# Cybercrime Digest

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

1-15 July 2016

---

*Source: New York Times*

*Date: 14 July 2016*

## Microsoft wins appeal on overseas data searches

On Thursday, Microsoft won a surprise victory in one such legal battle against the government over access to data that is stored outside the United States. In the case, the United States Court of Appeals for the Second Circuit reversed a lower court's ruling that Microsoft must turn over email communications for a suspect in a narcotics investigation stored in a Microsoft data center in Dublin. READ MORE

---

*Source: ALL AFRICA*

*Date: 14 July 2016*

## Kenya Govt Calls for Public Participation On Computer and Cyber Crimes Bill 2016

The Ministry of Information, Communications and Technology (ICT) has invited Kenyans to make contributions to the Computer and Cyber Crimes Bill 2016 available on the Ministry's Website. ... The Bill borrows heavily from international standards and global scholars. It has the input of experts from Europe, Inter-Agency Committee for Formulation on Cyber-crime, the Budapest Convention on Cybercrime and the Council of Europe experts. READ MORE

---

*Source: NewsDay*

*Date: 15 July 2016*

## Draft of the Computer Crime and Cybercrime Bill discussed in Zimbabwe

"The Computer Crime and Cybercrime Bill, currently being discussed by different stakeholders in Harare, seeks to impose three-year jail sentences to people who use others' identity to commit crimes via electronic means. The stakeholders were on Wednesday and Thursday gathered at a Harare hotel to discuss the draft Bill by the Ministry of Information Communication Technology at a workshop organised by the Centre for Applied Legal Research (CALR)." READ MORE

---

*Source: ITWeb*

*Date: 6 July 2016*

## SA cyber security laws must be 'modernised'

The highly-criticised national Cyber Crimes and Cyber Security Bill (cyber security Bill) may be what SA needs to effectively combat cyber crime, says Graham Croock, director of IT audit, risk and cyber lab at BDO South Africa. … firstly, our laws need to be modernised, and secondly, the requisite of having one comprehensive law that is able to account for any of these circumstances. Croock says the cyber security Bill will put SA on par with other related international laws such as the Council of Europe's Budapest Convention on Cyber Crime. READ MORE

RELATED ARTICLES

We must modernise cybersecurity law Gadget. 30 June 2016

Anonymous Leaks Data from South Africa's Arms Acquisition Agency, SoftPedia, 12 July 2016

*Source: Council on Foreign Relations*

*Date: 7 July 2016*

## Cyber Diplomacy with Africa: Lessons learned from the African Cybersecurity Convention

The AU's development of the Convention reflects a desire of African states to have autonomy over their response to cyberspace challenges. The AU chose to develop its own Convention instead of promoting African participation in existing cyber treaties, most notably the Council of Europe's Budapest Convention on Cybercrime (2001). READ MORE

*Source: AFCEA Signal*

*Date: 1 July 2016*

## Romania Battles State Actors in Cyberspace

"Romania, now a stalwart member of NATO and the European Union, is playing an increasing role in cybersecurity, both regionally and internationally. It is passing a national cybersecurity law and reaching out to assist other nations, directly and indirectly, with cyber defense. Romania is striving to become a regional cybersecurity hub, says Florin Cosmoiu, head of the Romanian Intelligence Service's (SRI's) National Cyberint Center. The country's related efforts range from creating nationwide education and awareness programs to participating in multinational cybersecurity organizations and activities." READ MORE

*Source: Essential Retail*

*Date: 11 July 2016*

## NCA calls for better reporting of cybercrime incidents

"The National Crime Agency is urging businesses to make use of the cybercrime reporting paths available to them and to share intelligence with law enforcement and each other, in an effort to clamp down on this rising problem in the corporate world. According to the organisation, cybercrime should be treated not only as a technical issue but as a board-level responsibility, arguing that existing levels of under-reporting continue to obscure the full impact of cybercrime in the UK. This shortfall in reporting hampers the process for law enforcement to understand the operating methods of those responsible for these crimes and provides an obstacle in developing an effective response to the threat." READ MORE

*Source: European Commission*

*Date: 5 July 2016*

## European Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats

"The Commission today launches a new public-private partnership on cybersecurity that is expected to trigger €1.8 billion of investment by 2020. This is part of a series of new initiatives to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector. According to a recent survey, at least 80% of European companies have experienced at least one cybersecurity incident over the last year and the number of security incidents across all industries worldwide rose by 38% in 2015. This damages European companies, whether they are big or small, and threats to undermine trust in the digital economy. As part of its Digital Single Market strategy the Commission wants to reinforce cooperation across borders, and between all actors and sectors active in cybersecurity, and to help develop innovative and secure technologies, products and services throughout the EU." READ MORE

| | |
|---|---|
| *Source: Guyana Government Information Agency*<br><br>*Date: 11 July 2016* | ## Guyana, draft cybercrime legislation ready to be presented to Cabinet<br><br>"The cybercrime draft legislation is ready for presentation to Cabinet now that consultations and adjustments on the bill have been completed. Attorney General Basil Williams noted that he will make a special appeal to Cabinet for the legislation to be sent to a select committee when it is presented in Parliament. Once the draft legislation is cleared by Cabinet, it will be laid in Parliament." READ MORE |
| *Source: CybrViews*<br><br>*Date: 4 July 2016* | ## UNODC seeking solutions to stopping drug trade on dark web<br><br>"The United Nation's Office on Drugs and Crime (UNODC) published its annual report on Thursday and placed special emphasis on curbing the illicit trade on the Dark Web. According to the Global Drug Survey report for 2016, drug users are increasingly turning to dark web marketplaces. The UN's report concedes: "Law enforcement and the criminal justice system in many countries are still not in a position to deal effectively with the anonymous online marketplace known as the 'dark net'."" READ MORE |
| *Source: Europol*<br><br>*Date: 12 July 2016* | ## Launch of the IPC3: Europe's response to Intellectual Property Crime<br><br>"To strengthen the fight against counterfeiting and piracy online and offline, Europol and the European Union Intellectual Property Office have joined forces to launch the Intellectual Property Crime Coordinated Coalition (IPC3). The IPC3 will provide operational and technical support to law enforcement agencies and other partners in the EU and beyond." READ MORE |
| *Source: Sophos*<br><br>*Date: 11 July 2016* | ## Big "carding gang" bust announced by Europol: 105 arrests across 15 countries<br><br>EC3, which is shorthand for Europol's *European Cybercrime Centre*, just announced a big "carder gang" bust. Carding is the general term for crimes involving the fraudulent use of credit cards... READ MORE<br><br>RELATED ARTICLE<br><br>International credit card syndicate in Europe and Asia disrupted, EUROPOL, 8 July 2016 |
| *Source: HackRead*<br><br>*Date: 3 July 2016* | ## Internet Bot Exposes 20 Million MTN Irancell Users' Data<br><br>"In a strange incident, an Internet bot has been blamed for hacking 20 million MTN Irancell users, one of the most popular and second largest mobile phone operator in Iran. Fars news agency reported the incident took place on Telegram message app when a @MTNProBot appeared on the service allowing anyone to insert user's phone number and collect their personal information including first name, last name, address, national code, landline number, postal code and city." READ MORE |

*Source: The Daily Observer*

## The Dropping Elephant – aggressive cyber-espionage in the Asian region

*Date: 10 July 2016*

"Dropping Elephant (also known as "Chinastrats" and "Patchwork") is a relatively new threat actor that is targeting a variety of high profile diplomatic and economic targets using a custom set of attack tools. Its victims are all involved with China's foreign relations in some way, and are generally caught through spear-phishing or watering hole attacks. Overall, the activities of this actor show that low investment and ready-made offensive toolsets can be very effective when combined with high quality social engineering." READ MORE

## Latest reports

- NCA, Cyber Crime Assessment 2016, July 2016

- Checkpoint, In-depth analysis of the Hummingbad Android malware campaign, July 2016

- Kaspersky, Industrial cybersecurity threat landscape, 11 July 2016

- KPMG and BT, Taking the offensive: Disrupting Cyber Crime, July 2016

- BitDefender, Ransomware: A Victim Perspective, July 2016

## Upcoming events

- 18 – 19 July 2016, Tbilisi, Georgia – Workshop on cooperation and relations between 24/7 points of contact with relevant stakeholders, particularly Prosecutor's Office, and evaluation of the regulations for the 24/7 points of contact, EAP II
- 18 – 19 July 2016, Johannesburg, South Africa – Advanced Judicial Training for district magistrates, GLACY
- 18 – 21 July 2016, Johannesburg, South Africa – Conference for the regional/district magistrates (awareness raising on Cybercrime issues), GLACY
- 22 – 23 July 2016, Johannesburg, South Africa – Finalization of judicial training curriculum on cyber and electronic evidence, GLACY
- 27 – 28 July 2016, Rabat, Morocco – International Workshop on Effectiveness of legislation on cybercrime and electronic evidence measured through statistics, GLACY

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