ST Electronics
Info-Security
A member of ST Engineering

ICTA
ideas actioned

SRI LANKA
CERT|CC

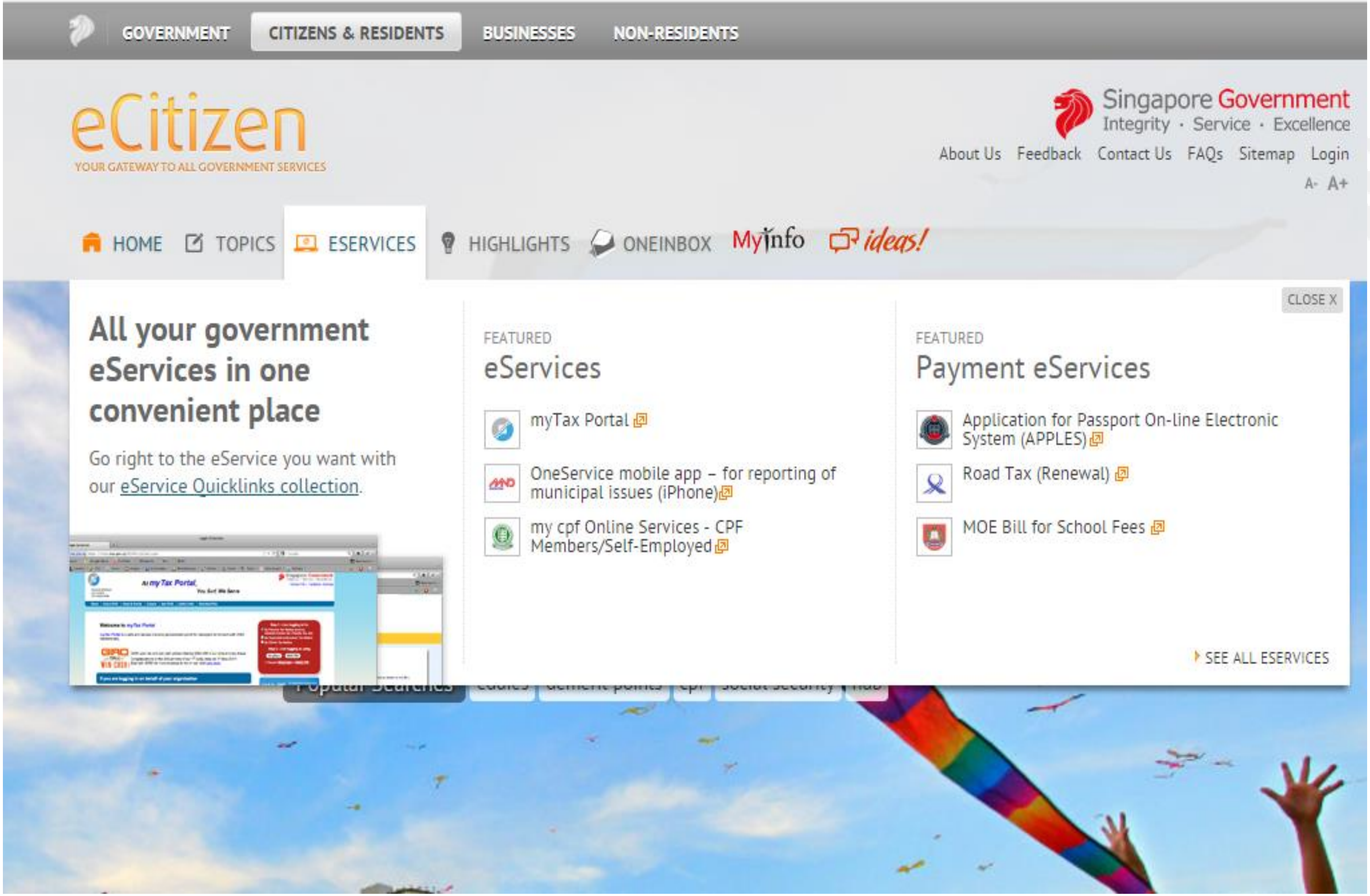
Global Cyber Threat Landscape

Presented by:

Victor Yeo, CISSP, QISP
Deputy General Manager
27 April 2017

50 ENGINEERING WITH PASSION

Empowering thru' Innovation



All your government eServices in one convenient place

Go right to the eService you want with our eService Quicklinks collection.

FEATURED

eServices

- myTax Portal
- OneService mobile app – for reporting of municipal issues (iPhone)
- my cpf Online Services - CPF Members/Self-Employed

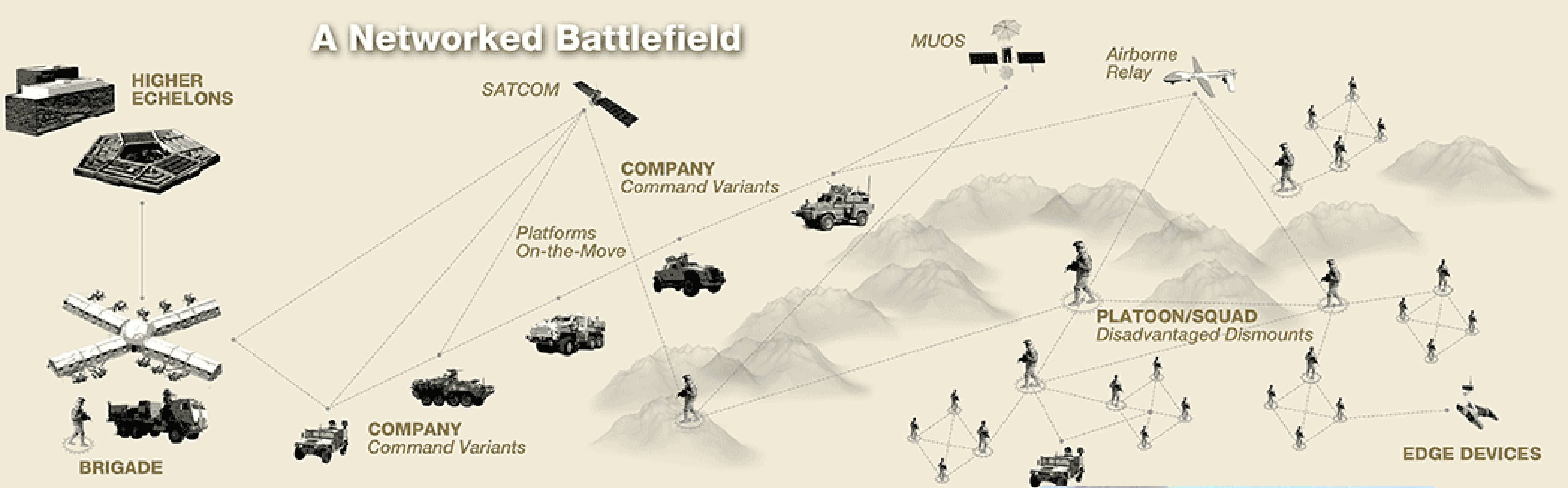
FEATURED

Payment eServices

- Application for Passport On-line Electronic System (APPLES)
- Road Tax (Renewal)
- MOE Bill for School Fees

SEE ALL ESERVICES

Networked Military Operations



fintech
lending
money transfers
payments
wealth management
cryptocurrencies
bypass banks
p2p lending
crowd funding
mobile payment

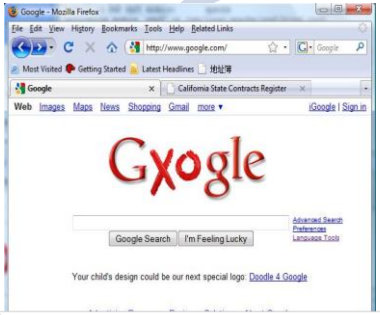
Interconnectivity in the Era of Internet of Things

SMART NATION

Who and What are the Threats in Cyber Space?

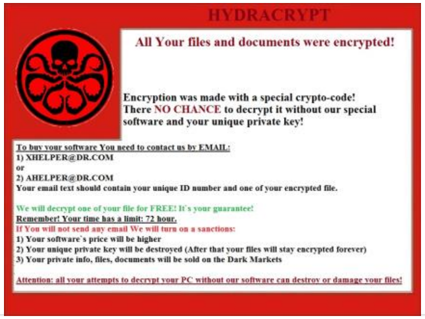
Evolving Cyber Security Threats

- Attention seeking hobbyist
- Posting of graffiti on websites



Defaced websites

- Motivated by money
- Glory-seeking



HYDRACRYPT

All Your files and documents were encrypted!

Encryption was made with a special crypto-code!
There NO CHANCE to decrypt it without our special software and your unique private key!

To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your unique ID number and one of your encrypted file.

We will decrypt one of your file for FREE! It`s your guarantee!
Remember! Your time has a limit: 72 hour.
If You will not send any email We will turn on a sanctions:
1) Your software`s price will be higher
2) Your unique private key will be destroyed (After that your files will stay encrypted forever)
3) Your private info, files, documents will be sold on the Dark Markets

Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

Ransonware

Fake SPF website for exploitations of personal data

- Professional organised group
- Involved scouting and intelligence gathering

Hackers stole $81 million from Bangladesh Bank

Yahoo says 500 million accounts stolen

20 years

10 years

Present

Evolving Cyber Security Threats

46% Criminals

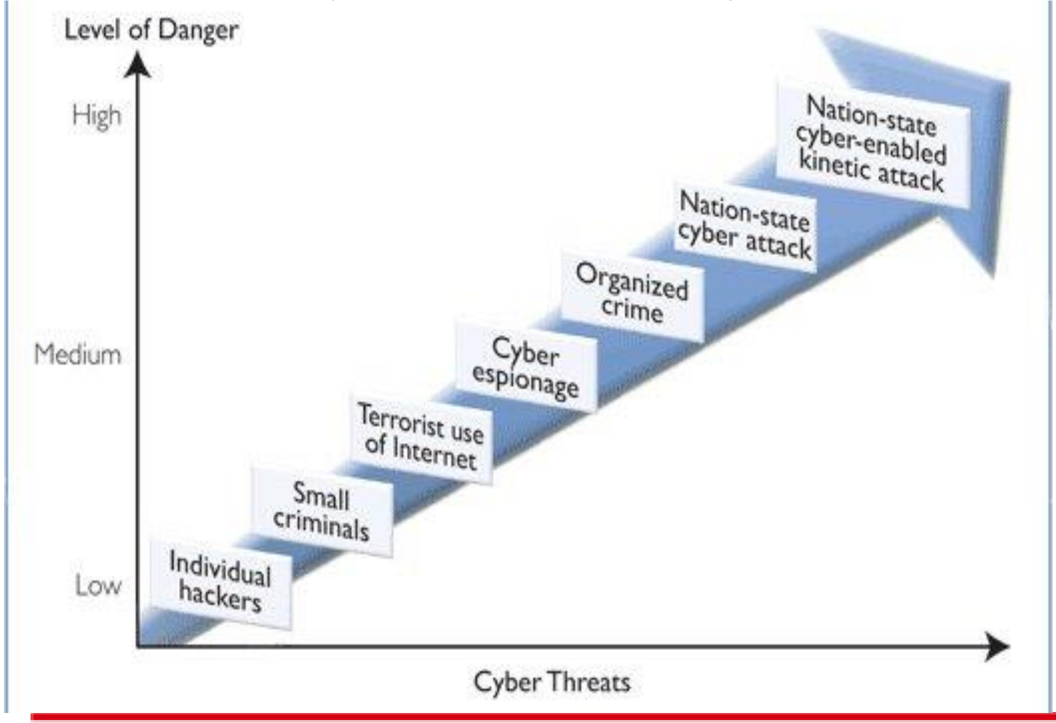
Primary target assets:
Financial

33% Hacktivists

Primary target assets:
Website

21% Nation State

Primary target assets:
Information

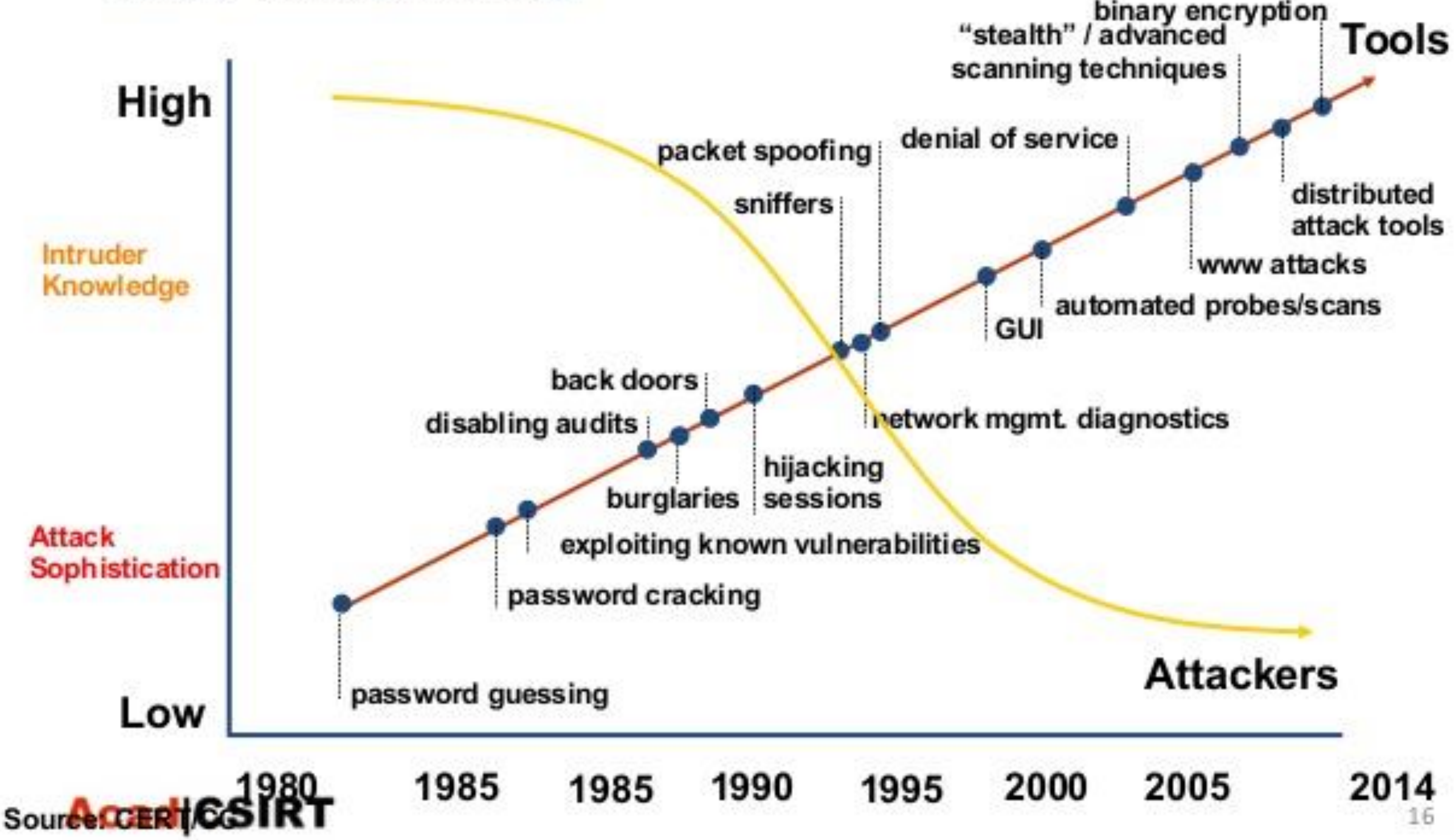


North Korea hacking of Sony Pictures in 2014

Stuxnet sabotage of Iranian nuclear complex in Natanz

Increasing Attack Sophistication

Attack sophistication vs
Intruder Technical Knowledge



Source: CERT/CC

Exploit Tools Market

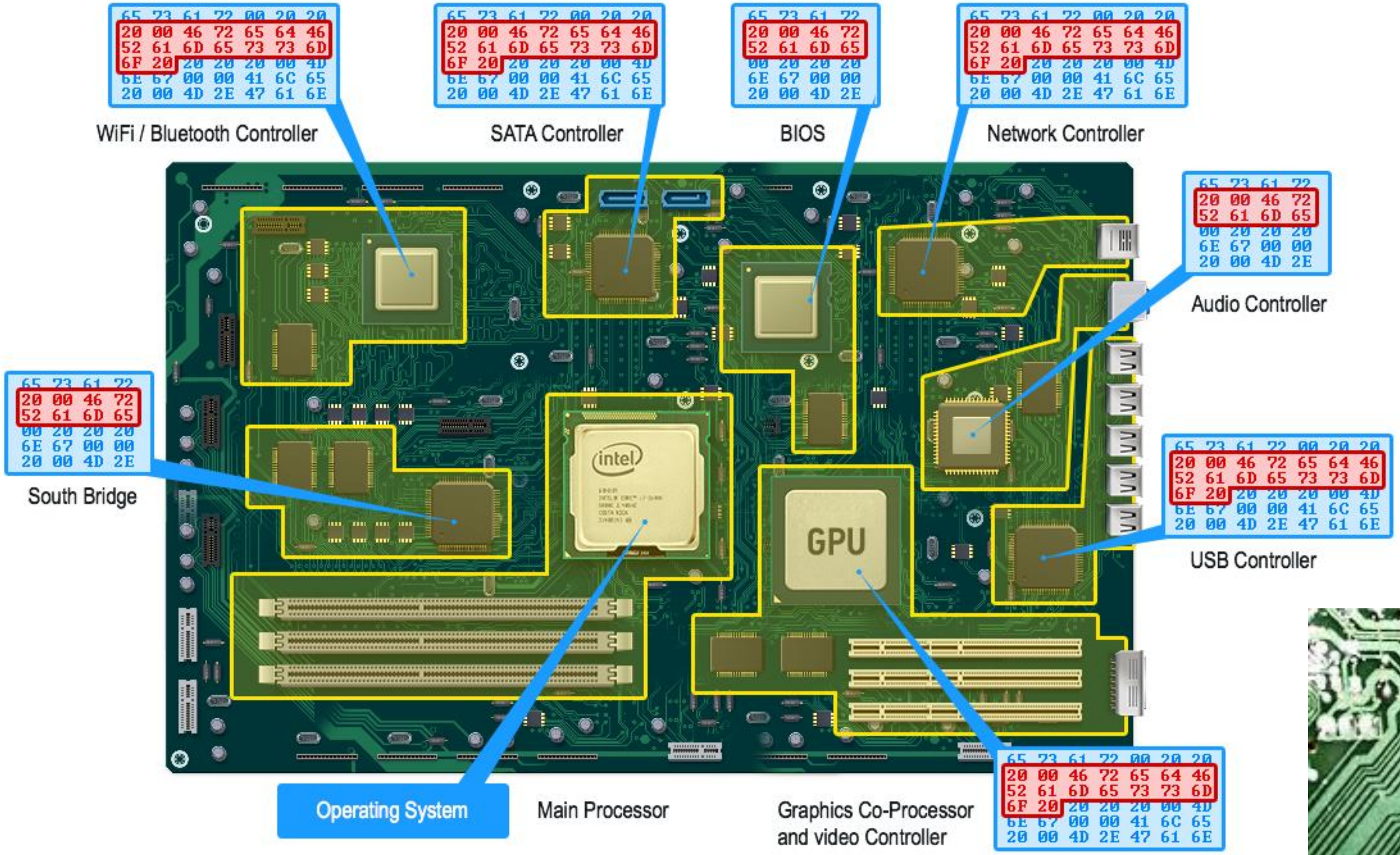
ELECTRONIC FRONTIER FOUNDATION
MOTHER SHOULD I TRUST THE HACKERS?

- ► Wireless Hacking.
- ► Network Hacking.
- ► Rubber Ducky USB.
- ► Lock Picks and Practice Tools.
- ► Software Defined Radio.

DEFCON Hands-on Hacking Villages

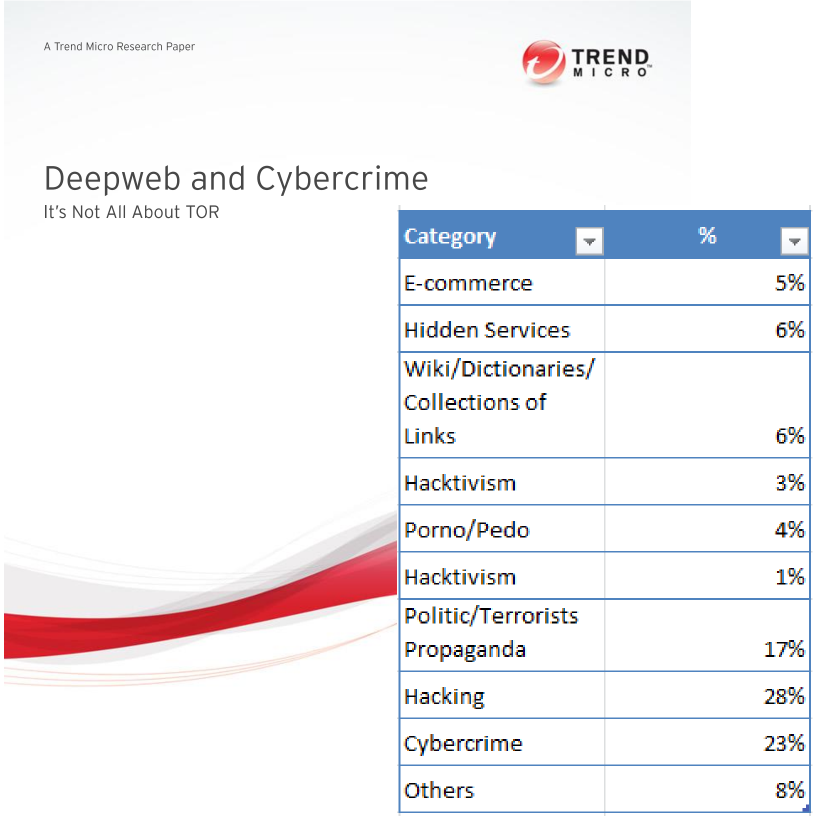
CTF Games; Web, Network, IOT, CAR, Wireless

It might already been hacked.



Embedded
Backdoor

Deepweb + Social Media



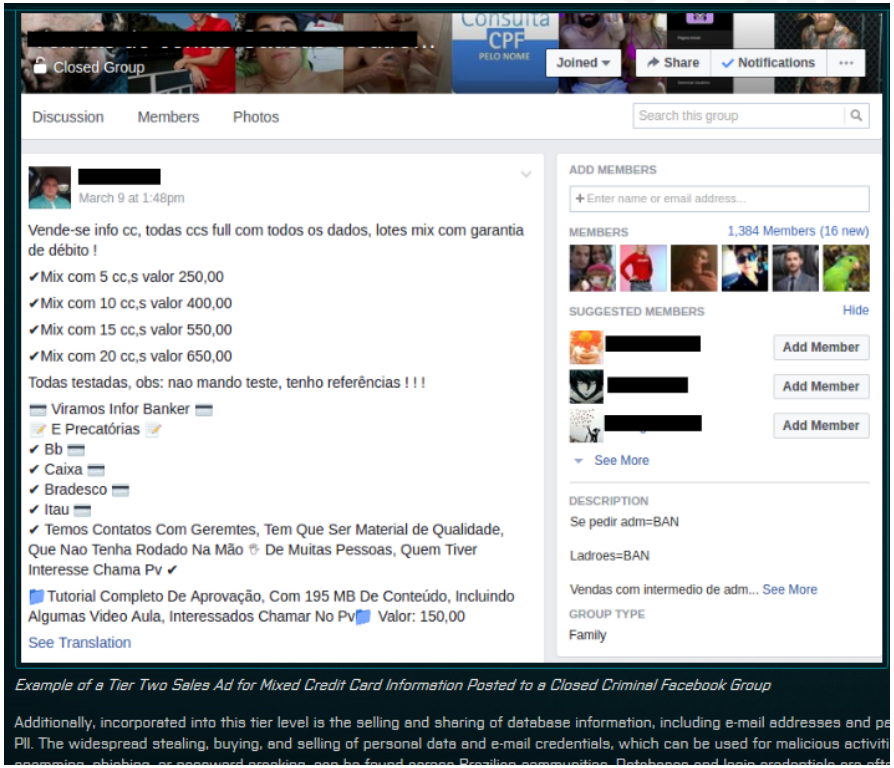
A Trend Micro Research Paper

Deepweb and Cybercrime

It's Not All About TOR

Category	%
E-commerce	5%
Hidden Services	6%
Wiki/Dictionaries/ Collections of Links	6%
Hacktivism	3%
Porno/Pedo	4%
Hacktivism	1%
Politic/Terrorists Propaganda	17%
Hacking	28%
Cybercrime	23%
Others	8%

A sample of around 25,000 Tor addresses randomly generated by their crawlers inspections.



[redacted]
March 9 at 1:48pm

Vende-se info cc, todas ccs full com todos os dados, lotes mix com garantia de débito !

✓Mix com 5 cc,s valor 250,00

✓Mix com 10 cc,s valor 400,00

✓Mix com 15 cc,s valor 550,00

✓Mix com 20 cc,s valor 650,00

Todas testadas, obs: nao mando teste, tenho referências ! ! !

💳 Viramos Infor Banker 💳
📝 E Precatórias 📝
✓ Bb 💳
✓ Caixa 💳
✓ Bradesco 💳
✓ Itau 💳
✓ Temos Contatos Com Geremtes, Tem Que Ser Material de Qualidade, Que Nao Tenha Rodado Na Mão De Muitas Pessoas, Quem Tiver Interesse Chama Pv ✓

📁 Tutorial Completo De Aprovação, Com 195 MB De Conteúdo, Incluindo Algumas Video Aula, Interessados Chamar No Pv📁 Valor: 150,00

See Translation

[redacted] [redacted] [redacted]

DESCRIPTION

Se pedir adm=BAN

Ladroes=BAN

Vendas com intermedio de adm... See More

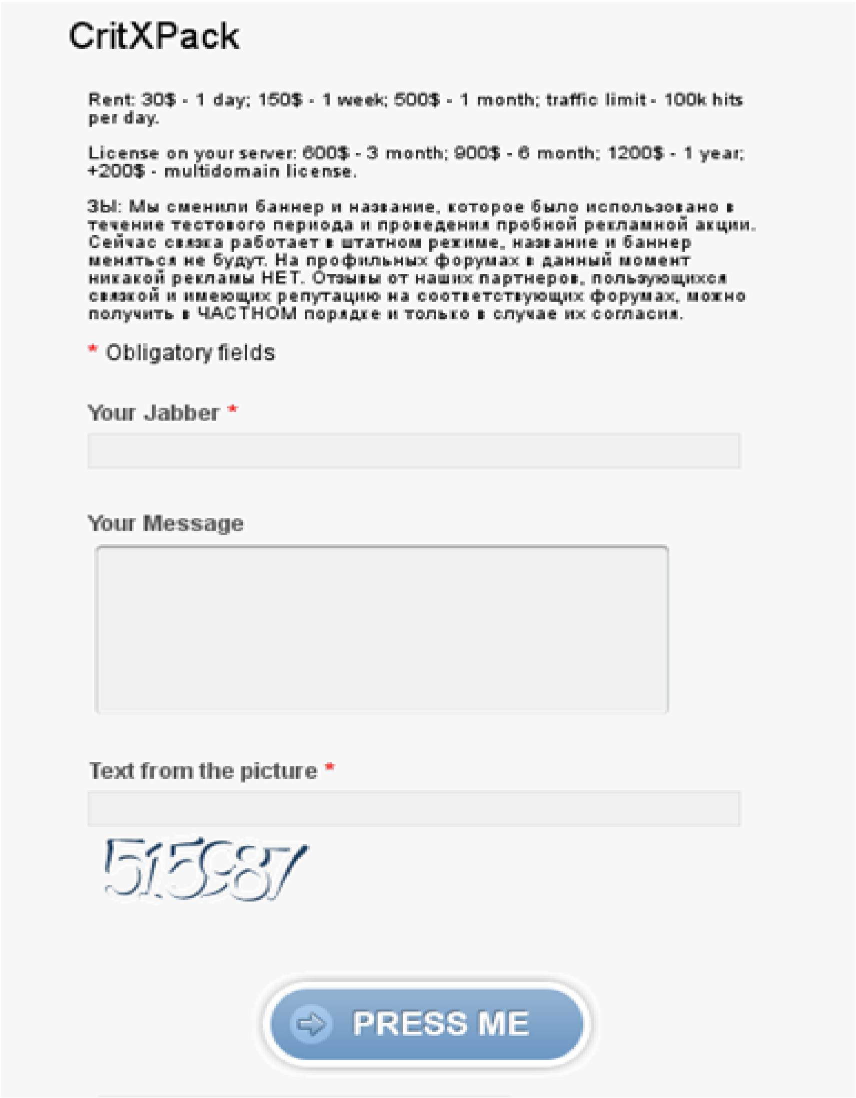
GROUP TYPE

Family

Example of a Tier Two Sales Ad for Mixed Credit Card Information Posted to a Closed Criminal Facebook Group

Additionally, incorporated into this tier level is the selling and sharing of database information, including e-mail addresses and pe
PII. The widespread stealing, buying, and selling of personal data and e-mail credentials, which can be used for malicious activiti

- http://resources.infosecinstitute.com/project-artemis-osint-activities-on-deep-web/



CritXPack

Rent: 30$ - 1 day; 150$ - 1 week; 500$ - 1 month; traffic limit - 100k hits per day.

License on your server: 600$ - 3 month; 900$ - 6 month; 1200$ - 1 year; +200$ - multidomain license.

ЗЫ: Мы сменили баннер и название, которое было использовано в течение тестового периода и проведения пробной рекламной акции. Сейчас связка работает в штатном режиме, название и баннер меняться не будут. На профильных форумах в данный момент никакой рекламы НЕТ. Отзывы от наших партнеров, пользующихся связкой и имеющих репутацию на соответствующих форумах, можно получить в ЧАСТНОМ порядке и только в случае их согласия.

* Obligatory fields

Your Jabber *

Your Message

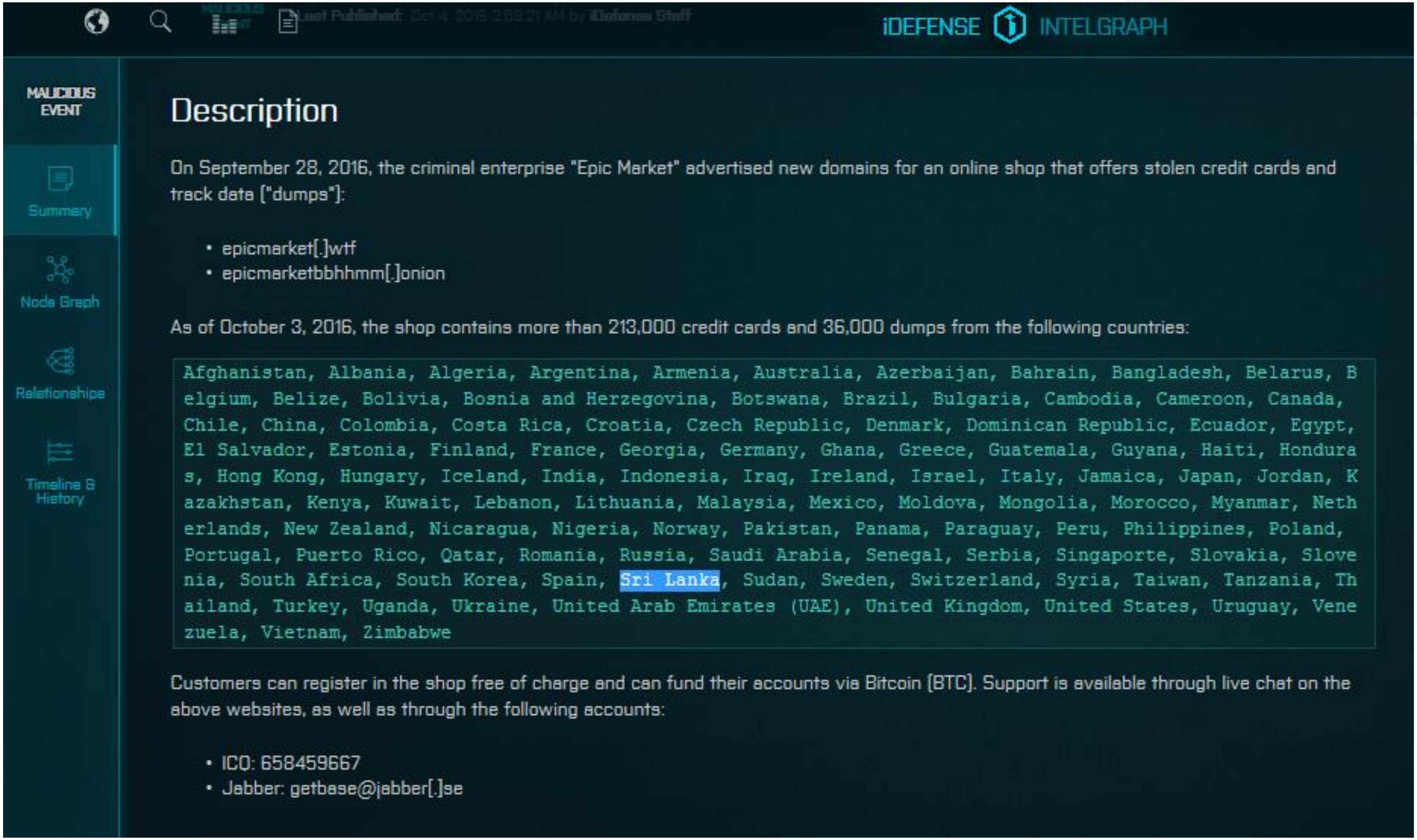
Text from the picture *

515987

Security expert Dancho Danchev in a post on Webroot threat blog revealed newly launched underground service offering access to thousands of malware-infected machine for upsetting prices, a thousand US-based hosts costs $200 meanwhile for a thousand EU-based hosts price varies between $60/$120, and the price for a thousand international mix type of hosts is $20.
Botnet_as_services

Loads
Loads
$200/k
USA
EU
$60-$120/k
$20/k
WorldMix
ICQ:
Jabber:

http://securityaffairs.co/wordpress/12339/cyber-crime/botnets-for-rent-criminal-services-sold-in-the-underground-market.html
http://www.csoonline.com/article/729655/prices-fall-services-rise-in-malware-as-a-service-market



Description

On September 28, 2016, the criminal enterprise "Epic Market" advertised new domains for an online shop that offers stolen credit cards and track data ("dumps"):

- epicmarket[.]wtf
- epicmarketbbhhmm[.]onion

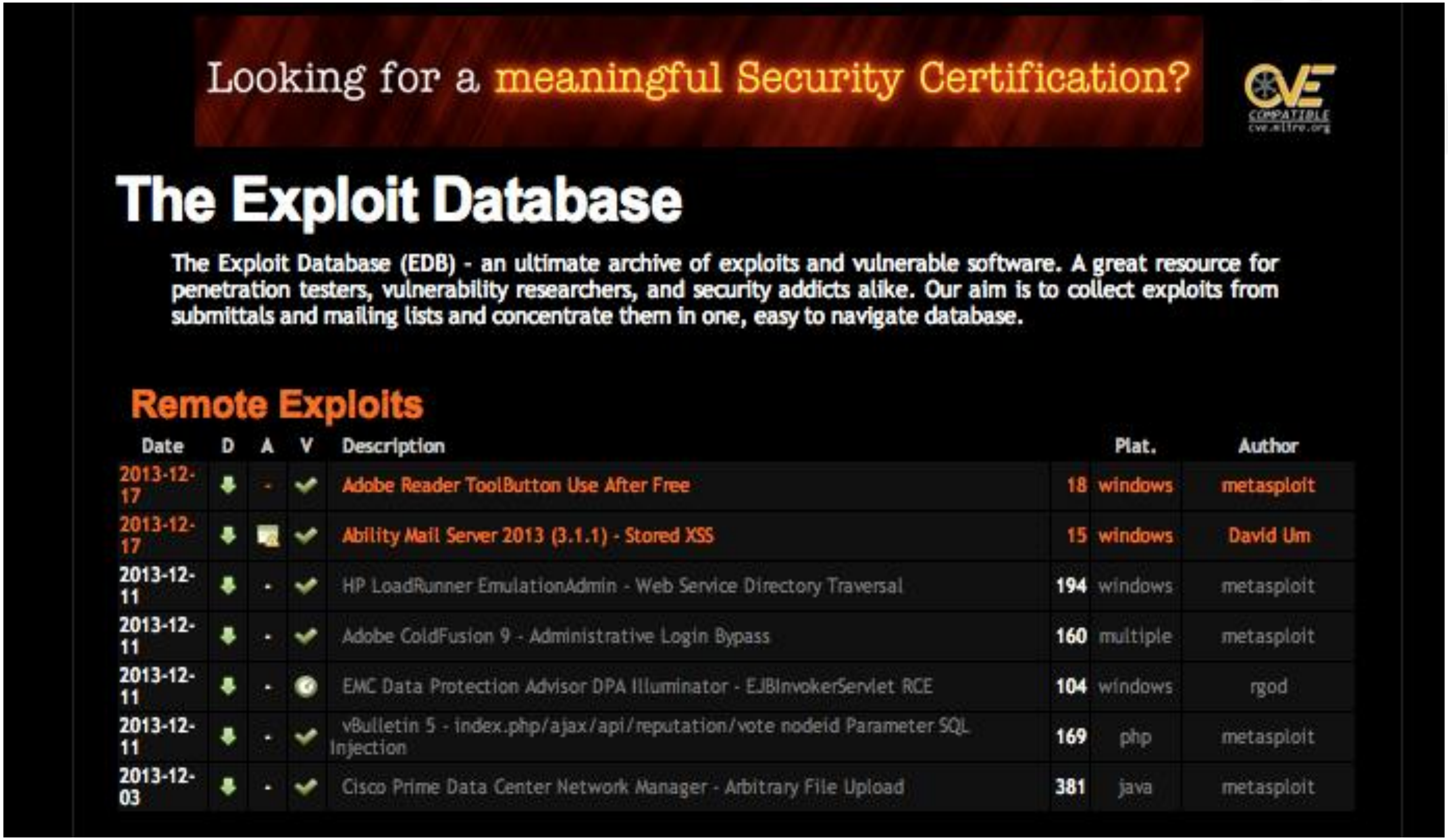
As of October 3, 2016, the shop contains more than 213,000 credit cards and 36,000 dumps from the following countries:

Afghanistan, Albania, Algeria, Argentina, Armenia, Australia, Azerbaijan, Bahrain, Bangladesh, Belarus, Belgium, Belize, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Bulgaria, Cambodia, Cameroon, Canada, Chile, China, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Ecuador, Egypt, El Salvador, Estonia, Finland, France, Georgia, Germany, Ghana, Greece, Guatemala, Guyana, Haiti, Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Iraq, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Lebanon, Lithuania, Malaysia, Mexico, Moldova, Mongolia, Morocco, Myanmar, Netherlands, New Zealand, Nicaragua, Nigeria, Norway, Pakistan, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Puerto Rico, Qatar, Romania, Russia, Saudi Arabia, Senegal, Serbia, Singaporte, Slovakia, Slovenia, South Africa, South Korea, Spain, Sri Lanka, Sudan, Sweden, Switzerland, Syria, Taiwan, Tanzania, Thailand, Turkey, Uganda, Ukraine, United Arab Emirates (UAE), United Kingdom, United States, Uruguay, Venezuela, Vietnam, Zimbabwe

Customers can register in the shop free of charge and can fund their accounts via Bitcoin (BTC). Support is available through live chat on the above websites, as well as through the following accounts:

- ICQ: 658459667
- Jabber: getbase@jabber[.]se

Finding exploits



Looking for a meaningful Security Certification?
CVE COMPATIBLE cve.mitre.org

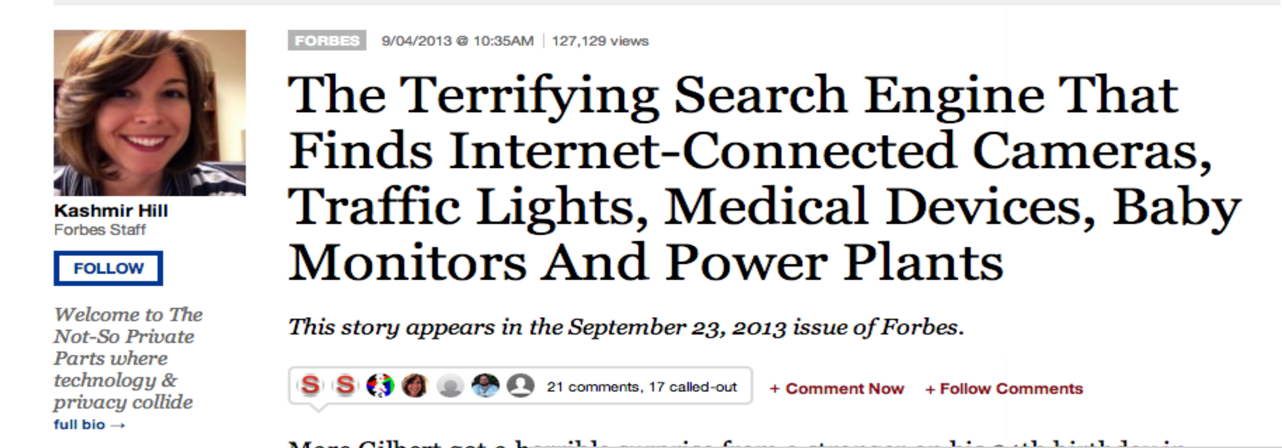
The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

Remote Exploits

Date	D	A	V	Description		Plat.	Author
2013-12-17	⬇	-	✓	Adobe Reader ToolButton Use After Free	18	windows	metasploit
2013-12-17	⬇	▨	✓	Ability Mail Server 2013 (3.1.1) - Stored XSS	15	windows	David Um
2013-12-11	⬇	-	✓	HP LoadRunner EmulationAdmin - Web Service Directory Traversal	194	windows	metasploit
2013-12-11	⬇	-	✓	Adobe ColdFusion 9 - Administrative Login Bypass	160	multiple	metasploit
2013-12-11	⬇	-	◷	EMC Data Protection Advisor DPA Illuminator - EJBInvokerServlet RCE	104	windows	rgod
2013-12-11	⬇	-	✓	vBulletin 5 - index.php/ajax/api/reputation/vote nodeid Parameter SQL Injection	169	php	metasploit
2013-12-03	⬇	-	✓	Cisco Prime Data Center Network Manager - Arbitrary File Upload	381	java	metasploit

Finding devices with vulnerability



FORBES 9/04/2013 @ 10:35AM | 127,129 views

The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors And Power Plants

Kashmir Hill
Forbes Staff

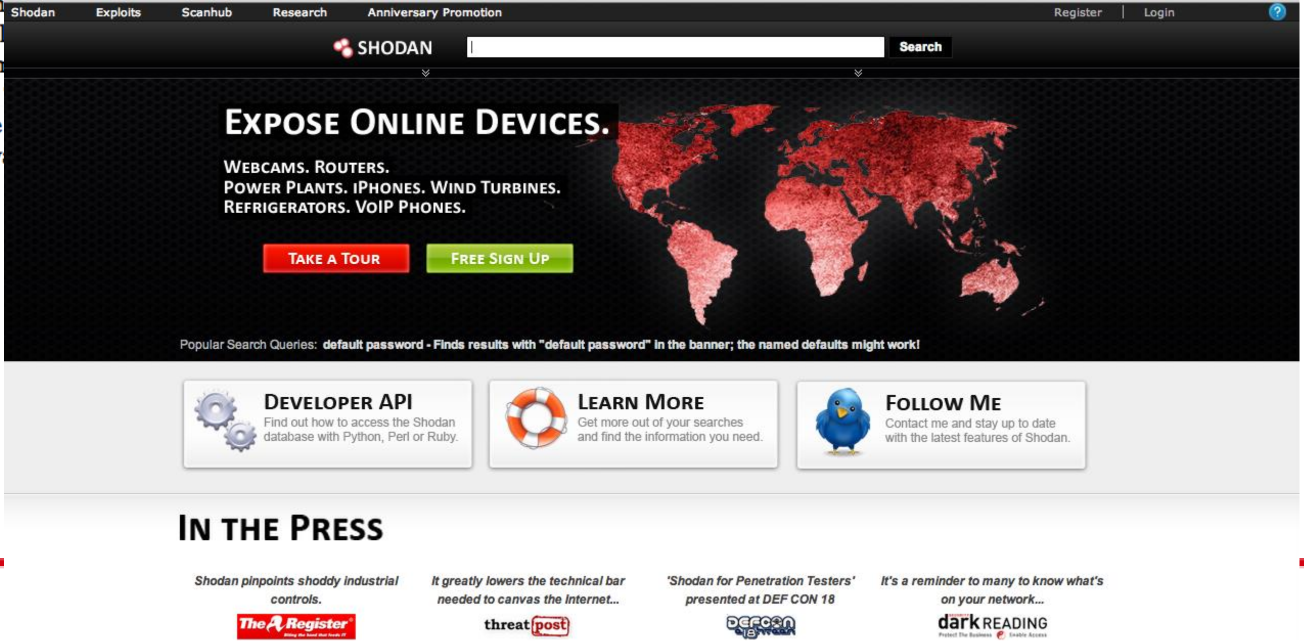
FOLLOW

Welcome to The Not-So Private Parts where technology & privacy collide
full bio →

This story appears in the September 23, 2013 issue of Forbes.

21 comments, 17 called-out + Comment Now + Follow Comments

Marc Gilbert got a h
August. After the cel
unfamiliar voice con
sleeping 2-year-old,
discovered the voice
taken control of it w



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

Popular Search Queries: **default password - Finds results with "default password" in the banner; the named defaults might work!**

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

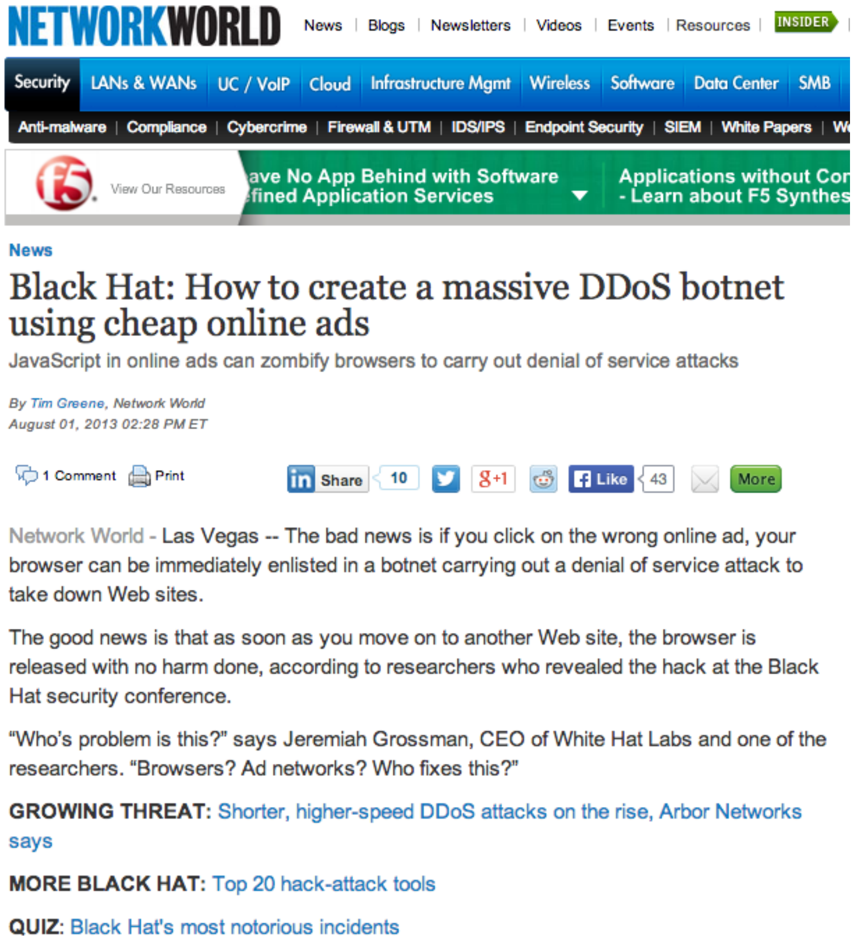
Shodan pinpoints shoddy industrial controls. — The Register

It greatly lowers the technical bar needed to canvas the Internet... — threatpost

'Shodan for Penetration Testers' presented at DEF CON 18 — DEFCON 18

It's a reminder to many to know what's on your network... — dark READING

Attacker will exploit whatever means available


NETWORKWORLD
News | Blogs | Newsletters | Videos | Events | Resources | INSIDER |
Security | LANs & WANs | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center | SMB
Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SIEM | White Papers | W
f5 View Our Resources
ave No App Behind with Software
fined Application Services
Applications without Cor
- Learn about F5 Synthes
1 Comment
Print
Share
10
g+1
Like
43
More

News

Black Hat: How to create a massive DDoS botnet using cheap online ads

JavaScript in online ads can zombify browsers to carry out denial of service attacks

By Tim Greene, Network World
August 01, 2013 02:28 PM ET

Network World - Las Vegas -- The bad news is if you click on the wrong online ad, your browser can be immediately enlisted in a botnet carrying out a denial of service attack to take down Web sites.

The good news is that as soon as you move on to another Web site, the browser is released with no harm done, according to researchers who revealed the hack at the Black Hat security conference.

"Who's problem is this?" says Jeremiah Grossman, CEO of White Hat Labs and one of the researchers. "Browsers? Ad networks? Who fixes this?"

GROWING THREAT: Shorter, higher-speed DDoS attacks on the rise, Arbor Networks says

MORE BLACK HAT: Top 20 hack-attack tools

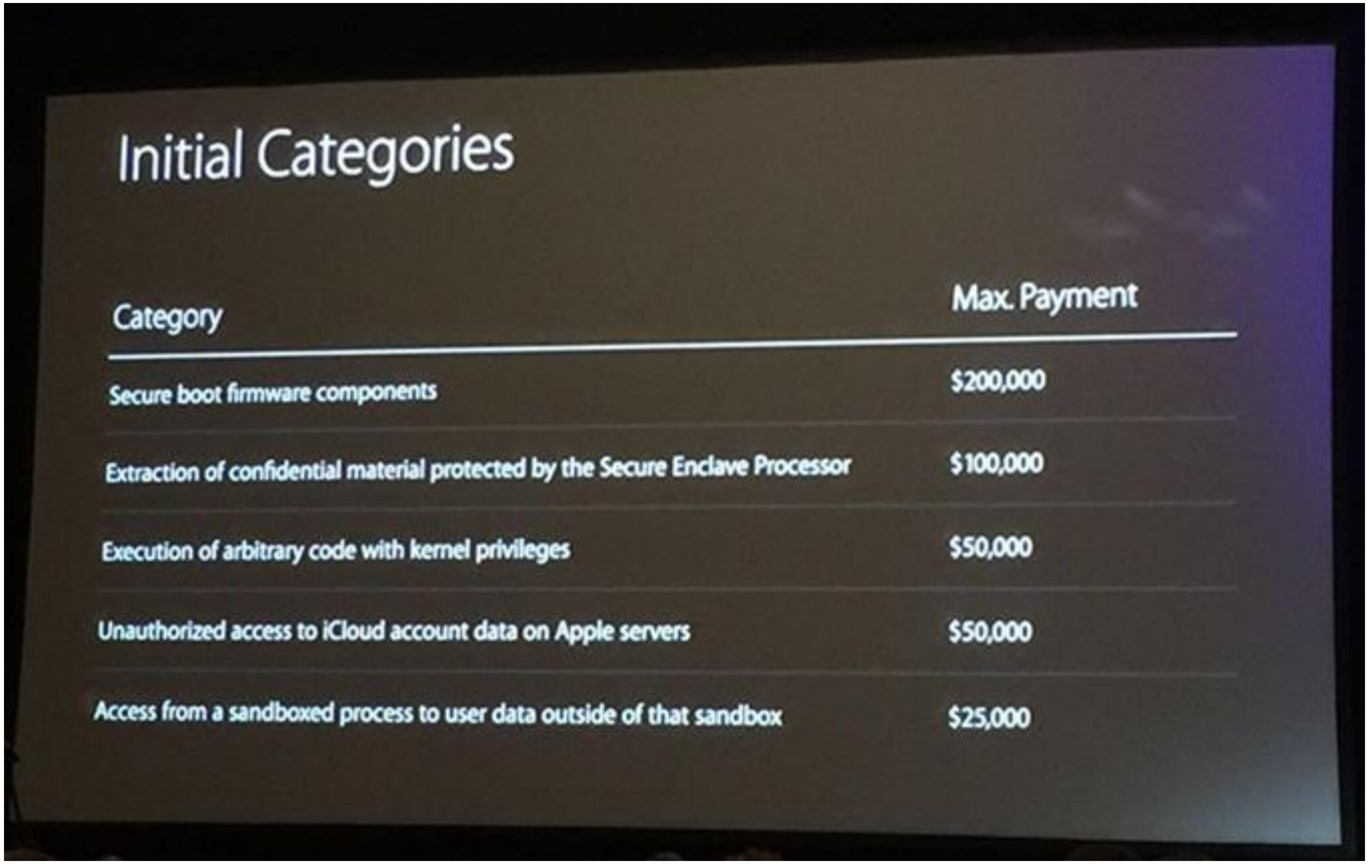
QUIZ: Black Hat's most notorious incidents

In the case of creating an on-the-fly botnet, Grossman and his associate Matt Johansen placed JavaScript within ads that they placed on Web pages via an advertising network. They paid to have the ad garner a certain number of clicks. The cost of a million-browser botnet is about $150.

- http://www.networkworld.com/news/2013/080113-black-hat-ddos-botnets-272447.html

Hackers as Internet Guardian

- Hackers can serve as defender as well (White-hat).
- Companies are employing hackers to find vulnerabilities.



Initial Categories

Category	Max. Payment
Secure boot firmware components	$200,000
Extraction of confidential material protected by the Secure Enclave Processor	$100,000
Execution of arbitrary code with kernel privileges	$50,000
Unauthorized access to iCloud account data on Apple servers	$50,000
Access from a sandboxed process to user data outside of that sandbox	$25,000

The Agenda

The growing threat of cyber mercenaries

Washington is focused on combating cyber attacks from nation states. But the real threat is elsewhere.

Anonymous

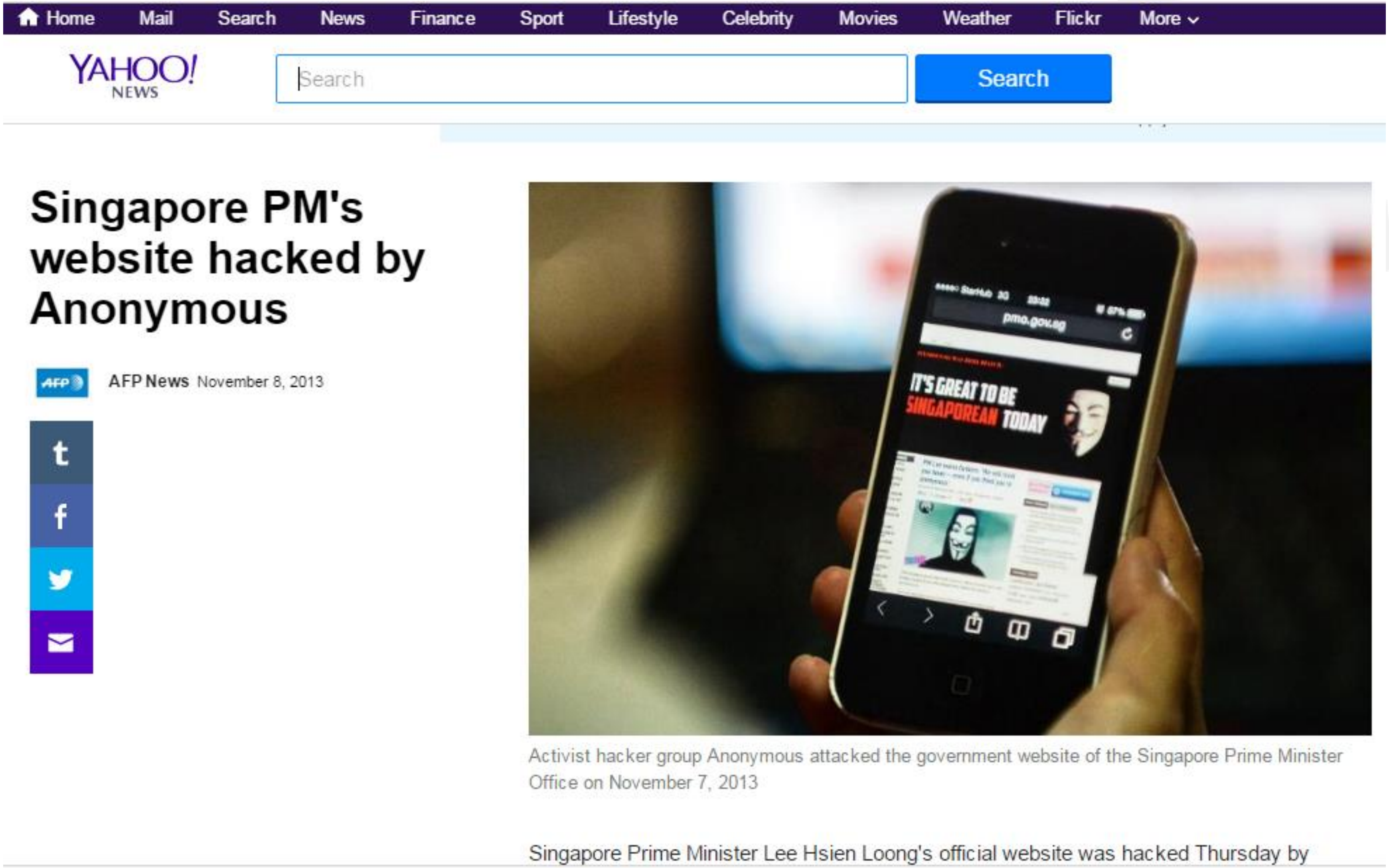
2008. Project Chanology—hacks targeting the Church of Scientology.

2011. Operation Tunisia, Operation Egypt in support of Arab Spring movements.

2011 Attack on Sony in retaliation for trying to stop hacks of the PlayStation 3 game console.

September 2011 -Occupy Wall Street protests began in New York City.

Image Source: http://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221



Singapore PM's website hacked by Anonymous

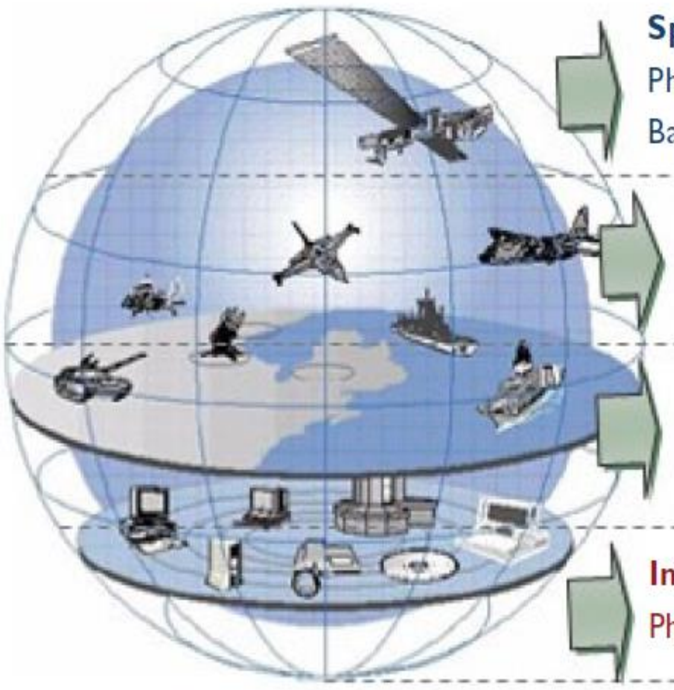
AFP News November 8, 2013

Activist hacker group Anonymous attacked the government website of the Singapore Prime Minister Office on November 7, 2013

Singapore Prime Minister Lee Hsien Loong's official website was hacked Thursday by

Nation States already have Information Warfare Capabilities

INFORMATION WARFARE | With Advancement in Technology, Information Environment is set to be the Next Domain of Conflict



Space

Photographic Satellites, GPS, Communications, Ballistic Missile Defence, Signals, Astronauts

Air

ISR Platforms, Combat Aircraft, Transport, Helicopters, Maritime Surveillance, Communications, Airmen

Naval

Combat Platforms, Communications, ISR, Transport, Sailors

Land

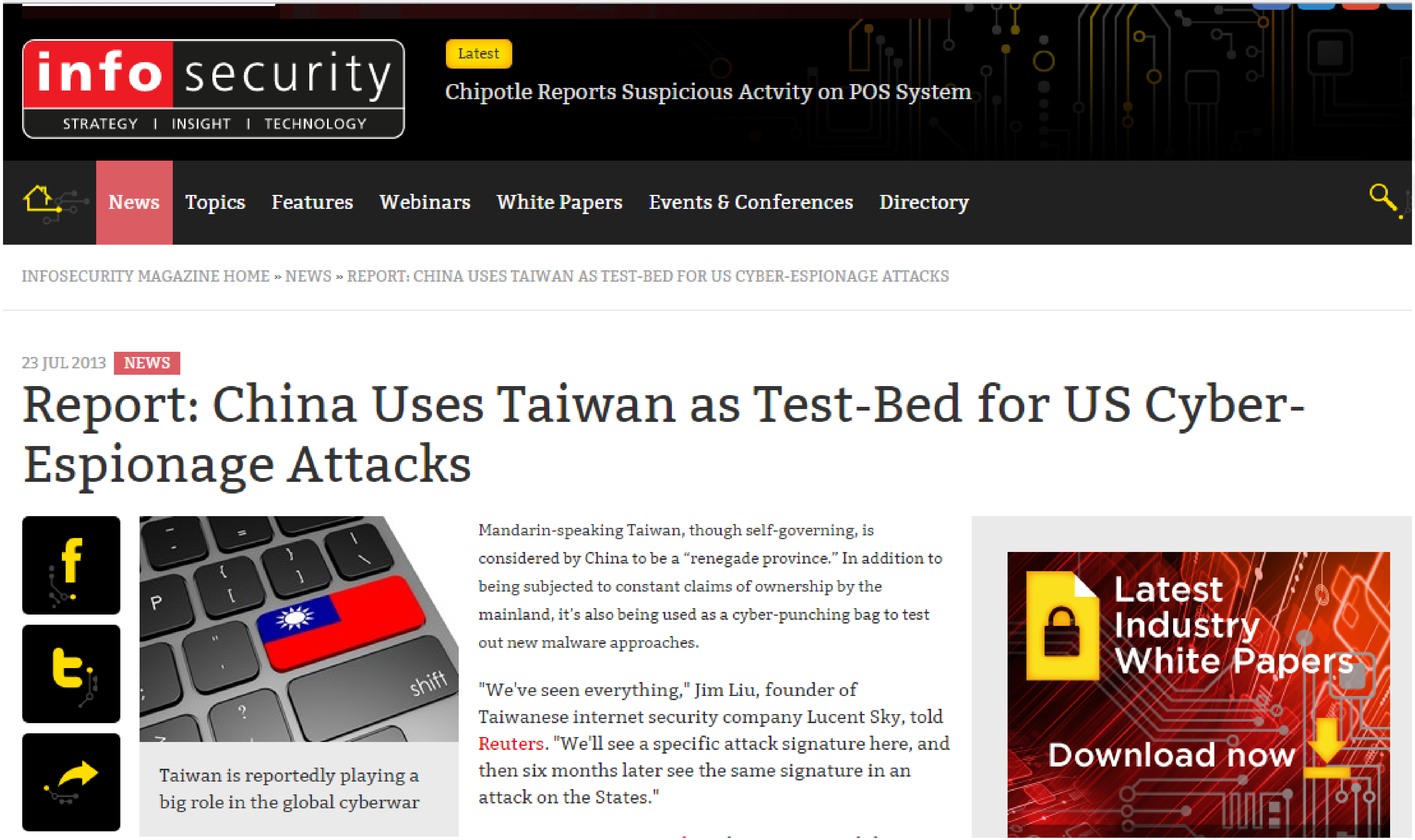
Combat Vehicles, Transport, Communications, Soldiers

Information Environment

Physical, Cognitive, Informational Dimensions

Information is a key enabler in Joint Operations

Source: Frost & Sullivan



Chipotle Reports Suspicious Actvity on POS System

INFOSECURITY MAGAZINE HOME » NEWS » REPORT: CHINA USES TAIWAN AS TEST-BED FOR US CYBER-ESPIONAGE ATTACKS

23 JUL 2013 NEWS

Report: China Uses Taiwan as Test-Bed for US Cyber-Espionage Attacks

Taiwan is reportedly playing a big role in the global cyberwar

Mandarin-speaking Taiwan, though self-governing, is considered by China to be a “renegade province.” In addition to being subjected to constant claims of ownership by the mainland, it's also being used as a cyber-punching bag to test out new malware approaches.

"We've seen everything," Jim Liu, founder of Taiwanese internet security company Lucent Sky, told Reuters. "We'll see a specific attack signature here, and then six months later see the same signature in an attack on the States."

National Infrastructure at Risk

Government

Energy

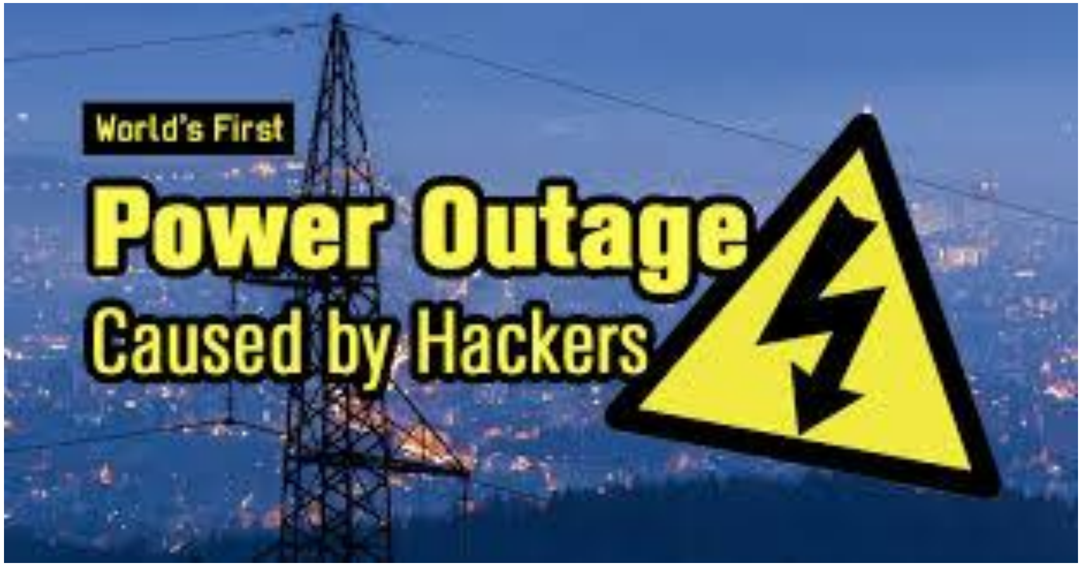
Transport

Homeland Security

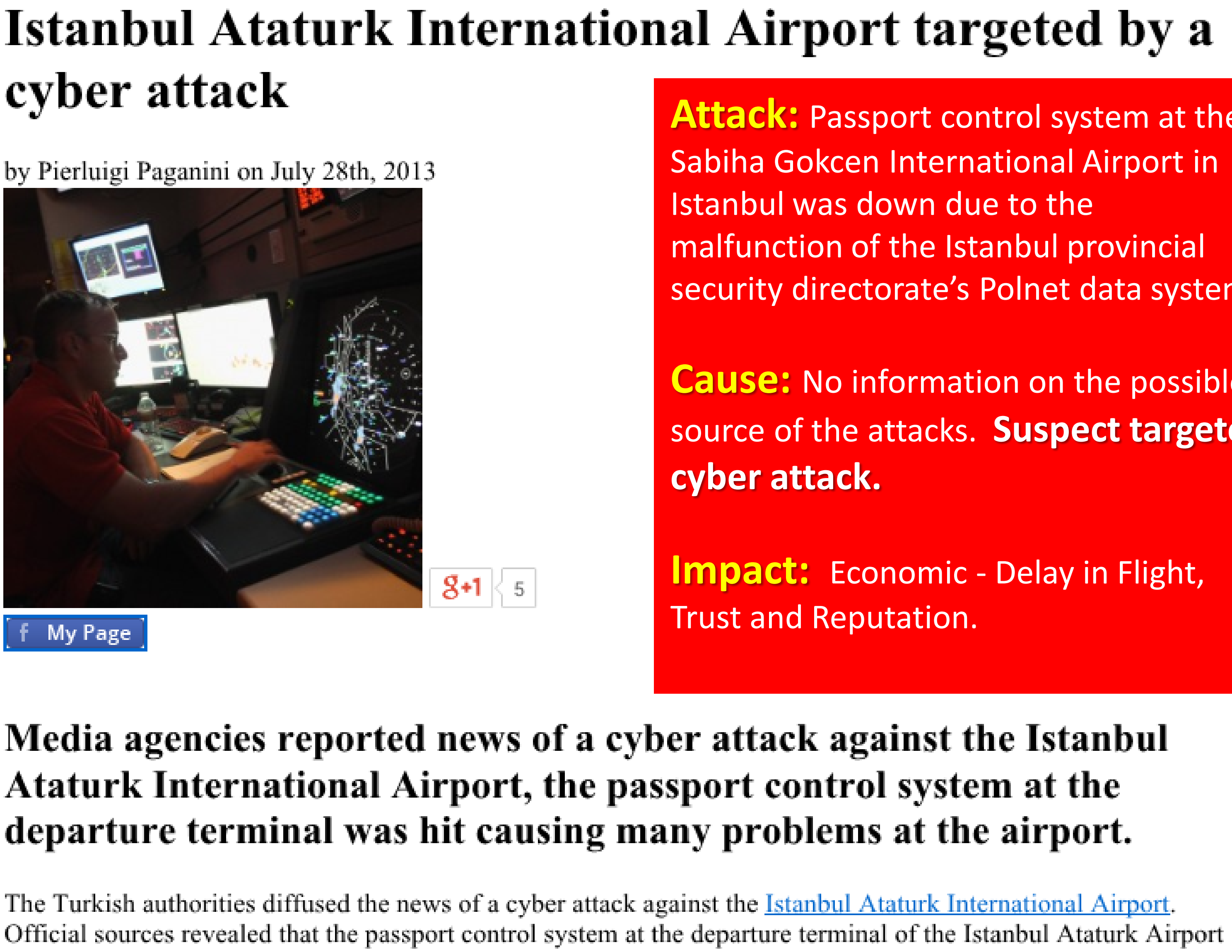
Financial Services

Military

We need to protect our National Critical Infrastructures



Dec 2015: Cyber-attack on Ukraine's electricity distribution network left 225,000 people without power.



Istanbul Ataturk International Airport targeted by a cyber attack

by Pierluigi Paganini on July 28th, 2013

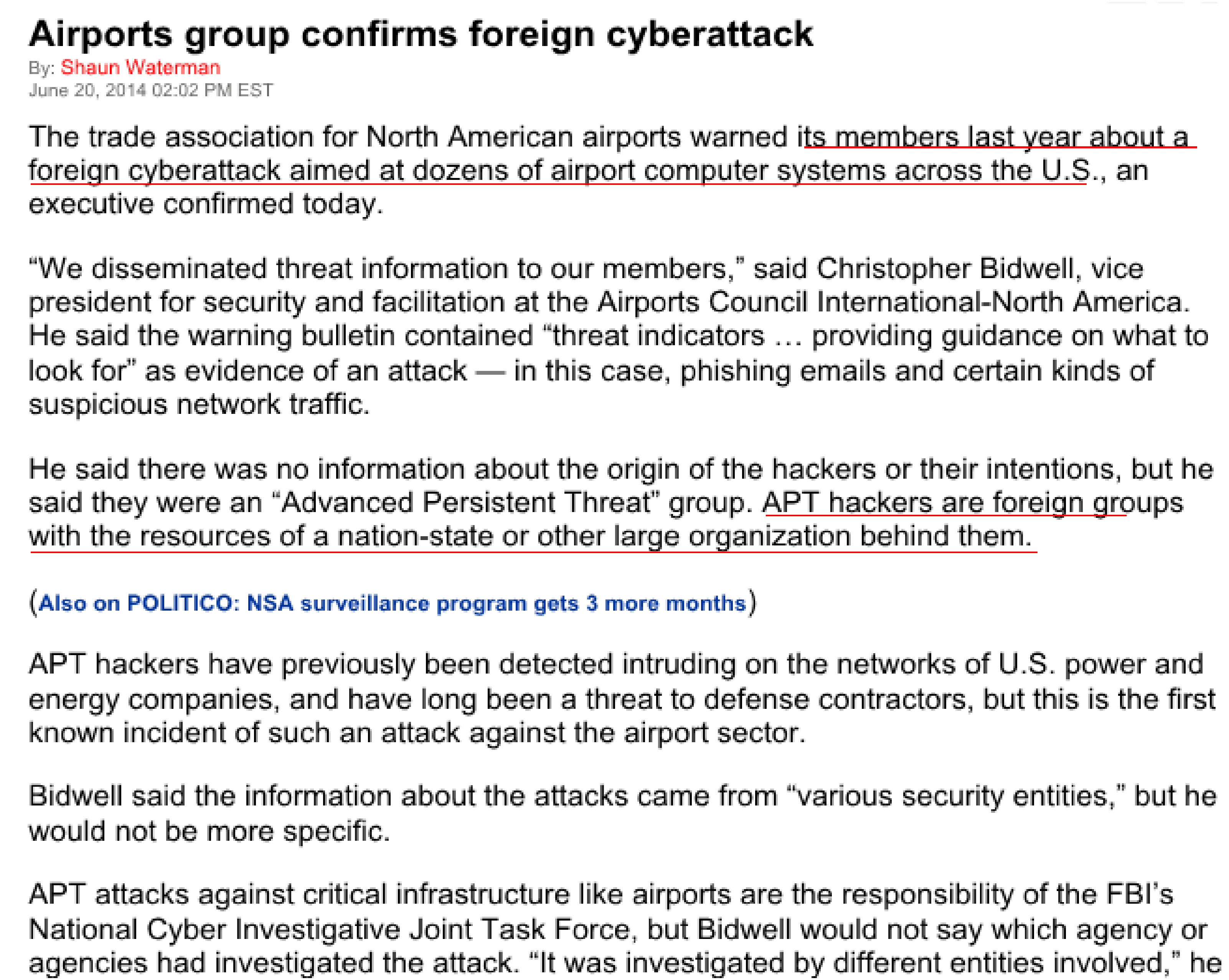
Media agencies reported news of a cyber attack against the Istanbul Ataturk International Airport, the passport control system at the departure terminal was hit causing many problems at the airport.

The Turkish authorities diffused the news of a cyber attack against the [Istanbul Ataturk International Airport](). Official sources revealed that the passport control system at the departure terminal of the Istanbul Ataturk Airport

Attack: Passport control system at the Sabiha Gokcen International Airport in Istanbul was down due to the malfunction of the Istanbul provincial security directorate's Polnet data system.

Cause: No information on the possible source of the attacks. **Suspect targeted cyber attack.**

Impact: Economic - Delay in Flight, Trust and Reputation.



Airports group confirms foreign cyberattack

By: Shaun Waterman
June 20, 2014 02:02 PM EST

The trade association for North American airports warned its members last year about a foreign cyberattack aimed at dozens of airport computer systems across the U.S., an executive confirmed today.

“We disseminated threat information to our members,” said Christopher Bidwell, vice president for security and facilitation at the Airports Council International-North America. He said the warning bulletin contained “threat indicators … providing guidance on what to look for” as evidence of an attack — in this case, phishing emails and certain kinds of suspicious network traffic.

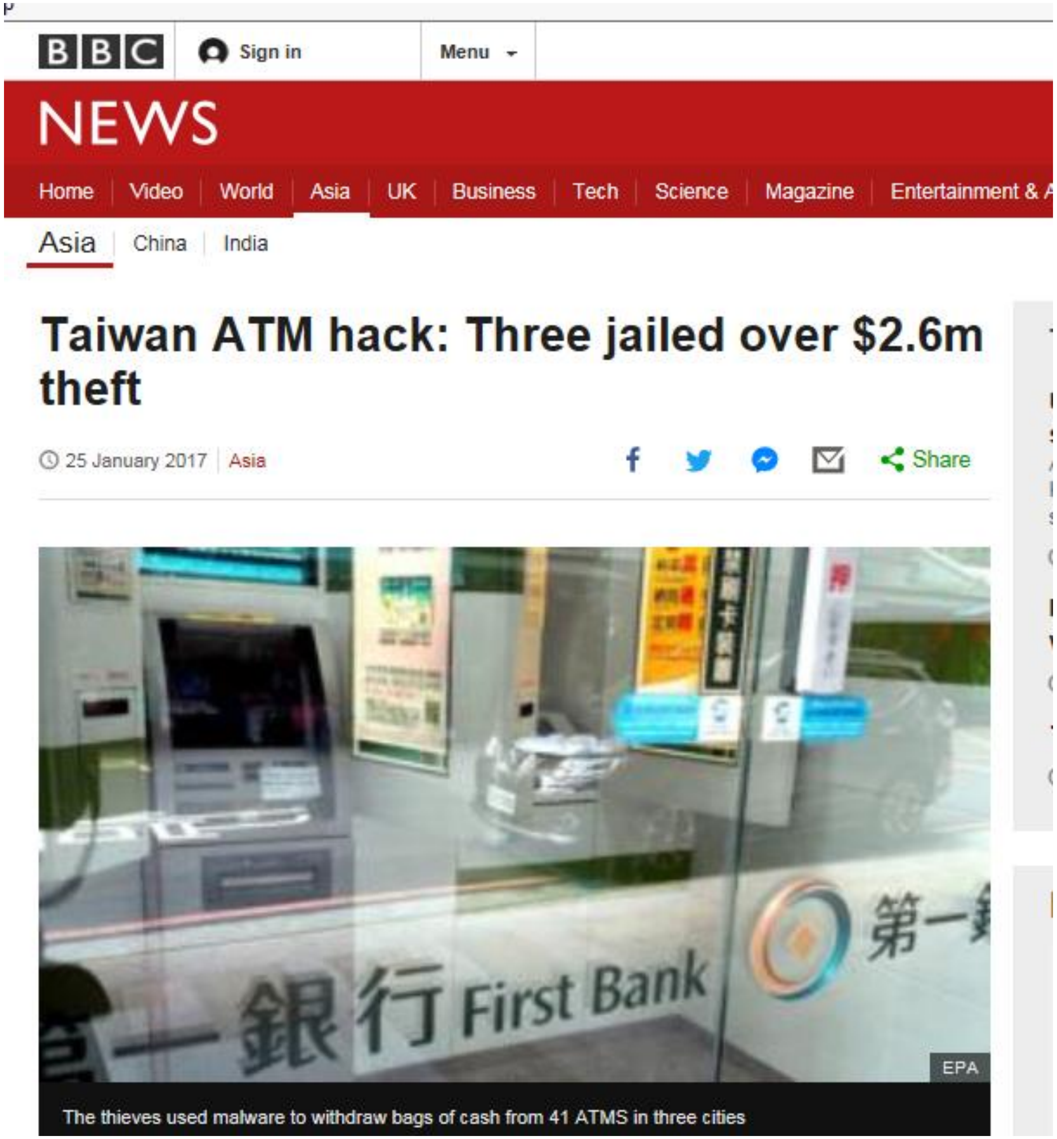
He said there was no information about the origin of the hackers or their intentions, but he said they were an “Advanced Persistent Threat” group. APT hackers are foreign groups with the resources of a nation-state or other large organization behind them.

(**Also on POLITICO: NSA surveillance program gets 3 more months**)

APT hackers have previously been detected intruding on the networks of U.S. power and energy companies, and have long been a threat to defense contractors, but this is the first known incident of such an attack against the airport sector.

Bidwell said the information about the attacks came from “various security entities,” but he would not be more specific.

APT attacks against critical infrastructure like airports are the responsibility of the FBI’s National Cyber Investigative Joint Task Force, but Bidwell would not say which agency or agencies had investigated the attack. “It was investigated by different entities involved,” he



Taiwan ATM hack: Three jailed over $2.6m theft

25 January 2017 | Asia

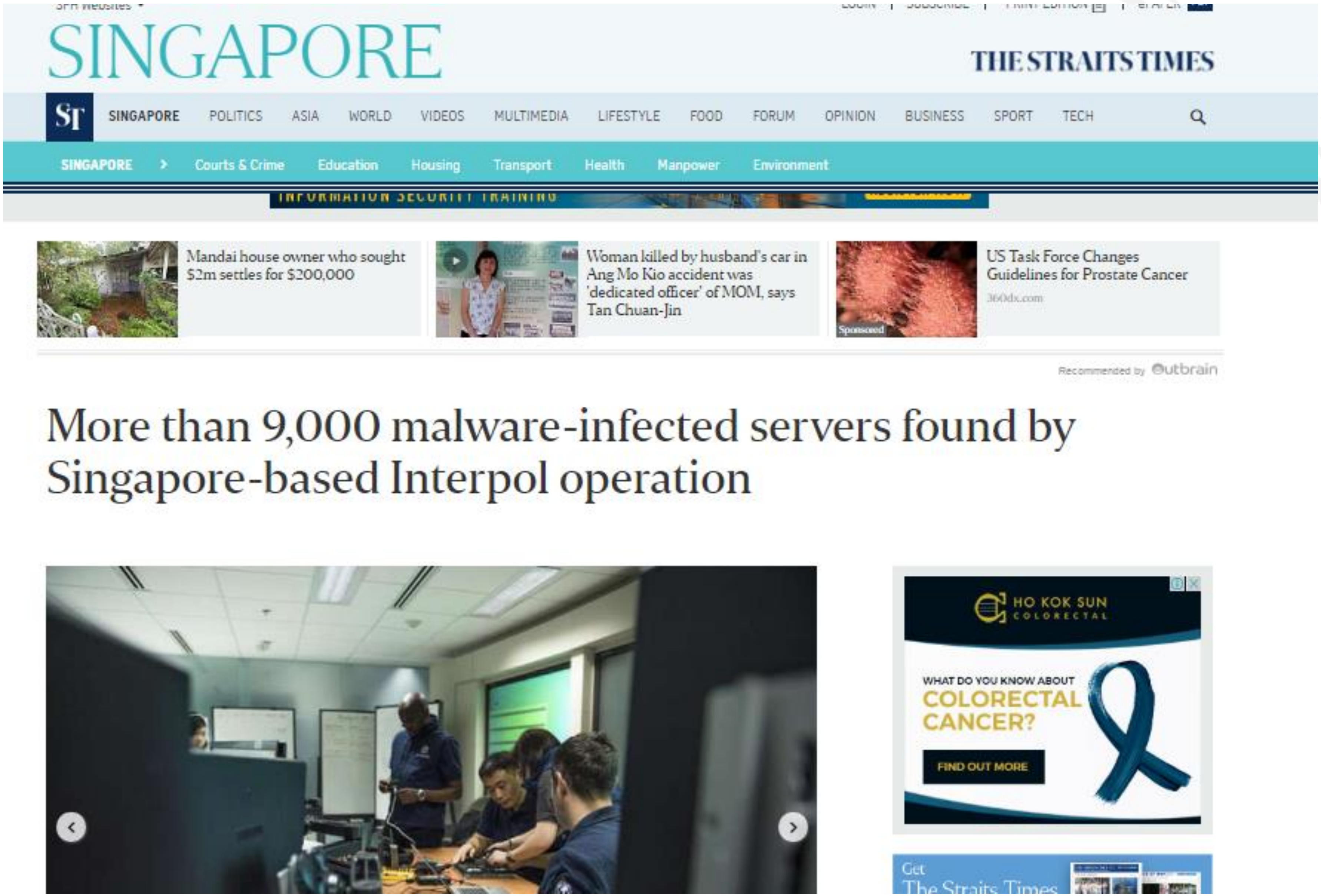
The thieves used malware to withdraw bags of cash from 41 ATMS in three cities

The thieves used malware to withdraw bags of cash from 41 ATMS in three cities.

In response to the heist, banks temporarily froze withdrawals from more than 1,000 cash machines.

3 were all convicted by a Taipei court.

19 suspects, including one French national and one Australian, are believed to have fled Taiwan.



SPH Websites ▾

LOGIN | SUBSCRIBE | PRINT EDITION | ePAPER

SINGAPORE

THE STRAITS TIMES

Mandai house owner who sought $2m settles for $200,000

Woman killed by husband's car in Ang Mo Kio accident was 'dedicated officer' of MOM, says Tan Chuan-Jin

More than 9,000 malware-infected servers found by Singapore-based Interpol operation

Findings

- **8,800 servers across eight countries in the Asean region which were acting as command and control points, which are systems used to control and spread malicious software known as malware.**
- **Affected servers were involved in targeting financial institutions, spreading ransomware, launching Distributed Denial of Service (DDoS) attacks and distributing spam.**
- **270 websites from the Asean region infected with a malware code which exploited a vulnerability in the website design application.**
- **Among them were several government websites which may have contained personal data of their citizens.**

Public and Private sectors across ASEAN together in combating cybercrime

PUBLISHED BY THE STRAIT TIMES
APR 24, 2017

RAND Study Examines 200 Real-World 'Zero-Day' Software Vulnerabilities

”RAND researchers have determined that zero-day vulnerabilities have an average life expectancy—the time between initial private discovery and public disclosure—of 6.9 years. That long timeline plus low collision rates—the likelihood of two people finding the same vulnerability (approximately 5.7 percent per year)—means the level of protection afforded by disclosing a vulnerability may be modest and that keeping quiet about—or “stockpiling”—vulnerabilities may be a reasonable option for those entities looking to both defend their own systems and potentially exploit vulnerabilities in others'.”

Media Resources

RAND Office of Media Relations

(703) 414-4795
(310) 451-6913
media@rand.org

Researcher Spotlight

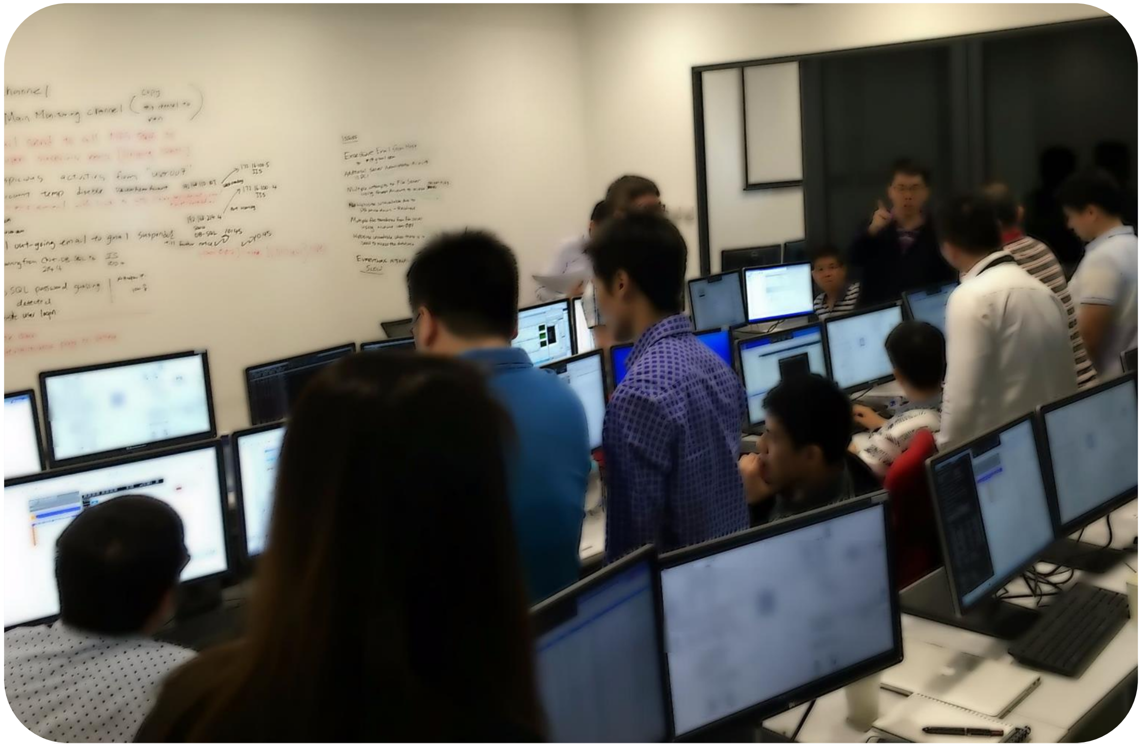
Lillian Ablon
Information Scientist

Lillian Ablon is an information scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School. She conducts technical and policy research on topics spanning cyber security, emerging

The odds is against the defender in countering Cyber Threats.

- Challenges
  - Growing attack surfaces and evolving threat sophistication and players.
  - Attackers are often better resourced because the ROIs of their efforts are easier to quantify.
    - Financial Returns
    - New Dimension of Warfare to secure their country's National Interest.
  - Defender often have too much to protect and limited resources to ensure the security.
- How do we fight cyber and optimize?
  - Collaborate at National level to give our self superior situation awareness . Build strategic depth and have sizable and effective reserve to deal with unexpected incident.
  - Share information to help yourself.
  - Collaboration allow you to optimise your dollars and avoid duplication.

People is central to cyber defence, invest in their training



ST Electronics
Info-Security
A member of ST Engineering

Thank You

ENGINEERING
WITH PASSION

Empowering thru' Innovation

I AWARD