

CYBERCRIME

RECENT DEVELOPMENTS

BANGKOK, 23.03.2015

PROF DR MARCO GERCKE

CYBERCRIME – NOT A NEW PHENOMENON

DEVELOPMENT OF NEW TECHNOLOGIES

LED TO NEW TYPE OF CRIMES

1960TH

Picture removed
in print version

1970TH

Picture removed
in print version

1980TH

Picture removed
in print version

1990TH

Picture removed
in print version

The Wi-Fi sniffing drones are here

By [Russell Brandom](#) on February 23, 2015 06:18 pm



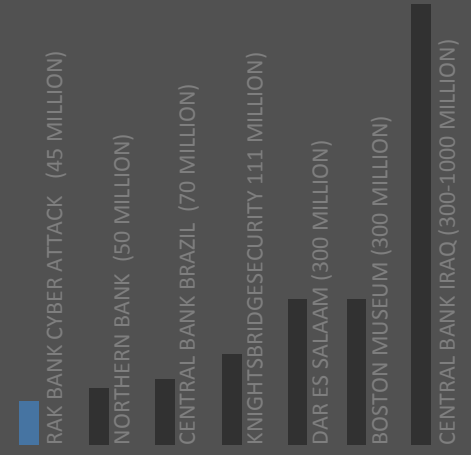
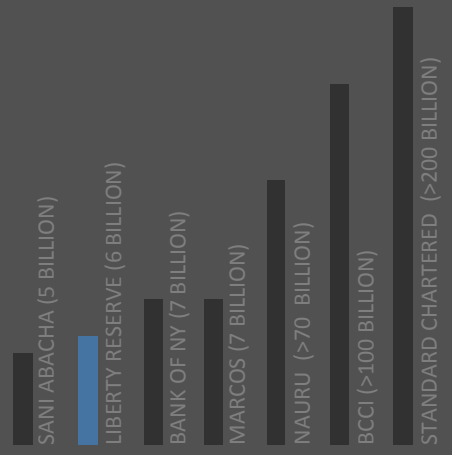
SOURCE: THE VERGE

DEVELOPMENT

NEW DEVELOPMENTS

DEVELOPMENT

LOSSES ARE INCREASING



ATTACKS/BREACHES

2/16/2015
09:30 PMKelly Jackson
Higgins
News

Connect Directly



1 COMMENT

Cybercriminals Target Bank Employees, Steal \$1 Billion From Financial Institutions Worldwide

'Carbanak' includes operatives from Russia, Ukraine, China, and other parts of Europe.

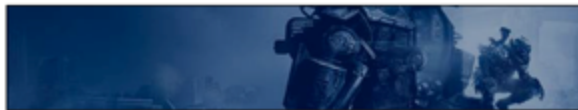
KASPERSKY SECURITY ANALYST SUMMIT -- Cancun, Mexico -- An international cybercrime ring based out of Eastern Europe has pilfered some \$1 billion in two years from 100 different banks in nearly 30 countries using spearphishing emails targeting bank employees.

Russian financial institutions so far have been hardest hit, followed by Denmark and the US, by the so-called Carbanak cybercrime gang that includes operatives from Russia, Ukraine, China, and other parts of Europe.

SOURCE: DARK READING

DEVELOPMENT

LOSSES ARE INCREASING



A CNBC SPECIAL REPORT

5 billion Android apps open to hack

Arjun Kharpal | @ArjunKharpal
Friday, 27 Feb 2015 | 8:58 AM ET



Over five billion downloaded Android apps are vulnerable to being hacked, cybersecurity researchers have found, as attackers exploit flaws in Google's operating system.

Some 96 percent of malware -- or malicious software -- employed by hackers target **Google** Android, according to U.S. firm FireEye, which analysed more than 7 million mobile apps on Android and Apple iOS between January and October 2014.

Apps designed to steal financial data were especially popular, the researchers found. The open-source nature of Android allows hackers to find the code behind a popular app, they said, and recreate the app almost identically but with a malicious code to infect users.

Business spotlight on cybercrime

In the wake of the Sony email hacking case, business expert Rachel Bridge looks at cybercrime and how you can protect your business

 0  527  0  67  594  Email



SOURCE: THE TELEGRAPH

DEVELOPMENT

FOCUS ON END USERS AS WELL AS BUSINESSES

MISLEADING INFORMATION

The screenshot shows a webpage from examiner.com with a navigation bar (ABE, News, Life, Leisure) and a breadcrumb trail (Tech > Gadgets & Tech > Tech Gear). The main headline reads "15 percent of the world's Internet traffic was hijacked to China, in April" with social media share icons. Below the headline, there are social sharing buttons (Facebook, Twitter, Email, etc.), a date (November 16, 2010), and a "Follow me on Twitter" link. The article text begins with "It's been said the next major war may not take place on a physical battlefield, but on the Internet. We've already seen instances of cyber warfare. How would you feel if you knew that for 18 minutes a country hijacked 15 percent of the world's Internet traffic? Not too safe, probably." A small image of a server room is visible on the left side of the article.

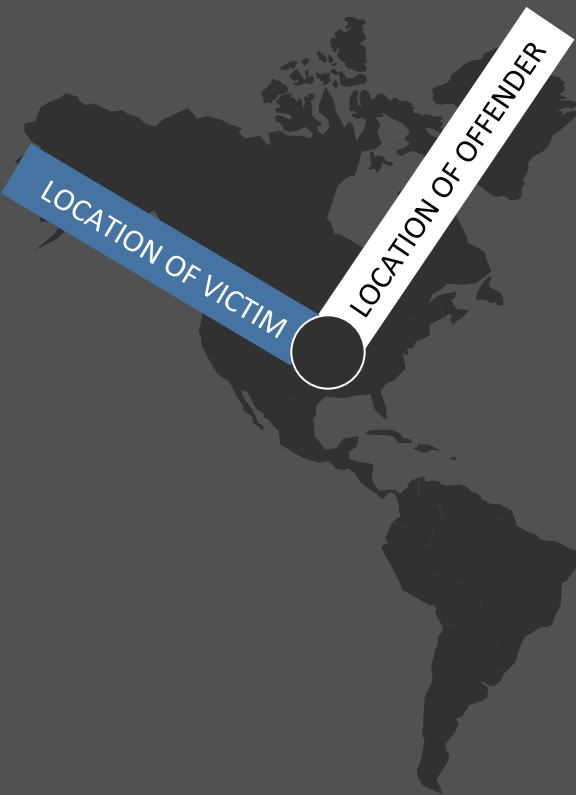
SOURCE: EXAMINER.COM

244

For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers.* Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from U.S. government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.¹¹⁶

Although the Commission has no way to determine what, if anything, Chinese telecommunications firms did to the hijacked data, incidents of this nature could have a number of serious implications. This level of access could enable surveillance of specific users or sites † It could disrupt a data transaction and prevent a user

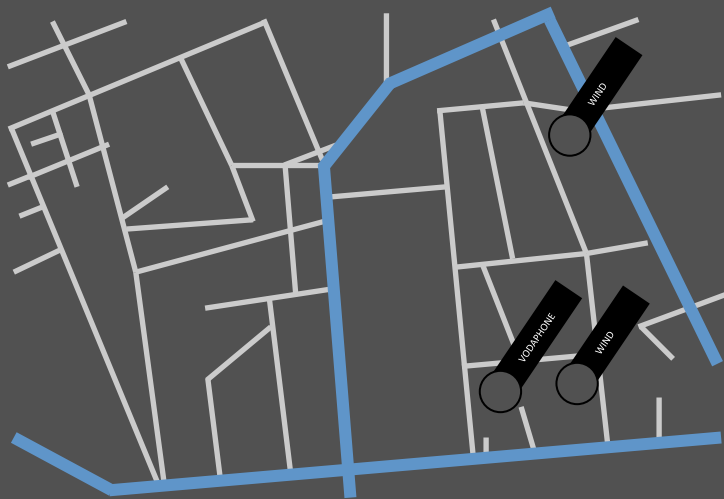
MURDER



CYBERCRIME



ADVANCED INVESTIGATIONS



EDITION: INTERNATIONAL | U.S. | MEXICO | ARABIC
Set edition preference

CNN

Home Video World U.S. Africa Asia Europe Latin America Middle East Business

CNN Travel
THE NEW ONLINE DESTINATION

Italy convicts 'U.S. agents' in CIA kidnap trial

November 4, 2009 -- Updated 21:26 GMT (05:26 HKT)

ROME, Italy (CNN) -- Nearly two dozen Americans -- most thought to work for the CIA -- were sentenced to five years in prison Wednesday by an Italian court for their role in the seizing of a suspected terrorist in Italy in 2003, the prosecutor in the case told CNN.

The Americans did not appear for trial and are not in custody, but the ruling could effectively make them international fugitives.

Italian prosecutor Armando Spataro speaks Wednesday in the court in Milan at the end of the trial.

SOURCE: CNN

CHALLENGES

PROTECTING INDIVIDUAL FREEDOMS

COURT ORDERS

LIMITATIONS OF INVESTIGATIONS

LIMITATION OF CRIMINALIZATION

MINDFUL ABOUT THE NATIONAL DEMAND BUT ALSO INTERNATIONAL

STANDARDS