

Cybercrime Digest

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

16-30 September 2016

Source: *The New York Times*

Date: 22 Sep 2016

Yahoo Says Hackers Stole Data on 500 Million Users in 2014

“Yahoo announced on Thursday that the account information of at least 500 million users was stolen by hackers two years ago, in the biggest known intrusion of one company’s computer network. In a statement, Yahoo said user information — including names, email addresses, telephone numbers, birth dates, encrypted passwords and, in some cases, security questions — was compromised in 2014 by what it believed was a “state-sponsored actor.” While Yahoo did not name the country involved, how the company discovered the hack nearly two years after the fact offered a glimpse at the complicated and mysterious world of the underground web.” [READ MORE](#)

RELATED ARTICLES

Ars Technica, [Yahoo says half a billion accounts breached by nation-sponsored hackers](#), 22 Sep 2016

Yahoo, [An Important Message About Yahoo User Security](#), 22 Sep 2016

Source: *Acento*

Date: 23 Sep 2016

La República Dominicana será sede regional GLACY+ para luchar contra el cibercrimen en América Latina y el Caribe

“El Consejo de Europa y la Policía Internacional (INTERPOL) incorporarán a la República Dominicana al proyecto GLACY+ (Acción Global Contra el Cibercrimen Extendido), con miras a dotar al país de políticas, estrategias y recursos humanos con capacidad de enfrentar los delitos que se generan en las redes de Internet. La República Dominicana, único entre 10 países del hemisferio que integran el proyecto GLACY+, servirá como centro regional para todos los países de América Latina y el Caribe. Una misión del Consejo de Europa e INTERPOL realizan del 19 al 23 de este mes, un levantamiento de las capacidades e identifican necesidades de la República Dominicana para incorporarla en el proyecto GLACY+ sobre creación de capacidades en la lucha contra la delincuencia cibernética.” [READ MORE](#)

Source: *Nineoclock*

Date: 18 Sep 2016

Romanian Police conduct 5,655 computer searches and seizures to dismantle 24 cybercrime rings

“Cybercrime officers with the Romanian Police conducted 5,655 computer searches and seizures and 451 domiciliary visits in the first eight months of 2016 to dismantle 24 cybercrime rings made up of 182 people. [...] The Romanian Police General Inspectorate says in order to recoup the damage involved, liens have been put on 12 buildings and 19 motor vehicles, with more than 140,000 lei, 200,000 euros and 370,000 US dollars impounded. Part of the same action, 330 people were investigated, of whom 143 were detained, 118 arrested and 83 placed under court supervision, all on suspicion of cybercrimes.” [READ MORE](#)

Source: *Belarusian
Telegraph Agency*

Date: 23 Sep 2016

Council of Europe eager to cooperate with Belarus in fighting cybercrimes

"The Council of Europe has expressed interest in stepping up cooperation with Belarus in fighting cybercrimes, BelTA learned from representatives of the Belarusian Justice Ministry after the second regional meeting of the Eastern Partnership Initiative participating states on public private partnership in the sphere of cybercrime control and digital evidence. [...] Experts of the Council of Europe and representatives of Belarusian government agencies presented the best practices of public private partnership in this sphere. Interaction of power-wielding agencies with international corporations and the legal framework for counteracting high-tech crimes were discussed." [READ MORE](#)

Source: *UK
Government*

Date: 22 Sep 2016

Joint statement by the governments of the United Kingdom and Germany

"The Home Secretary of the United Kingdom, The Rt Hon Amber Rudd, and the Interior Minister of Germany, Dr. Thomas de Maizière, met in Berlin on 22 September 2016. [...] In recognition of the ongoing terrorist threat to Europe, our ministries as well as our security and law enforcement agencies will: [...] call on those who have not yet signed and ratified the Budapest Convention on Cybercrime to do so as soon as possible." [READ MORE](#)

Source: *Roar.Ik*

Date: 22 Sep 2016

Mauritius, only African state party to Budapest Convention on Cybercrime

"The East African country of Mauritius is the only nation from the continent that has acceded and is a state party to the Budapest Convention on Cybercrime. Head, Cybercrime Division, Council of Europe, Mr. Alexander Seger confirmed this to ITRealms and said that Mauritius, an Indian Ocean island nation, stands out among equal for this remarkable position on cybercrime. Mr. Seger told that invitation has been extended to three countries in Africa, including Senegal, Ghana and Morocco to accede to the convention on cybercrime. [...] Mr. Seger acknowledged that South Africa participated in the negotiation of the treaty and has signed the Convention and its Protocol on Xenophobia and Racism but has not yet ratified these. [...] He disclosed that given the commitment of these States to implement the Budapest Convention they are also priority countries for capacity building." [READ MORE](#)

Source: *Roar.Ik*

Date: 22 Sep 2016

Cybercrime in Sri Lanka – What We Know

"[...] Computer crimes are borderless – in that geographical boundaries pose little or no roadblocks. There have been cases where an individual from overseas hacked into a person's bank account in Sri Lanka, and transferred the money to another foreign account, from which it would be withdrawn by a third party. Therefore, it is imperative that authorities in all countries are aware of such activities, in order to successfully tackle cybercrime. This is where the Budapest Convention comes into play. [...] Sri Lanka ratified the Convention and signed its entry in 2015." [READ MORE](#)

Source: *US Mission
to France*

First France-U.S. Cyber Bilateral Meeting in Paris

"[...] The representatives of US and France discussed countering use of the Internet for terrorist and criminal purposes, as well as management and coordination efforts of

Date: 15 Sep 2016

governments mitigating cyber incidents. The discussion of capacity building focused on coordinating our efforts in various venues. The US and France intend to continue their productive collaboration on countering the use of the Internet for terrorist purposes and countering violent extremism, both online and offline, improve cyber incident management and coordination, promote accessions to the Budapest Convention, and build cyber capacity of other countries." [READ MORE](#)

Source: Dialogo

Cyberdefense and Cybersecurity in Colombia

Date: 22 Sep 2016

"In March 2014, Colombian President Juan Manuel Santos sought advice from international cybersecurity experts and support from the Organization of American States (OAS) [...] to draw up a series of recommendations that would give the government a solid and professional technical base when implementing its system. Among the main recommendations: that the system be harmonized in accordance with the Convention on Cybercrime, known as the Budapest Convention, to take into account successful legislation on digital crime." [READ MORE](#)

Source: Prothom Alo

Cybercrime cases on the rise in Bangladesh

Date: 24 Sep 2016

"Cybercrime has increased in Bangladesh rapidly in recent years. The number of cybercrime cases has risen almost 200 times. Most of the cases were filed under section 57 of the Information Communication Technology (Amendment) Act 2013. However, recent statistics from the cyber tribunal shows that this law is being used to harass people with baseless cases. The cyber tribunal started in 2013 with only three cases. The next year, the number became 32, in 2015 it was 152. The number within 15 September 2016 is 156, with 250 cases under investigation." [READ MORE](#)

Source: Reuters

Kosovo hacker gets 20 years in U.S. for helping Islamic State militants

Date: 23 Sep 2016

"A Kosovo citizen was sentenced to 20 years in prison on Friday for hacking the personal data of more than 1,000 U.S. military and government personnel and passing the information to Islamic State militants, the U.S. Department of Justice said. Ardit Ferizi, 20, who was also known as Th3Dir3ctorY, was arrested in Malaysia last year and extradited to the United States, where he pleaded guilty in a Virginia federal court in June." [READ MORE](#)

Source: Fintech
Finance

UK, 4.5 million people forced to cancel credit & debit cards in the last year due to online fraud

Date: 19 Sep 2016

"One in ten people have been the victim of a cyber-attack on their credit or debit card in the last year, according to new research. In 62% of cases, money was successfully removed from the account with an average of £475 stolen. At a national level this equates to 4.5 million credit or debit cards cancelled in the last twelve months with more than £2.1 billion stolen in total." [READ MORE](#)

Source: Daily News

Zimbabwe's Cyber Bill "not cast in stone"

Date: 23 Sep 2016

"The Computer Crime and Cyber Security Bill should be reviewed after every two years for it to remain relevant to ever-changing technological advancement, a senior Government official has said. Secretary for Information Communication and Technology, Postal and Courier Services Engineer Sam Kundishora said this during a consultative workshop on the Bill that was attended by several stakeholders in the ICT sector recently." [READ MORE](#)

Source: Daily News

Cybercrime touted as key new ICT policy focus area in Tanzania

Date: 23 Sep 2016

"Innovation and cybercrime should be among the key areas in implementing national policy on Information Communication Technology (ICT). The Permanent Secretary (PS) in the Ministry of Works, Transport and Communications, Professor Faustin Kamuzora, said in Dar es Salaam yesterday that stakeholders should consider changes that have occurred in the recent years in the sector." [READ MORE](#)

Source: Legally India

What is the India-US cyber partnership and why does it matter?

Date: 22 Sep 2016

"Both nations have agreed to promote close co-operation between their law enforcement agencies to combat cybercrime. They will share information on cybersecurity threats on a real-time basis, and will develop joint mechanisms to mitigate such threats. They will also conduct joint training programs for law enforcement agencies as a capacity-building measure. These commitments are likely to help India gain support and assistance with the investigation of cybercrimes. This is much needed support that we have lacked, in part because of India's refusal to sign the Budapest Convention, which arguably limited our ability to tackle several cybersecurity issues. This is particularly so in the context of the jurisdictional issues and information sharing for which the Convention creates a framework. The US-India Cyber Partnership commitments resemble the Budapest Convention (on Cybercrime), 2001 recommendations (contained within Article 23)." [READ MORE](#)

Source: Contralinea

México, indefenso ante ciberataques

Date: 18 Sep 2016

"México cuenta con escasa capacidad de prevención y casi nula de reacción ante incidentes cibernéticos con potencial para comprometer infraestructuras críticas del país e información sensible de las instituciones y las personas, según se desprende del capítulo sobre ciberseguridad de la Agenda Nacional de Riesgos." [READ MORE](#)

Source: Club of Mozambique

Mozambique must ratify Budapest Convention on Cyber Crime – Attorney General Beatriz Buchili

Date: 28 Sep 2016

"Mozambique's Attorney General is recommending that the country proceed with ratifying the Budapest Convention on cyber crime. [...] the ratification could occur while concurrently studying other measures that may entail the amendment of Mozambique's criminal code or the creation of specific legislation on the matter." [READ MORE](#)

Source: Europol

The relentless growth of cybercrime

Date: 28 Sep 2016

"Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) identifies an expanding cybercriminal economy exploiting our increasingly Internet-enabled lives and low levels of digital hygiene. Informed largely by Europol's law enforcement and cooperation partners, the report identifies eight main cybercrime trends and provides key recommendations to address the challenges: Crime-as-a-Service, Ransomware, The criminal use of data, Payment fraud, Online child sexual abuse, Abuse of the Darknet, Social engineering, Virtual currencies." [READ MORE](#)

Latest reports

- Europol – [IOCTA - Internet Organized Crime Threat Assessment 2016](#), 28 Sep 2016
- ENISA, [A week to go for the European Cyber Security Month launch!](#), 23 Sep 2016
- Arbor Networks, [20 years of DDoS attacks targeting ISP networks](#), 18 Sep 2016
- McAfee, [Cryptocurrencies a Target for Cybercriminals, Part 2: Social Platforms Come Next](#), 18 Sep 2016
- Council of Europe – Cloud Evidence Group of the Cybercrime Convention Committee, [Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY](#), 16 Sep 2016

Upcoming events

- 3-4 October 2016, Podgorica, Montenegro – Advisory mission and workshop for the setting up or improvement of reporting mechanisms, [iPROCEEDS](#)
- 3-6 October 2016, Rabat, Morocco – Progress review meetings and updated situation reports, [GLACY/ GLACY+](#)
- 3-7 October 2016, Abuja, Nigeria – INTERPOL Training on investigating cybercrime cases for investigators from African countries, [GLACY+](#)
- 6-7 October 2016, Chisinau, Republic of Moldova – Public-Private cooperation: Workshop on crime and incident reporting framework including national CERT, [EAP III](#)
- 3-8 October 2016, Accra, Ghana – Initial Assessment mission, [GLACY+](#)
- 11-12 October 2016, Zagreb, Croatia – Regional workshop on judicial training curricula on cybercrime, electronic evidence and online crime proceeds, [iPROCEEDS](#)
- 12-14 October 2016, Baku, Azerbaijan – Public-Private cooperation: Workshop on cooperation between the law enforcement and ISPs, focusing on preservation, [EAP III](#)

Announcements

- ▶ [OCTOPUS Conference 2016](#) – Cooperation against Cybercrime, 16–18 November 2016, Strasbourg, France: registrations are open until 15 October 2016
- ▶ The [Call for tenders 2016AO48 - Framework Agreement for the provision of services of consultancy on cybercrime and electronic evidence](#) is open for applications until 23 October 2016

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