Cybercrime Digest

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

1-15 January 2018

Source: ENISA

Date: 15 Jan 2018

ENISA Threat Landscape Report 2017

"2017 was the year in which incidents in the cyberthreat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence regarding monetization methods, attacks to democracies, cyber-war, transformation of malicious infrastructures and the dynamics within threat agent groups. But 2017 has also brought successful operations against cyber-criminals. Law enforcement, governments and vendors have managed to shut down illegal dark markets, de-anonymize the Darknet and arrest cyber-criminals. […] Moreover, state-sponsored campaigns have been revealed and details of technologies deployed by nation states have been leaked. […] Although 2017 has reached records in security investments, it has also brought new records in cyber-attacks of all kinds." READ MORE

Source: BBC

Date: 12 Jan 2018

Apple health data used in murder trial

"Health data has provided crucial evidence at a trial in Germany, in which a refugee is accused of rape and murder. Apple's Health App accurately records steps and has been pre-installed on the iPhone 6S and newer models. Data suggesting the suspect was climbing stairs could correlate to him dragging his victim down a riverbank and climbing back up, police said. […] The suspect - identified by a hair found at the scene of the crime - refused to provide police with the PIN code to his phone so investigating officers turned to an unnamed cyber-forensics firm in Munich, which broke into the device. The health data app on iPhones records activity - including how many steps are taken, nutrition and sleep patterns as well as various body measurements. As well as locating suspect's movements, the phone also suggested periods of more strenuous activity, including two peaks, which the app put down to him "climbing stairs". An investigator of similar build to the suspect went to the area where the body was found and recreated how the police believe he disposed of the body. The officer's movement data on the same app showed him also "climbing stairs"." READ MORE

Source: Hurriyet Daily News

Date: 27 Dec 2017

Ankara prosecutor demands release of 1,000 FETÖ suspects after Bylock investigation

"The Ankara Public Prosecutor's Office has demanded the release of 1,000 Fethullahist Terrorist Organization (FETÖ) suspects detained for using Bylock, an encrypted smartphone messaging application, after they determined that around 11,000 telephone numbers were directed to the application's server through an online application called Mor Beyin. "We will demand the release of some 1,000 imprisoned people in different cities who were detected as being directed to the ByLock through Mor Beyin, if there isn't any other evidence against them," Yüksel Kocaman, the Ankara Chief Public Prosecutor, said." READ MORE

RELATED ARTICLES

Reuters, Turkey reinstates 1,823 civil servants linked to app used by coup plotters, 12 Jan 2018

Source: Europol

Date: 12 Jan 2018

EU law enforcement joins together with Facebook against online terrorist propaganda

"On 11 January 2018, Europol's Internet Referral Unit organised the eighth joint Referral Action Day with colleagues from the national referral units of Belgium, France and the United Kingdom, to identify and secure the swift removal of terrorist and violent extremism content uploaded on

Facebook and Instagram. The intensive referral campaign was hosted at Europol's headquarters in The Hague and targeted content by terrorist groups and terrorist sympathisers, aiming at radicalising, recruiting and propagating terrorist activities." READ MORE

Source: Reuters

Date: 4 Jan 2018

How a researcher hacked his own computer and found 'worst' chip flaw

"The flaw, now named Meltdown, was revealed on Wednesday and affects most processors manufactured by Intel since 1995. Separately, a second defect called Spectre has been found that also exposes core memory in most computers and mobile devices running on chips made by Intel, Advanced Micro Devices and ARM Holdings, a unit of Japan's Softbank. Both would enable a hacker to access secret passwords or photos from desktops, laptops, cloud servers or smartphones. It's not known whether criminals have been able to carry out such attacks as neither Meltdown nor Spectre leave any traces in log files." READ MORE

RELATED ARTICLES

Bruce Schneier, Spectre and Meltdown Attacks Against Microprocessors, 5 Jan 2018

Source: RTL

Date: 14 Jan 2018

Qu'est-ce que Pharos, la plateforme qui a permis de sauver un jeune suicidaire ?

"Le "17 du web" a permis de sauver la vie d'un jeune homme à Paris, ce dimanche 14 janvier. La Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (Pharos) est entrée en action après le signalement de plusieurs internautes concernant les messages particulièrement inquiétants d'un jeune Parisien sur Twitter. […] Affirmant avoir "perdu foi en l'humanité", il affichait clairement son envie de mettre fin à ses jours. Mais les internautes ont partagé son message en nombre. C'est grâce à cela que la plateforme Pharos, qui est rattachée au pôle cybercriminalité de la police judiciaire, est intervenue pour signaler une urgence vitale à Twitter afin d'obtenir des informations déterminantes dans cette affaire, comme l'adresse IP mais aussi et surtout le nom et l'adresse du jeune homme." READ MORE

Source: Zambia Daily News

Date: 5 Jan 2018

Zambia to deal with fake news decisively

"Authoring, publishing or uttering false information is criminal and should not be tolerated by law enforcement agencies. The Zambia Police Service has a fully-fledged cyber crime unit to deal with social media sycophants. We are a flourishing democracy, but that should not give people the freedom to deliberately abuse social media, hence the need to bring the culprits to book. Like any developing country, we should be using social media to communicate information and share ideas that are beneficial to an individual, as opposed to abusing it." READ MORE

Source: The Irish Times

Date: 12 Jan 2018

Ireland, less than 5% of cybercrime reported to gardaí

"Less than 5 per cent of cyber crime is reported to gardaí, a conference has heard. Speaking at the conference Cyber Fraud in a Digital Age at University College Cork on Friday, Det Supt Mick Gubbins of the Garda Cyber Crime Bureau appealed to company owners and individuals to contact them when they find themselves under attack by criminals. […] Det Supt Gubbins said one third of Irish and Northern Irish businesses have suffered a data security breach in the past year. He says companies do not approach gardaí to report attacks on their systems, which prevents the authorities from sharing their experiences with the wider community." READ MORE

Source: The Daily Star

Date: 11 Jan 2018

Transparency International Bangladesh for guidelines of specialised police unit to check cybercrime

"Transparency International Bangladesh (TIB) today called for formulating a guideline before a specialised police unit launches its operation to combat cyber crimes. Experts and stakeholders should be included into the formulation process of the guideline, the TIB said in a press statement. […] TIB Executive Director Dr Iftekharuzzaman said they have learnt from media that the government has taken initiative to form a specialised police unit, which will be equipped with modern software, to mine any remarks or postings in social media that are defamatory, offensive and can hurt religious sentiment. […] "There is a risk of violation of people's freedom of speech and expression, as guaranteed by the constitution, if the law enforcers, who will get involved in such surveillance, lacks of skill, honesty, professionalism and impartiality". Especially, such surveillance can be risky and suicidal if the unit fails to discharge duties going out from political and administrative influence and also from irregularities and corruption, he added." READ MORE

Source: Inquirer

Date: 6 Jan 2018

Cybercrime top threat to Philippines banks in 2018

"Cybersecurity is one of the biggest threats that the Philippine banking system must confront this year as malicious hackers from here and overseas become more aggressive and attacks become more damaging, the Bangko Sentral ng Pilipinas said. To address this, local banks must allocate more resources to boost not only their technical capabilities, but also to ensure that they have the right technical people who can secure internal systems and reassure clients who are increasingly sensitive about the security of their transactions." READ MORE

Source: FTN

Date: 10 Jan 2018

Visitors to Dubai can be jailed under cybercrime laws

"[…] The laws applied against Yaseen could just as readily be applied against someone who leaves a negative review online of a restaurant or shop or any other business. It is essentially illegal to express criticism or dissatisfaction with a person or company in Dubai, as this could be subjectively construed as an insult, and typically, an accused person will have little or no opportunity to defend themselves or even explain why the criticism was made. Comments may be misunderstood or misinterpreted and there is a growing culture of using the police to report things that would largely be ignored in other countries. In fact, the UAE cybercrime laws can be applied to someone retroactively and extraterritorially; in other words, someone can be prosecuted in Dubai for something they said online years ago and in another country." READ MORE

Source: Huffpost Maroc

Date: 6 Jan 2018

Le "Blue Whale Challenge" aurait fait ses premières victimes au Maroc

"Le jeu de la baleine bleue, ou "Blue Whale Challenge", a encore frappé. Cette fois-ci, c'est au Maroc qu'il aurait fait ses premières victimes. Un lycéen adepte de ce jeu viral a mis fin à sa vie en se jetant d'un l'immeuble où il résidait à Agadir, comme l'a rapporté ce jeudi la presse locale. L'ultime défi de ce jeu morbide? Le suicide. L'adolescent, qui devait passer son baccalauréat cette année, était connu pour être introverti, poursuit la presse locale. D'après sa famille, le jeune garçon jouait beaucoup aux jeux vidéos et était devenu accro au "Blue Whale Challenge"." READ MORE

Source: Algérie Press Service

Date: 14 Jan 2018

Algérie, un plan d'action pour lutter efficacement contre la cybercriminalité

"Le Directeur général de la Sûreté nationale, le Général major Abdelghani Hamel a fait état, dimanche à Alger, d'un plan d'action complémentaire visant à doter les personnels de la Sûreté de moyens technologiques innovants pour lutter efficacement contre toute forme de

cybercriminalité en vue de "garantir un espace électronique sécurisé pour tous. […] Dans ce contexte, le Général major Hamel a souligné que "la recrudescence des crimes cybernétiques -qui ne se limitent pas seulement à attaquer les individus et leurs biens mais également les systèmes informatiques- a amené le secteur de la Sûreté nationale à créer un service spécialisé dans la lutte et la prévention contre ces crimes et à approuver des programmes de sensibilisation avec les partenaires concernés et la société civile pour hisser le niveau de conscience quant aux dangers de l'Internet, particulièrement chez les mineurs." READ MORE

Source: The Middle East Media Research Institute

Date: 2 Jan 2018

Jordanian Journalists, Politicians Receive Death Threats On Social Media

"In September 2017, death threats appeared on social media against two liberal Jordanian journalists: Zuleikha Abu Risha and Basel Rafayeh, as well as against a parliament member from the Muslim Brotherhood, Dima Tahboub. These threats prompted a renewed debate about a phenomenon that has become prevalent in Jordan in the last few years, namely the use of social media as an arena for mutual sparring and mudslinging between liberal and Islamist circles, and also gave rise to renewed complaints about the authorities' failure to address the danger of incitement on social media. […] In September 2017 the Legislation and Opinion Bureau at the Prime Minister's Office drafted an amendment to the cybercrime law which, for the first time, criminalizes the spreading of online hate speech and penalizes offenders." READ MORE

Source: Europol

Date: 12 Jan 2018

Law enforcement and private sector join forces to shut down illegal Streaming Network

"On 11 January 2018, a crime group suspected of hosting a large-scale illegal IPTV streaming business has been dismantled. […] The network is accused of illicitly distributing Greek, Cypriot and foreign pay TV subscriber channels, using several servers to facilitate illegal signal dissemination via subscription channels. These services were allegedly offered through retailers throughout Europe and sold as a monthly illegal subscription for as little as 20 Euros." READ MORE

Source: ETH News

Date: 10 Jan 2018

South Korea Asks For Global Participation In Cryptocurrency Regulation

"On January 8, 2018, vice chairman of the South Korean Financial Services Commission, Kim Yong-bum, appeared before the Steering Committee of the Financial Stability Board (FSB), an international body that monitors and makes recommendations about the global financial system, convened in Basel, Switzerland. […] Kim recommended that the FSB take measures to investigate cryptocurrency and assess cautionary factors. He said, "It is necessary [for the FSB] to speedily study the potential risks of virtual currency in financial stability ... we must support virtual currency countermeasures by integrating and sharing relevant information such as the contents and effects of the virtual currency regulation of each country." READ MORE

Source: The Merkle

Date: 7 Jan 2018

Technique to Analyze Bitcoin Transactions Unveiled

"Even though Bitcoin is not suited for criminal activity, a lot of people still use it to hide their tracks. As a result, we are seeing more and more companies focus their attention on analyzing patterns associated with Bitcoin transactions and the blockchain. Bitfury Group, one of the largest Bitcoin transaction processors in the world today […], has been working on a new solution to analyze related Bitcoin addresses. Because everyone can publicly track all Bitcoin transactions in real time without any software, it's easy to find connections between specific addresses. At the same time, it can be quite cumbersome to follow the trail of digital breadcrumbs, especially when funds move through exchanges, mixers, and other conversion solutions." READ MORE

Latest reports

- ICANN, Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion, 13 Jan 2018
- ENACT Project, Africa's changing place in the global criminal economy, 9 Jan 2018
- CircleID, Internet Governance Outlook 2018: Preparing for Cyberwar or Promoting Cyber Détente?, 6 Jan 2018
- Diplo Foundation, A tipping point for the Internet: 10 predictions for 2018, 11 Jan 2018
- World Economic Forum, Cyber Resilience: Playbook for Public- Private Collaboration, 12 Jan 2018

Upcoming events

- 15-18 January, Sarajevo, Bosnia and Herzegovina – Case simulation exercise on cybercrime and financial investigations, iPROCEEDS
- 16-18 January, Kampala, Uganda – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 22-24 January, Port Louis, Mauritius – Advisory mission on harmonization of legislation on cybercrime and electronic evidence, GLACY+
- 25-26 January, Port Louis, Mauritius – Advice on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence, GLACY+
- 29 January-2 February, Nuku'alofa, Tonga – ECTEG Course on Open-Source Forensic and Mobile Forensic, 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