Cybercrime Digest

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

1-15 October 2016

Source: Council of Europe

Date: Oct 2016

Global Action on Cybercrime: From GLACY to GLACY+

“Building on the positive results of GLACY, a new joint project of the European Union and the Council of Europe commenced in March 2016, that is, the Global Action on Cybercrime Extended (GLACY+). The Closing Conference of the GLACY project and the Launching Conference of GLACY+ will be held from 26 to 28 October in Bucharest, Romania. The aims of the conference are:

- To review the achievements of the GLACY project;
- To engage decision-makers, project teams and project partners to the GLACY+ project;
- To facilitate cooperation with relevant international organisations;
- To reach agreement on the GLACY+ project workplan.”

READ MORE

Source: News18

Date: 1 Oct 2016

Cybercrime as a Service: Europol Hints at Militants Using Darknet

“Cybercriminals offering contract services for hire offer militant groups the means to attack Europe but such groups have yet to employ such techniques in major attacks, EU police agency Europol said on Wednesday.

"There is currently little evidence to suggest that their cyber-attack capability extends beyond common website defacement," it said in its annual cybercrime threat assessment in a year marked by Islamic State violence in Europe.

But the internet's criminal shadow the Darknet had potential to be exploited by militants taking advantage of computer experts offering "crime as a service", Europol added: "The availability of cybercrime tools and services, and illicit commodities (including firearms) on the Darknet, provide ample opportunities for this situation to change." READ MORE

Source: ZD Net

Date: 13 Oct 2016

Google divulges more data on its users than ever, as government requests spike

“Google received a record number of government requests in the first six months of 2016, its latest Transparency Report reveals. […] Globally, Google received 44,943 government requests for information about 76,713 accounts during the current period. It produced user data for 64 percent of those requests. Also in the top five by user data requests are Germany, France, India, and the UK, though the percentage of requests where data is actually produced is far smaller than in the US. […] Google also received its first requests ever from Algeria, Belarus, Cayman Islands, El Salvador, Fiji, and Saudi Arabia.” READ MORE

Source: SCMagazineUK.com

Date: 5 Oct 2016

Russian special services to decrypt Internet traffic

"The Russian Federal Security Service (FSS, or FSB) together with the country's Ministry of Communications, are introducing of a set of technical procedures that will provide it with unencrypted access to the Internet traffic of all Russian citizens. This move is the implementation of the recently approved Yarovaya Law, (a package of bills which amended a pre-existing counter-terrorism law as well as separate laws regulating counter-terror and public safety measures), which obliged local and global IT companies, operating in Russia, including Google, "Yandex", Mail.ru Group, Whatsapp, Telegram, Viber, Facebook, "VKontakte" to provide encryption keys for their web-servers at the request of the FSB." READ MORE

Source: Vending Times

Date: 7 Oct 2016

International Effort Will Attempt To Halt Illegal Use Of Digital Currencies

"Europol and Interpol have joined with the Basel Institute on Governance to establish a working group to combat the spread of money laundering through digital currencies such as Bitcoin. According to a statement released by the group, there is a clear consensus that digital currencies pose money-laundering and terrorism-financing threats. […] The multi-agency cooperation agreement was reached during the recent 4th annual Interpol-Europol Cybercrime Conference in Singapore. The newly established working group will share, gather, analyze and exchange nonoperational information regarding the use of digital currencies as a means of money laundering, as well the investigation and recovery of criminal proceeds." READ MORE

Source: Modern Ghana

Date: 14 Oct 2016

G7 Boost Banking Cybersecurity as New SWIFT Threat Emerges

"The G7 group of leading economies laid out a new framework for battling the hacking of financial institutions Tuesday as a new threat using the SWIFT interbank network emerged. The two-page "Fundamental Elements of Cybersecurity" outlines the building blocks of an effective risk-based bank program to defend itself and the broader financial system from cyber threats. The guidelines are aimed at public and private sector financial institution board members and top management to use for shaping and assessing their company's cyber strategy." READ MORE

Source: Modern Ghana

Date: 14 Oct 2016

Ghana Police set October deadline for political parties, others to comply with data protection law

"The Cyber Crime Unit of the Ghana Police Service has set the end of October to political parties and organisations involved in the collection of personal data to register under the Data Protection Act or face sanctions. […] Executive Director of the Data Protection Commission, Teki Akuetteh Falkoner, has told Joy News her office has filed an official complaint against thousands of organizations including all the political parties who have failed to comply with Act. […] Director of Cybercrime Unit at the Ghana Police Service, Chief Superintendent Herbert Gustav Yankson, says heads of organisatons that violate the law could be jailed for two years." READ MORE

Source: CSO Online

Date: 14 Oct 2016

Almost 6000 online shops compromised for credit card theft

"Almost 6,000 online shops have been compromised by hackers who added specially crafted code that intercepts and steals payment card details. These online skimming attacks were first discovered by Dutch researcher Willem de Groot a year ago. At that time, he found 3,501 stores containing the malicious JavaScript code. However, instead of getting better, the situation is increasingly worse. By March the number of infected shops grew by almost 30 percent to 4,476, and by September, it reached 5,925. More than 750 online stores who were unwillingly skimming payment card details for attackers in 2015 are still doing so today, showing that this type of activity can go undetected for months." READ MORE

Source: SC Magazine

Date: 5 Oct 2016

Turkey is the country with the most bot Infections

"Turkey has the largest number of total "bot" infections with one bot for every 1,139 internet users in the country and also contains 18.5 percent of all of the bots across the EMEA region, according to researchers at Symantec's Norton division. Most of the affected computers resign in the cities of Istanbul and Anakara which together account for more than half of the country's population, according to the firm's interactive botnet map. The report also found that following Turkey, the top ten countries by total bot population in descending order include, Italy, Hungary, Germany, France, Spain, the U.K., Poland, Russia, and Israel." READ MORE

Source: Business Times

Date: 10 Oct 2016

Prime Minister Lee launches Singapore's new cybersecurity strategy

"Prime Minister Lee Hsien Loong said on Monday that the government will work with key stakeholders, including private sector operators and the cybersecurity community, to strengthen the resilience of Critical Information Infrastructure (CII) that supports Singapore's essential services. […] Mr Lee said the government will establish robust and systematic cyber risk management processes, as well as response and recovery plans, across all critical sectors. To do so, it is necessary to grow a culture of cyber-risk awareness across CIIs, the Prime Minister said. The increased adoption of security-by-design practices to address cybersecurity issues across the supply chain will remain an important focus, he added." READ MORE

Source: The Nation

Date: 13 Oct 2016

Thailand: Computer crime law changes could violate freedom of expression

"Human rights and international legal organisations yesterday voiced concerns over the new amendment to the Computer Crime Act, saying it could violate international standards, infringe on the right to expression and hamper digital economic growth. The amendment, pending deliberation by the National Legislative Assembly (NLA), will deter people's freedom of expression as it will be used to criminalise offences deemed to affect national security, Kanathip Thongraweewong, a data privacy and social media law specialist from St John University, said." READ MORE

Source: The Daily Mail

Date: 30 Sep 2016

UK's first national anti-cybercrime centre to open with 700-strong team

"Britain's first national centre for combating cyber criminals is set to open next week, as the threat posed by online attacks continues to increase. Terrorists, hackers and online gangs will be targeted by intelligence bosses at the new National Cyber Security Centre (NCSC) in central London. A team of around 700 people are expected to be advancing the Government's war against cybercrime." READ MORE

Source: SapoTek

Date: 7 Oct 2016

Conselho de Ministros aprova criação de Unidade Nacional de Combate ao Cibercrime

"A Polícia Judiciária vai ganhar uma Unidade Nacional especializada no combate ao cibercrime. Em agosto de 2015 o anterior Governo já tinha publicado em Diário da República um diploma que previa a criação desta unidade que, dada a falta de regulamentação, nunca se chegou a materializar. O decreto-lei que prevê a criação da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) foi aprovado esta quinta-feira pelo Conselho de Ministros." READ MORE

Source: Daily Nation

Date: 5 Oct 2016

Communication Authority of Kenya launches centre to fight cybercrime

"Kenya has established a Cyber Coordination Centre, where attacks on critical infrastructure can be reported. The centre, set up by the Communication Authority of Kenya (CA), will respond to actual online attacks or threats, which have led to an increase in online insecurity in the country. [...] CA chairman Ngene Gituku said his agency has also set up an awareness campaign, called Child Online Protection, to provide tips on safe interaction online and ways to identify and (or) avoid predators with ill intentions." READ MORE

Source: Doha News

Date: 8 Oct 2016

What the UAE law says about cybercrimes, penalties

"The UAE has clear - and strict - laws against cybercrimes, with various penalties that can include lengthy prison terms and fines of up to Dh3 million. UAE Cybercrime Law No. 5 of 2012, which was issued by the President, His Highness Shaikh Khalifa bin Zayed Al Nahyan, includes a range of violations and penalties, with fines ranging between Dh50,000 and Dh3 million depending on the type and severity of offence." READ MORE

Source: Linux Magazin

Date: 13 Oct 2016

Jeder zweite ein Cybercrime-Opfer

„Einer von zwei Internetnutzern ist ein Opfer von Computerkriminalität. Die häufigsten Delikte sind Virenangriffe, Betrug und Identitätsdiebstahl.

418 Die Vorfälle reichen von gefährlichen Virusinfektionen über Online-Betrug und Erpressung bis hin zu schweren Beleidigungen: Fast jeder zweite Internetnutzer (47 Prozent) ist in Deutschland in den vergangenen 12 Monaten Opfer von Cybercrime geworden". READ MORE

Source: Doha News

Date: 8 Oct 2016

Qatar's cybercrime law is being abused by criminals and must be changed

"Two years ago, Qatar passed a cybercrime law to protect its people against hackers, child pornography and online fraud, among other things. To date, prosecutors have used the legislation sparingly when it comes to such crimes, in part because other laws have already outlawed such behavior. But in a troubling development, the law instead is being exploited by criminals and individuals with personal agendas to silence others. These people have been capitalizing on the legislation's controversial privacy provisions, which make it illegal to publish news related to the personal or family life of individuals – even if the information is true. The cybercrime law also contains a vaguely worded clause that criminalizes any content found to violate the country's "social values" or "general order." READ MORE

Latest reports

- European Parliament, Study - A Comparative Analysis of Media Freedom and Pluralism in the EU Member States - PE 571.376 - Committee on Civil Liberties, Justice and Home Affairs, 15 Sep 2016
- European Commission, European Agenda on Security: First report on progress towards an effective and sustainable Security Union, 12 Oct 2016
- ENISA, Annual Incident Report 2015, 5 Oct 2016
- The Hamburg Commissioner for Data Protection and Freedom of Information – Administrative order against the mass synchronisation of data between Facebook and WhatsApp, 27 Sep 2016
- Fortinet, Threat Landscape Report, Oct 2016

Upcoming events

- 20 – 21 October, 2016, Chisinau, Moldova - Workshop on Electronic Evidence, EAP II
- 24 – 25 October 2016, International Meeting on Cooperation with Multinational Service providers, iPROCEEDS and EAP III;
- 26 – 28 October 2016, Bucharest, Romania – GLACY Closing and GLACY+ Launching Conference;

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