# Cybercrime Digest

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

1-15 February 2017

*Source: Prensa Libre*

*Date: 13 Feb 2017*

## Gobernación elabora ley para combatir el cibercrimen en Guatemala

"El viceministro de Gobernación Walter Girón, explicó que el borrador de esta normativa será elaborada en los próximos tres días en la denominada Misión Consultiva de Legislación sobre Delitos Cibernéticos y Pruebas Electrónicas. El Ministerio de Gobernación creará una iniciativa de ley sobre los ciberdelitos. "En tres días se creará un marco legal para después someterla al conocimiento, estudio, análisis y posterior aprobación de la ley y sus reglamentos por parte del Congreso de la República", indicó el funcionario. Agregó que la iniciativa se tiene que regir a las normas internacionales para perseguir el cibercrimen. Según Girón, en Guatemala hasta ahora no está tipificado el delito informático o cibernético, por lo que las instituciones encargadas de investigar no tienen las herramientas y esos delitos quedan impunes." READ MORE

RELATED ARTICLES

Ministerio de Gobernacion de Guatemala, Crearán borrador para propuesta de ley para el combate al Cibercrimen, 13 February 2017

---

*Source: ENISA*

*Date: 8 Feb 2017*

## ENISA Threat Landscape 2016 report: cyber-threats becoming top priority

"This year is characterised by numerous serious cyber-incidents which have dominated the news. Main objectives of malicious activities detected was monetization and political impact. ETL 2016 is streamlined towards the top cyber-threats, providing information on threat agents and attack vectors including all the remarkable developments, trends and issues. Moreover, it reports about threat agents their motivations, and how their practices, tools and techniques have advanced. Though the defenders have made significant progress in disrupting cyber-threats and in the attribution of incidents, adversaries continue to advance their tactics and techniques." READ MORE

---

*Source: NATO CCD-COE*

*Date: 9 Feb 2017*

## International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms

"The new Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations reaffirms that cyber operations do not occur in a legal vacuum. The influential handbook is published by Cambridge University Press and authored by an international group of experts. The NATO Cooperative Cyber Defence Centre of Excellence facilitated the drafting process. Tallinn Manual 2.0, as well as state practice, affirms that international law applies to cyber space, emphasizes Liis Vihul, managing editor of the Tallinn Manual 2.0. "Cyber operations do not occur in a legal vacuum and states both have rights and bear obligations in cyber space. Norms, including those predating the cyber-era, apply to cyber operations, both conducted by and directed against states. The Manual draws on international law ranging from sovereignty and state responsibility to human rights and space law." READ MORE

---

*Source: United Nations*

*Date: 13 Feb 2017*

## UN Security Council calls on member states to address threats against critical infrastructure, unanimously adopting resolution 2341 (2017)

"The Security Council today called upon Member States to address the danger of terrorist attacks against critical infrastructure, adopting a related resolution before holding a day-long open debate on that subject. Unanimously adopting resolution 2341 (2017), the Council encouraged all States to make concerted and coordinated efforts — including through international cooperation — to raise awareness and expand knowledge of challenges posed by terrorist attacks, so as to be better prepared for such attacks. […] Sven Mikser, Minister for Foreign Affairs of Estonia, underlined the importance of the Convention on Cybercrime, the only binding international instrument of its kind, and called on all countries to adopt policies that fostered an open, resilient cyberspace." READ MORE

RELATED ARTICLES

Permanent Mission of Estonia to the UN, Remarks by Minister for Foreign Affairs of Estonia H.E. Mr Sven Mikser at UN Security Council open debate on 13 February 2017, 13 February 2017

*Source: NextGov*

*Date: 6 Feb 2017*

## New international cyber rules likely off the table for UN Experts Group

"A United Nations cybersecurity experts group meeting this month in Geneva should focus on encouraging UN member states to adopt existing cyber rules of the road and confidence-building measures rather than developing new ones, the U.S. delegate said Monday. […] "We don't need a continual norms machine ramping out a lot of norms," State Department Deputy Coordinator for Cyber Issues Michele Markoff told an audience at the Carnegie Endowment for International Peace. "What we need to do is consolidate what we've done and get states to implement," she said, "both in the internalization of the norms but also in the operationalization of [confidence-building measures] which will help the norms." Confidence-building measures include nations sharing information about transnational cyber threats and about national cybersecurity strategies." READ MORE

*Source: BBC*

*Date: 14 Feb 2017*

## Queen to open today the new National Cyber Security Centre in UK

"A new centre to protect the UK against cyber-attacks is to be officially opened by the Queen later. The National Cyber Security Centre (NCSC) in London is designed to improve Britain's resilience to attacks and act as an operational nerve centre. "We want to make the UK the hardest target," Ciaran Martin, the centre's chief executive, told the BBC. The NCSC - part of intelligence agency GCHQ - says the UK is facing about 60 serious cyber-attacks a month. There were 188 attacks classed by the NCSC as Category Two or Three during the last three months. And even though the UK has not experienced a Category One attack - the highest level, e.g. the theft of confidential details of millions of Americans from the Office of Personnel Management - there is no air of complacency at the NCSC's new headquarters in Victoria." READ MORE

*Source: Europol*

*Date: 14 Feb 2017*

## Victims of child sexual abuse at the centre of Europol efforts

"Europol's European Cybercrime Centre has successfully supported efforts to identify several victims of child sexual abuse through its third Victim Identification Task Force (VIDTF). The VIDTF 3 hosted at Europol headquarters from 28 January to 10 February saw experts from around the world identifying victims of child sexual abuse and exploitation using advanced techniques, software and their knowledge and expertise. As a result, victims of this damaging crime have been located living in several countries in the EU and beyond. Law enforcement authorities in those countries are currently working to finalise the identification of the children and save them from further atrocities." READ MORE

*Source: The Philippine Star*

*Date: 14 Feb 2017*

## U.S. – Philippines cooperation against sex cyber crimes

"Joint efforts of the US Homeland Security Investigations and the National Bureau of Investigation as well as the Departments of Justice and Social Welfare and Development resulted in the successful conviction of an American who was sexually exploiting Filipino children. The 54-year-old pedophile – who was given a 50-year prison term – used Facebook to convince a 14-year-old girl to produce sexually explicit images that included sadism and masochism and send them through the internet." READ MORE

*Source: HackRead*

*Date: 6 Feb 2017*

## Anonymous shut down thousands of Dark Web sites for hosting child porn

"The Anonymous-affiliated hacker group has managed to take down the Freedom Hosting II servers affecting more than 10,000 websites. It must be noted that Freedom Hosting II is regarded as one of the largest hosting services on the Dark Web with hosting rights of around 20% of all the sites on this underground platform. According to researcher Sarah J Lewis, the websites bear the domain .onion and therefore, can be accessed through Tor browser. The stolen information includes email IDs of more than 380,000 users." READ MORE

RELATED ARTICLES

DeepDotWeb, Anonymous Hacks Freedom Hosting II, Bringing Down Almost 20% of Active Darknet Sites, 9 February 2017

*Source: News18*

*Date: 1 Feb 2017*

## India, CERT-Fin proposed to check cyber frauds

"Amid government's push on digital transactions, Finance Minister Arun Jaitley on Wednesday announced setting up of a Computer Emergency Response Team to strengthen security of the financial sector amid increasing incidents of cyber frauds. "Cyber security is critical for safeguarding the integrity and stability of our financial sector. A Computer Emergency Response Team for Financial Sector (CERT-Fin) will be established," Jaitley said in his Budget Speech in the Lok Sabha on Wednesday. The entity, Jaitley said, will work in close coordination with all financial sector regulators and other stakeholders." READ MORE

*Source: ALnavío*

*Date: 8 Feb 2017*

## Los ciberdelincuentes tienen un blanco fácil en toda América Latina

"Nada es un crimen, tampoco en el mundo cibernético, a menos que esté definido por la ley. Es la máxima de Alexander Seger, director de la división de cibercrimen del Consejo de Europa, y que también participó en el Informe de Ciberseguridad 2016. […] Además, este experto constata que las medidas de seguridad cibernética y la justicia penal contra la ciberdelincuencia son complementarias. Igualmente insiste en la importancia de formar parte del Convenio de Budapest, un acuerdo internacional para la prevención de ciberdelitos: "Este Convenio sirve a los países de América Latina como guía para la preparación de la legislación interna". En este contexto, Seger define como un desafío particular en América Latina la lentitud a la hora de adoptar reformas legislativas. […] República Dominicana y Panamá ya son miembros de este tratado. Argentina, Chile, Colombia, Costa Rica, México, Paraguay y Perú tienen su invitación para adherirse." READ MORE

*Source: ArsTechnica*

*Date: 8 Feb 2017*

## A rash of invisible, fileless malware is infecting banks around the globe

"Fileless malware is going mainstream, as financially motivated criminal hackers mimic their nation-sponsored counterparts. According to research Kaspersky Lab plans to publish Wednesday, networks belonging to at least 140 banks and other enterprises have been infected by malware that relies on the same in-memory design to remain nearly invisible. Because infections are so hard to spot, the actual number is likely much higher." READ MORE

*Source: Technology Decisions*

*Date: 7 Feb 2017*

## Australian Cybercrime Online Reporting Network (ACORN) receives more than 45,500 reports in 2016

"With more than 45,500 cybercrime reports during 2016, the Australian Cybercrime Online Reporting Network (ACORN) is continuing its crackdown. The leading types of cybercrime being reported to the ACORN are online fraud and scams. Scammers are known to set up sophisticated websites designed to trick consumers into thinking they are legitimate businesses, often using a '.com.au' domain name and stolen Australian Business Number (ABN). Online trading issues which affect Australians who buy and sell goods online were the second-highest type of cybercrime reported, with ACORN receiving 8783 reports in 2016." READ MORE

*Source: Journal de Brazza*

*Date: 3 Feb 2017*

## Lutte contre la cybercriminalité au Congo

"Lancement d'une campagne sur la responsabilité et citoyenneté. Le ministre congolais des Postes et télécommunications Léon Juste IBOMBO, a procédé, ce jeudi 2 février 2017, à Brazzaville, au lancement de la campagne nationale de lutte contre la mauvaise utilisation des réseaux sociaux. «Soyons responsables et citoyens dans l'utilisation des réseaux sociaux» est contenu de cette campagne lancée par le ministre Léon Juste Ibombo, et destinée aux internautes. Cette campagne sous forme d'invite à la responsabilité et à la citoyenneté n'est pas une manière de reteindre la liberté de communiquer et d'utiliser les réseaux. Elle est, plutôt, une interpellation au respect de l'éthique et de la morale dans l'usage de l'internet." READ MORE

*Source: Punch*

*Date: 6 Feb 2017*

## 13.58 mln Nigerian Internet users suffer cyberattacks

"About 13.58 million of the 97 million Internet users in the country suffer cyberattacks annually, the Director-General, National Information Technology Development Agency, Dr. Isa Ibrahim, has said. Ibrahim said this at the inaugural meeting of the Inter-ministerial Technical Committee on the Implementation of the National Cyber Security Strategy […]. Ibrahim said such a high number of attacks was part of the reasons that informed the establishment of the technical committee, which has the mandate to design the strategy for the country to be safe in the cyberspace." READ MORE

*Source: Jamaica Information Service*

*Date: 12 Feb 2017*

## Government to Curtail Cybercrimes in Jamaica

"The Government remains committed to the ongoing implementation of safeguards to curtail the incidence of cybercrimes. These, according to Science, Energy and Technology Minister, Dr. the Hon. Andrew Wheatley, include amendments to Cybercrimes Act, where necessary. […] Dr. Wheatley said the Ministry was monitoring the technology sector keenly to keep abreast of developments, which could potentially threaten the stability of the industry's operations. He indicated that support in this endeavour was being provided by several stakeholders, including the Jamaica Bankers Association and the police who, he said, have been proactive in introducing preventative measures." READ MORE

*Source: The Jakarta Post*

*Date: 11 Feb 2017*

## New cyber agency to be established soon in Indonesia

"Indonesia will soon see the establishment of its long-planned National Cyber Agency. The country is only waiting for President Joko "Jokowi" Widodo to issue a presidential decree that will set the operation of the body, which is assigned to tackle cyber crimes in the country, in motion […]. First Marshall Sigit Priyono, the assistant deputy 2/VII for the coordination of telecommunications and information at the Office of the Coordinating Political, Legal and Security Affairs Minister, said the process to establish the body was already complete, including the synchronization of regulations and coordination among cyber divisions within the government." READ MORE

*Source: El Siete*

*Date: 11 Feb 2017*

## Internet en México ocupa penúltimo lugar mundial en seguridad

"En México, 65 millones de personas usan diariamente el internet, es decir 7 de cada 10 ciudadanos, según la Asociación Mexicana de Internet (Ampici). […] Precisamente según un estudio, el 54 por ciento de los usuarios temen al contacto no deseado a través de redes sociales, correo electrónico u otros medios. En segundo lugar, se encuentran las peticiones y extorsiones de carácter sexual, y México ocupa la posición número 13 -de 14 países encuestados- con respecto a la percepción de inseguridad al navegar." READ MORE

*Source: European Aviation Safety Agency*

*Date: 14 Feb 2017*

## EASA cooperate with CERT-EU on cybersecurity

"The European Aviation Safety Agency (EASA) signed on 10 February 2017 a Memorandum of Cooperation with the CERT-EU of the EU Institutions. […] EASA and CERT-EU will cooperate in the establishment of a European Centre for Cyber Security in Aviation (ECCSA)." READ MORE

*Source: PC Tech*

*Date: 10 Feb 2017*

## Uganda, Malawi Partner to Boost e-Government, Cyber Security Capacity

"The Government of Uganda has on Friday morning signed a memorandum of understanding with the government of Malawi aimed at boosting cyber security capacity and electronic government of the two nations." READ MORE

# Latest reports

- ENISA, Updated Training Materials for Cyber Security Specialists, February 2017
- ENISA, Analysis of security measures deployed by e-communication providers, 9 February 2017
- Deloitte, 2017 Nigeria Cybersecurity Outlook, 6 February 2017
- Laura Jaitman, The Costs of Crime and Violence in Latin America and the Caribbean, February 2017
- The Citizen Lab, Nile Phish: Phishing Campaign Targeting Egyptian Civil Society, 2 February 2017
- Privacy International, Understanding surveillance in Thailand, January 2017
- Kaspersky, A look into the Russian-speaking ransomware ecosystem, 14 February 2017
- Cisco, 2017 Annual Cybersecurity Report, 1 February 2017

# Upcoming events

- 16–17 February, Sarajevo, Bosnia and Herzegovina – Advice and workshop on the preparation of interagency cooperation protocols and on domestic protocols for international sharing of intelligence and evidence, iPROCEEDS
- 16–17 February, Tbilisi, Georgia – Roundtable on reform of cybercrime laws and regulations, EAP III
- 20–21 February, Skopje, "The former Yugoslav Republic of Macedonia" – Advisory mission and workshop for the setting up or improvement of reporting mechanisms, iPROCEEDS
- 23-24 February, Tbilisi, Georgia – Development of cyber exercise scenarios in cooperation with the Georgian Data Exchange Agency, EAP III
- 27 February – 1 March, Singapore – INTERPOL - Workshop on 24/7 Points of Contact; Joint training for prosecution, central authorities and cybercrime units on obtaining electronic evidence from foreign jurisdictions and MLA issues; Workshops on cooperation with service providers, GLACY+ / EAP II
- 27 February – 3 March, Bucharest, Romania – Regional training for cybercrime units, economic crime units, financial investigators and specialised prosecutors on virtual currencies and the dark web (EMPACT), iPROCEEDS