of Dramatic Increase in Business E-Mail Scams

"The schemers go to great lengths to spoof company e-mail or use social engineering to assume the identity of the CEO, a company attorney, or trusted vendor. They research employees who manage money and use language specific to the company they are targeting, then they request a wire fraud transfer using dollar amounts that lend legitimacy. […] This amounted to more than $2.3 billion in losses." READ MORE

RELATED ARTICLES

FBI: $2.3 Billion Lost to CEO Email Scams, Krebs On Security, 7 April 2016

Source: ESET

Date: 7 April 2016

Mumblehard Botnet Finally Taken Down, Sending No More Spam

"A year ago, ESET analyzed the Mumblehard botnet which was comprised of thousands of infected Linux systems located all around the world. Today, ESET announces that in cooperation with CyS-CERT and the Cyber Police of Ukraine, Mumblehard has been successfully taken down. […] The forensics analysis revealed that at the moment of takedown, there were nearly 4000 systems from 63 different countries in the botnet." READ MORE

Source: Yahoo! Finance

Date: 7 April 2016

Victims paid more than $24 million to ransomware criminals in 2015

"The DOJ revealed that the Internet Crime Complaint Center (IC3) had received nearly 7,700 public complaints regarding ransomware since 2005, totaling $57.6 million in damages. Those damages include ransoms paid — generally $200 to $10,000, according to the FBI — as well as costs incurred in dealing with the attack and estimated value of data lost. In 2015 alone, victims paid over $24 million across nearly 2,500 cases reported to the IC3." READ MORE

Source: Star Africa

Date: 12 April 2016

Senegal to create structure to fight cybercrimes

"The Senegalese Posts and Telecommunications minister, Yaya Abdul Kane, announced Tuesday in Dakar, the creation of national structure that will be responsible for coordinating the efforts to ensure cyber security. "To counter the activities of cybercriminals, we will take several measures. One of them includes the establishment of a national structure on cyber security coordination" the minister said." READ MORE

Source: The Citizen

Date: 12 April 2016

South Africa taking fight to cyber crime

"With cyber crime costing South Africa R1 billion a year, training for police, prosecutors, judges and magistrates is essential in fight against online criminals worldwide. That was what a workshop on the integration of cyber crime and electronic evidence into the judicial training curriculum heard yesterday. At least seven countries, including South Africa, were part of the workshop, held in Johannesburg. The Council of Europe (CU) in 2009 adopted a concept recommending that modules on cyber crime be integrated into training curriculum for law enforcement authorities." READ MORE

Source: Symantec

Date: 12 April 2016

Cybercriminals go corporate

"Symantec's Internet Security Threat Report reveals an organizational shift by cybercriminals. They are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers." Major highlights for 2015:

- A New Zero-Day Vulnerability Discovered on Average Each Week.
- Over Half a Billion Personal Records Were Stolen or Lost.
- Major Security Vulnerabilities in 3/4 of Popular Websites.
- Spear-Phishing Campaigns Targeting Employees Increased 55%.
- Ransomware Increased 35%
- 100 Million Fake Technical Support Scams have been blocked.

READ MORE

Source: EU Neighbourhood Info Centre

Date: 1 April 2016

EU launches new project to battle cybercrime in Eastern Partnership countries

"The EU and the Council of Europe are together launching a new project to improve public-private cooperation on cybercrime and electronic evidence in Eastern Partnership countries. Criminal justice authorities, telecommunications regulators and major service providers will gather for a regional meeting in the Ukrainian capital Kyiv next week, when the new project, entitled 'Cybercrime EAP III', will be presented." READ MORE

Source:
WeLiveSecurity

Date:
23 March 2016

New Cybersecurity Bill to be tabled next year to strengthen Singapore's online defences

"A new Cybersecurity Bill that aims to strengthen laws against online crime will be tabled in Parliament next year (2017). Minister for Communications and Information Yaacob Ibrahim told Parliament the proposed law will ensure that operators of Singapore's critical information infrastructure take active steps to secure such systems and report incidents." READ MORE

Latest reports

- Europol, Fraud scams targeting employees - Infographic, April 2016
- Dell, Underground Hacker Markets Annual Report 2016, April 2016
- Symantec, Internet Security Threat Report (ISTR), Volume 21, April 2016
- Intelliagg, Deep Light – Shining a Light on the Dark Web, April 2016
- Buguroo, Analysis of Latest Dridex Campaign Reveals Worrisome Changes and Hints at New Threat Actor Involvement, April 2016

Upcoming events

- 13 – 15 April, 2016, Yerevan, Armenia – Country assessment visit on Public/Private Cooperation
- 14 – 15 April, 2016, Belgrade, Serbia – Country visit for meeting the relevant stakeholders and collecting the necessary information for the situation report
- 15 April 2016, Rabat, Morocco - Workshop on training strategies for law enforcement and magistrates
- 18 – 19 April, 2016, Podgorica, Montenegro – Country visit for meeting the relevant stakeholders and collecting the necessary information for the situation report
- 18 – 20 April, 2016, Tbilisi, Georgia – Country assessment visit on Public/Private Cooperation
- 21 – 22 April, 2016, Skopje, "the former Yugoslav Republic of Macedonia" – Country visit for meeting the relevant stakeholders and collecting the necessary information for the situation report
- 25-27 April 2016, Colombo, Sri Lanka – International Workshop and training for 24/7 points of contacts of GLACY countries

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