***

REUSER'S INFORMATION SERVICES

Cyberthings for Managers

overview of significant cyber warfare events from the news

This is Cyberthings for Managers, created on Sunday 22nd April, 2012, at 13:07 o'clock (GMT+1), reporting on significant developments in the world of Cyber warfare, intended for managers.

Subscription information in the back.

Contents

1 Introduction

Cyberthings for Managers is a summary of significant news or literature about the domain of Cyberwarfare and directly related areas. The summary is aimed at manager level and higher, thus there will be no listings of technical hacks, flaws or incidents. Only major developments especially from governmental level down, are listed. Cyberthings for Managers is produced by *Reuser's Information Services*.

2 CyberReports

Why social media users fall for scams

source: Trend Micro. **date**: 2012
url: http://bit.ly/IIT9kh
summary: Easily making information available to contacts and the trust that exists among social media "friends" often lead users to carelessly click random links to fake photos and videos without thinking twice about online security. These behaviors may be the primary criminal motivation behind the various crafty tricks employed to dupe users into giving out their personal credentials.

Every social networking site has a feature like Facebook's wall that lets users post their own updates or see what their contacts are up to. Since the wall is the most accessible Facebook feature, it is also where most scams in the guise of videos and news riding on trending topics usually appear. We have seen several dubious Facebook posts with links, that when clicked, led to scams. We have taken note

1Q 2912 Security Roundup : Security in the Age of Mobility

source: Trend Micro . **date**: 2012
url: http://bit.ly/Ak5FL2
summary: "Mobile technology" is just what the name implies—portable technology that isn't limited to mobile phones. This also includes devices like laptops, tablets, and global positioning system (GPS) devices. As with any other kind of technology though, there are drawbacks to "going mobile." Mobile devices can expose users' and organizations' valuable data to unauthorized people if necessary precautions are not taken.

3 CyberNews

Den Haag krijgt Europees Cybercrime Centrum

source: Trouw . **date**: 28 Mar 2012
url: http://bit.ly/GXJ6YS
summary: Den Haag krijgt er weer een belangrijk instituut bij: het Europees Cybercrime Centrum. Dat heeft Eurocommissaris Cecilia Malmström van Binnenlandse Zaken vandaag bekendgemaakt.

Cybercrime is lucratiever dan de wereldwijde handel in marihuana, cocaïne en heroïne bij elkaar opgeteld. Cecilia Malmström, Eurocommissaris Binnenlandse Zaken

Een van de belangrijkste doelen van het centrum is het helpen bestrijden en in kaart brengen van georganiseerde internetcriminaliteit, zoals diefstal van identiteit, kinderpornografie en fraude met kredietkaarten. In het instituut zullen ICT-experts onder verantwoordelijkheid van Europol, het Europese samenwerkingsverband van politiediensten, komen te werken.

Hacker attack underlines Web role in China scandal

source: AP . **date**: 20 Apr 2012
url: http://yhoo.it/Jo9v0I
summary: A massive hacker attack has crippled an overseas website that has reported extensively on China's biggest political turmoil in years, underscoring the pivotal role the Internet has played in the unfolding scandal.

North Carolina-based Boxun.com was forced to move to a new web hosting service Friday after its previous host said the attacks were threatening its entire business, website manager Watson Meng told The Associated Press. He believes the attacks were ordered by China's security services, but it isn't clear where they were launched from.

"All members of NATO must share a common understanding of cyber security"

source: DiploNews . **date**: 14 Apr 2012
url: http://bit.ly/JtL0zt
summary: Just like we all know in NATO what standards the tanks, airplanes and ammunition of the alliance have to meet, we also need similar international cooperation between the allies in defining common standards in the sphere of cyber security, emphasised the President, Toomas Hendrik Ilves, who yesterday delivered a lecture at Harvard University.

Trojan sneaks into hotel, slurps guests' credit card data

source: TheRegister . **date**: 19 Apr 2012
url: http://bit.ly/Jm50IV
summary: Cyberooks are selling malware through underground forums which they claim offers the ability to steal credit card information from a hotel point of sale (POS) applications.

The ruse, detected by transaction security firm Trusteer, shows how criminals are using malware on enterprise machines to collect financial information in addition to targeting consumer PCs with banking Trojans and other nasties.

The hospitality industry attack involves using a remote access Trojan program to infect hotel front desk computers. The malware includes spyware components that steal credit card and other customer information by capturing screenshots from the PoS application. The malware is capable of stealing credit card numbers and expiration dates, but not CVV2 numbers in the sample Trusteer inspected.

Protest targets US cyber intelligence legislation

source: Space War . **date**: 16 Apr 2012
url: http://bit.ly/HMz4gz
summary: Civil liberties groups on Monday launched protests targeting proposed US cyber intelligence law that they fear would let police freely dip into people's private online information.

The Electronic Frontier Foundation (EFF) and Reporters Without Borders were among organizations that signaled the start of a week of Internet protests against the Cyber Intelligence Sharing and Protection Act (CISPA).

Chinese spying erodes US tech lead, agencies say

source: MilitaryFeed.com . **date**: 21 Apr 2012
url: http://bit.ly/IwhIBY
summary: U.S. access to intelligence, navigation and communications satellites, according to a report from the State and Defense departments.

"China's continuing efforts to acquire U.S. military and dual-use technologies are enabling China's science and technology base to diminish the U.S. technological edge in areas critical to the development of weapons and communications systems," the report released this week found.

"Additionally, the technologies China has acquired could be used to develop more advanced technologies by shortening Chinese RD cycles."

Two U.S. intelligence officials said that while the Chinese military isn't preparing to fight a major land war, its goal is to deny the U.S. military access to the other four arenas in which a war might be fought — the seas around China, the airspace surrounding the country, space, and cyberspace. The officials spoke on condition of anonymity because intelligence matters are classified.

A divided Congress confronts a rising cyberthreat

source: AP News . **date**: 21 Apr 2012
url: http://bit.ly/JYr9b6
summary: The House this coming week will consider legislation to better defend [...] corporate networks from foreign governments, cybercriminals and terrorist groups. But deep divisions over how best to handle the growing problem mean that solutions are a long way off.

Chief among the disputes is the role of the government in protecting the private sector.

The U.S. Chamber of Commerce and other business groups oppose requiring cybersecurity stan-

dards. Rules imposed by Washington would increase their costs without reducing their risks, they say.

Anonymous creates Pastebin rival to combat 'censorship'

source: BBC News . **date**: 12 April 2012
url: http://bit.ly/HYBmIg
summary: Hackers linking themselves to the Anonymous collective have created an alternative to Pastebin - the site they had traditionally used to reveal details of their attacks.

The group describes AnonPaste as "a totally secure and safe alternative".

There has been a backlash against Pastebin since its owner told the BBC he planned to hire more staff to police "sensitive posts".

AnonPaste has already been used to spread details of a planned attack

Le parlement Européen veut une cyber-Europe flicable à 100%

source: CNIS mag . **date**: 13 Apr 2012
url: http://bit.ly/HTWw6J
summary: Une page du site du Parlement Européen explique dans les grandes lignes les bases d'un projet de loi anti hacker qui risque fort bien de transformer le Net du vieux continent en une sorte de panoptique exposé aux seuls yeux des polices... et des véritables black-hat.

Le projet est présenté comme un texte visant à défendre contre des attaques Scada et rassure en disant que les sanctions prévues ne concerneront pas les cas mineurs ... une pondération qui n'a bien entendu strictement aucune signification d'un point de vue juridique.

Anonymous on Time magazine's 100 most influential list

source: SiliconRepublic . **date**: 19 Apr 2012
url: http://bit.ly/JhZAOK
summary: Hacktivist collective Anonymous has made it onto Time magazine's 100 Most Influential People in the World list.

"They are the people who inspire us, entertain us, challenge us and change our world," Time magazine said of the people on its annual list.

India Breeds Twenty Percent of World's Spam

source: SiliconIndia news . **date**: 20 Apr 2012
url: http://bit.ly/IISb7v
summary: Twenty per cent of the spam mails that were sent out worldwide in the quarter ended March 31, 2012, originated in India, according to a study by security software firm Trend Micro.

"The quarter's top spam-sending countries included India at 20 percent, Indonesia at 13 percent, South Korea at 12 percent and Russia at 10 percent," the report said.

The report added that attacks are now more of a long-term, on-going campaign, versus the typical "smash-and-grab incidents" favoured by cy-

bercriminals in the past.

Google: 20.000 Websites mit Malware verseucht

source: Chip online . **date**: 20 Apr 2012
url: http://bit.ly/JrQNbz
summary: Google hat seine Kunden im Blick. Der Konzern hat jetzt 20.000 Webseitenbetreiber darauf aufmerksam gemacht, dass deren Seiten mit Malware verseucht sein könnten.

Möglicherweise seien die Seiten gehackt, hieß es in einer Aussendung. "Wir glauben, dass jemand infiziertes JavaScript missbraucht, um Nutzer auf maliziöse Seiten umzuleiten", schrieb das Google Search Quality Team.

Die Webseitenbetreiber sollten gezielt nach Dateien suchen, die "eval(function(p,a,c,k,e,r)" beinhalteten. Der Code könne in HTML-, JavaScript- oder PHP-Dateien versteckt sein.

6 Things You Need to Know About the Government's New Spy Law (CISPA)

source: AlterNet . **date**: 18 Apr 2012
url: http://bit.ly/HVpQK8
summary: Congress is seriously considering a bill called the Cyber Intelligence Sharing and Protection Act (CISPA). Intended to allow information-sharing both between corporations and between corporations and the government, it presents serious dangers to individual privacy. The most important parts of the proposed act permit corporations to share information about their customers with each other and with the government if they assert that this information-sharing is necessary for national security.

Battle for the Internet

source: The Guardian . **date**: Apr 2012
url: http://bit.ly/HJZGzm
summary: The Guardian is taking stock of the new battlegrounds for the internet. From states stifling dissent to the new cyberwar front line, we look at the challenges facing the dream of an open internet.

Canada's cybersecurity agency CSEC full of secrets

source: Vancouver Sun . **date**: 18 Apr 2012
url: http://bit.ly/I2707t
summary: Explosive budget, staff numbers raise questions from critics - who watches the watchers? Following a decade of explosive growth, the super-secret Communications Security Establishment Canada has emerged from the Defence Department to become a stand-alone federal agency, a change that will force it, for the first time, to inform Canadians of at least some of its activities.

CSEC, whose powers include the ability to sometimes eavesdrop on Canadians without their knowing, has largely escaped the axe as the federal government chops budgets. Where some departments face cuts of 10 per cent, CSEC will be pinched by just two per cent this year and the agency will see no layoffs.

4 CyberConferences

The SCADA Smart Grid Cyber Security Summit 2012

organised by: Oliver Kinross
place: London U.K.
dates: 26-27 April 2012
url:
summary: Assess the nature of the latest threats being faced by energy companies and the impact of these upon your organisation.

Discover why Utility Cyber Security has been reaching a state of near chaos and the latest strategies from utilities to gain the upper-hand against hackers.

Understand the importance of industrial control system (ICS) security and assess the latest solutions on offer.

Discuss the most promising cyber security technologies in the marketplace.

Assess the trends to watch in utility cyber security.

Discover the best practice from across Europe in protecting SCADA and the Smart Grid from cyber-attack. Benefit from case study presentations from a wide range of international utilities and energy companies.

5 Colofon

Cyberthings for Managers is created by *Reuser's Information Services* to meet a growing demand by managers in the domain of cyber warfare for a quick overview of the most important events of the past weeks in the field, without being overwhelmed by technical details, individual incidents, or repetitions of earlier news. Cyberthings will list a summary of significant events in the world of Cyberwarfare from Governmental level down. There will be no listings of technical hacks, detailed descriptions of cyberweapons, repetitions of detailed cybercrime events, only the more strategic events will be covered.

Cyberthings for Managers has clickable links and is intended to be used either online or in print. News will be covered from the previous weeks.

Cyberthings for Managers is published once a week on Sunday around 18:00 GMT+1. Distribution is free.

Subscribe? Mail "subscribe cyberthings" to: cyberthings@reuser.biz

Unsubscribe? Mail "unsubscribe cyberthings" to: cyberthings@reuser.biz

Archive. An archive of previous editions is maintained at http://www.opensourceintelligence.eu, choose Products, then Publications.

With special thanks to our regular contributors: MirceaM; Silobreaker (Infosphere)

Please contact me (a ATSIGN reuser DOT biz) if you have any questions.