Cybercrime Digest

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

1-15 May 2016

Source: The Telegraph

Date: 11 May 2016

iPhone seized from alleged terrorists suspected of planning attacks on London cannot be opened, Italian police say

"Key information about an alleged Islamist terrorist plot to strike targets in London could be contained in an iPhone seized from suspects arrested in Italy, but police are unable to access the device" READ MORE

Source: HackRead

Date: 8 May 2016

After Bank of Greece, OpIcarus Finds More Targets as Banks in Panama, Bosnia and Kenya Go Offline

"It's been over a week since Anonymous and Ghost Squad began conducting cyber attacks on banking websites worldwide. It's the weekend now but the hacktivists aren't taking a break; while you were sleeping they conducted distributed denial-of-service DDoS attacks on the websites of four International banks including the central bank of Kenya, National Bank of Panama, Central Bank of Bosnia and Herzegovina and Maldives Monetary Authority. […] Though most of the sites are back online, the Central Bank of Bosnia and Herzegovina is still offline since yesterday." READ MORE

RELATED ARTICLES

Anonymous attacks Greek Central Bank and vows to take down more banks' sites, CNN Money, 4 May 2016

After Bank of Greece, Cyprus Central Bank also reports cyber attack, Reuters, 6 May 2016

OpIcarus continues as hacktivists shut down 3 more banking websites, HackRead, 6 May 2016

Source: Sophos

Date: 28 April 2016

The flaw that left .AS (American Samoa) websites and owners exposed for at least 16 years

"A security researcher by the name of Infosec Guy has discovered a flaw in the website of the AS (American Samoa) domain registry nic.as that, in the registry's own words, "pre-dates the century". According to Infosec Guy the flaw allowed anyone to modify the records of any domain name accessible through the AS Registry website, giving them an easy way to hijack .as websites. The .as domain is the country code top-level domain for the US territory of American Samoa. As well as being used by sites associated with the territory, the .AS domain is used by organisations wanting to create short and memorable domains, such as the University of Texas (utex.as) and by URL shortening services." READ MORE

RELATED ARTICLE

Flaw allowed anyone to modify & take control over any .AS domain, Infosec Guy, 25 April 2016

Source: Cyber Parse

Date: 6 May 2016

The massive password breach that wasn't: Google says data is 98% "bogus"

"Earlier this week, mass panic ensued when a security firm reported the recovery of a whopping 272 million account credentials belonging to users of Gmail, Microsoft, Yahoo, and a variety of overseas services. […] Since then, both Google and a Russia-based e-mail service unveiled analyses that call into question the validity of the security firm's entire report. "More than 98% of the Google account credentials in this research turned out to be bogus," a Google representative wrote in an e-mail. […] Separately, Mail.ru, Russia's biggest e-mail provider, has said that more than 99.98 percent of the credentials it received from security firm Hold Security turned out to be invalid accounts." READ MORE

RELATED ARTICLE

Big data breaches found at major email services, Reuters, 4 May 2016

Source: UnderNews

Date: 4 May 2016

Un ransomware paralyse une centrale hydro-électrique

"La menace ransomware est devenue omniprésente et est redoutable. Aux USA, l'un d'eux a paralysé une centrale hydro-électrique après avoir infecté et bloquer les systèmes informatiques internes. C'est le premier cas d'un ransomware bloquant une centrale. Jusqu'à maintenant, le plus grave cas était la paralysie d'un hôpital. Mais il faut bien garder en tête que tout ce qui est connecté à Internet est une cible potentielle, sans aucune exception!" READ MORE

Source: International Business Times

Date: 6 May 2016

Passwords and sexual preferences of 40 million users up for sale on dark web

"Tens of millions of credentials reportedly stolen from an adult dating website called Fling.com have been put up for sale on the dark web. Currently listed on an underground marketplace called The Real Deal the information reportedly contains email addresses, plain text passwords, usernames, IP addresses and date of birth records. Additionally, the compromised data includes sexual preferences, whether the account was a free or paid version and the gender of the user. The hacker responsible for selling the credentials, using the pseudonym 'peace_of_mind' claims the data dump contains over 40 million records. It is currently on sale for 0.8874 bitcoins which is equivalent to approximately £280 based on the exchange rate at the time of writing." READ MORE

Source: HackRead

Date: 28 April 2016

Anonymous Leaks 1TB of Data from Kenya's Ministry of Foreign Affairs

"Anonymous has conducted a sophisticated cyber attack on the government of Kenya by breaching its Foreign ministry server, stealing a trove of data and ending up leaking some of it on the Dark Web. The cyber attack was conducted under the banner of operation OpAfrica which was launched last year against child abuse, child labour and corruption in the African countries." READ MORE

Source: The Diplomat

Date: 27 April 2016

The Trouble with Pakistan's Cybercrimes Bills

"[…] The passage of the Prevention of Electronics Crimes Bill 2015 by the National Assembly is a good endeavor of the government as the legislation on cybercrimes was badly needed. The cyber space in Pakistan is greatly used for spreading hate material, extremist ideologies, anti-state ideas and also other cyber related crimes like hacking and sharing of sensitive information. There was a dire need for a regulation." READ MORE

Source: Bangkok Post

Date: 7 May 2016

Cambodian Prime Minister's website hacked

"Cambodian Prime Minister Hun Sen said Saturday his official website was hacked in the morning, with some photos and sound clips being altered. In a posting on his Facebook page, Hun Sen said his website was hacked at 4.12am and that his online reputation had suffered as a result of the attack." READ MORE

Source: The Coin Telegraph

Date: 4 May 2016

British Commonwealth Adopts Blockchain to Fight Cross-Border Crime

"The British Commonwealth announced on 3rd May that there is a project to develop a Blockchain app to combat cross-border crime. A secure messaging system will be created to help law enforcement and prosecutors in member countries to co-operate more effectively in criminal investigations." READ MORE

Source: Juniper Research

Date: 3 May 2016

Online Transaction Fraud to more than double to $25bn by 2020

"A new study from Juniper Research has found that the value of online fraudulent transactions is expected to reach $25.6 billion by 2020, up from $10.7 billion last year. This means that by the end of the decade, $4 in every $1,000 of online payments will be fraudulent." READ MORE

Source: Security Intelligence

Date: 11 May 2016

It All Comes Out in the Wash: The Most Popular Money Laundering Methods in Cybercrime

"There are many ways in which a criminal can illegally acquire money electronically. […] In traditional money laundering schemes, the placement of funds begins when dirty money is put into a financial institution. When funds are stolen online through digital transactions at financial institutions, the process immediately jumps to layering." READ MORE

Source: Council of Europe

Date: 09 May 2016

Israel joins Budapest Convention

"Israel deposited today the instrument of accession to the Budapest Convention on Cybercrime. This will increase the number of Parties to 49." READ MORE

Source: Council of Europe

Date: 11 May 2016

GLACY: Improving international cooperation on cybercrime and electronic evidence in West Africa

"The workshop "Improving international cooperation on cybercrime and electronic evidence in West Africa" aims to provide a set of regional and country-specific recommendations with regard to regional and international cooperation on cybercrime and electronic evidence." READ MORE

Latest reports

- Council of Europe/Cybercrime Convention Committee, Criminal Justice Access to Evidence in the Cloud: Cooperation with "Foreign Providers" , April 2016
- République de Côte D'ivoire – Ministere d'Etat Ministere de l'Interieur et de la Securite – Direction Generale De La Police Nationale, Lutte contre la cybercriminalité – Défis des polices en Afrique, 5 May 2016
- Kaspersky, IT Threats evolution in Q1 2016, May 2016
- Microsoft, Security Intelligence Report, Volume 20 | July through December, 2015, (Key Findings, Regional Threat Assessment), May 2016

Upcoming events

- 16 – 18 May, 2016, Chisinau, Moldova – Country assessment visit on Public/Private Cooperation, EAP III Project
- 19 – 20 May, 2016, Pristina, Kosovo1– Country visit for meeting the relevant stakeholders and collecting the necessary information for the situation report, iPROCEEDS Project
- 23 May – Strasbourg, France, T-CY Hearing with data protection community
- 24 – 25 May – Strasbourg, France, Cybercrime Convention Committee (T-CY) 15th Plenary
- 26 May – Strasbourg, France, GLACY Steering Committee Meeting
- 30 May – 1 June - Manila, Philippines, Study visit of Sri Lankan CERT and police/forensics experts on benchmarking digital forensics services and standard operating procedures, GLACY Project
- 30 May – 1 June - Manila, Philippines, Support to national delivery of introductory judicial course, GLACY Project
- 31 May – Dakar, Senegal, In-country workshop on law enforcement training strategies, GLACY Project
- 30 – 31 May – Rabat/Casablanca, Morocco: Advisory mission on cybercrime reporting systems, interagency cooperation and public-private cooperation, GLACY Project

[1] This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence