

# Segurança da Informação

Professor: Raphael Machado

Motivação



# Sibéria, 1982

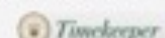
**"Com a cumplicidade dos vizinhos do norte, a CIA inseriu um código malicioso no software da empresa canadense."  
"...o software fez com que uma extremidade da bomba trabalhasse na taxa máxima, enquanto que na extremidade oposta outra válvula fechasse... maior explosão não nuclear já registrada..."**

Cyberwar

## War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

Jul 1st 2010 | From the print edition

 Timekeeper

 Like

561

 Tweet



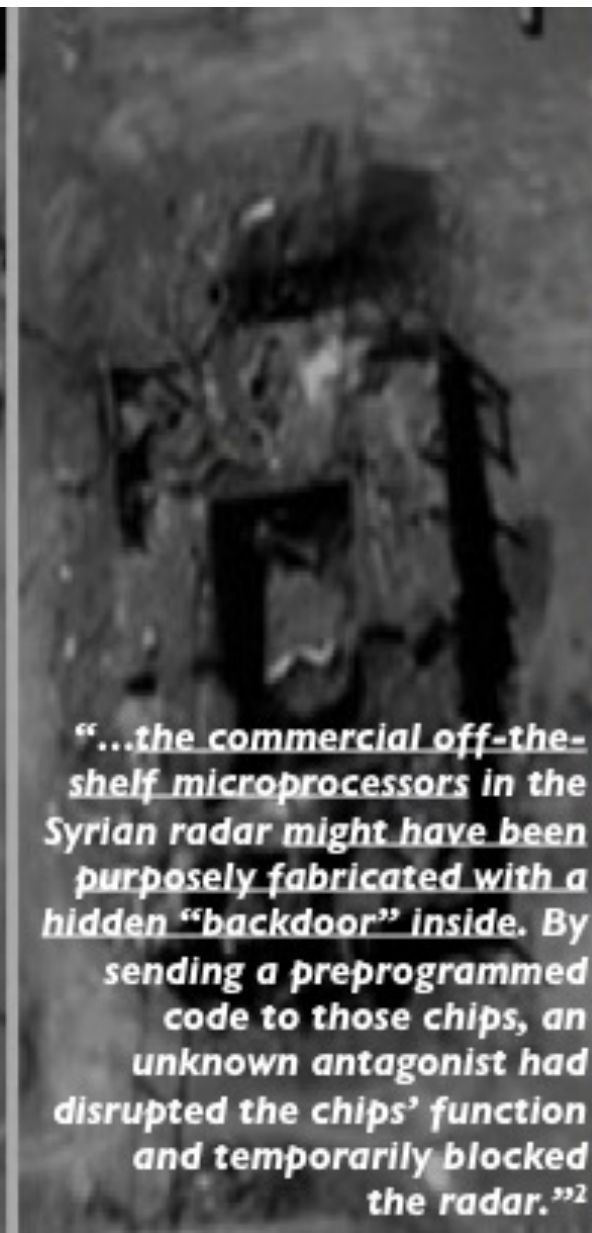
Matt Murphy

AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, "was the most monumental non-nuclear explosion and fire ever seen from space."

Síria, 2007



U.S. GOVERNMENT



***“...the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar.”<sup>2</sup>***

ANNALS OF WAR

SEPTEMBER 17, 2012 ISSUE

## THE SILENT STRIKE

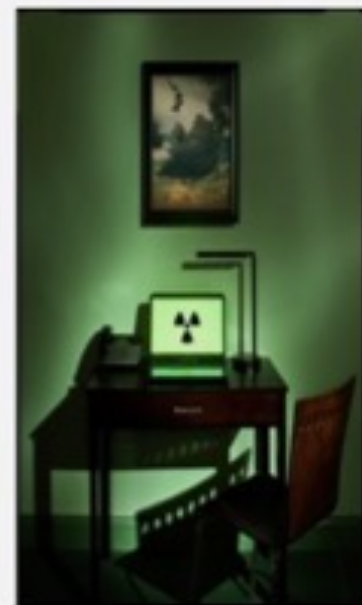
*How Israel bombed a Syrian nuclear installation and kept it secret.*

BY DAVID MAKOVSKY

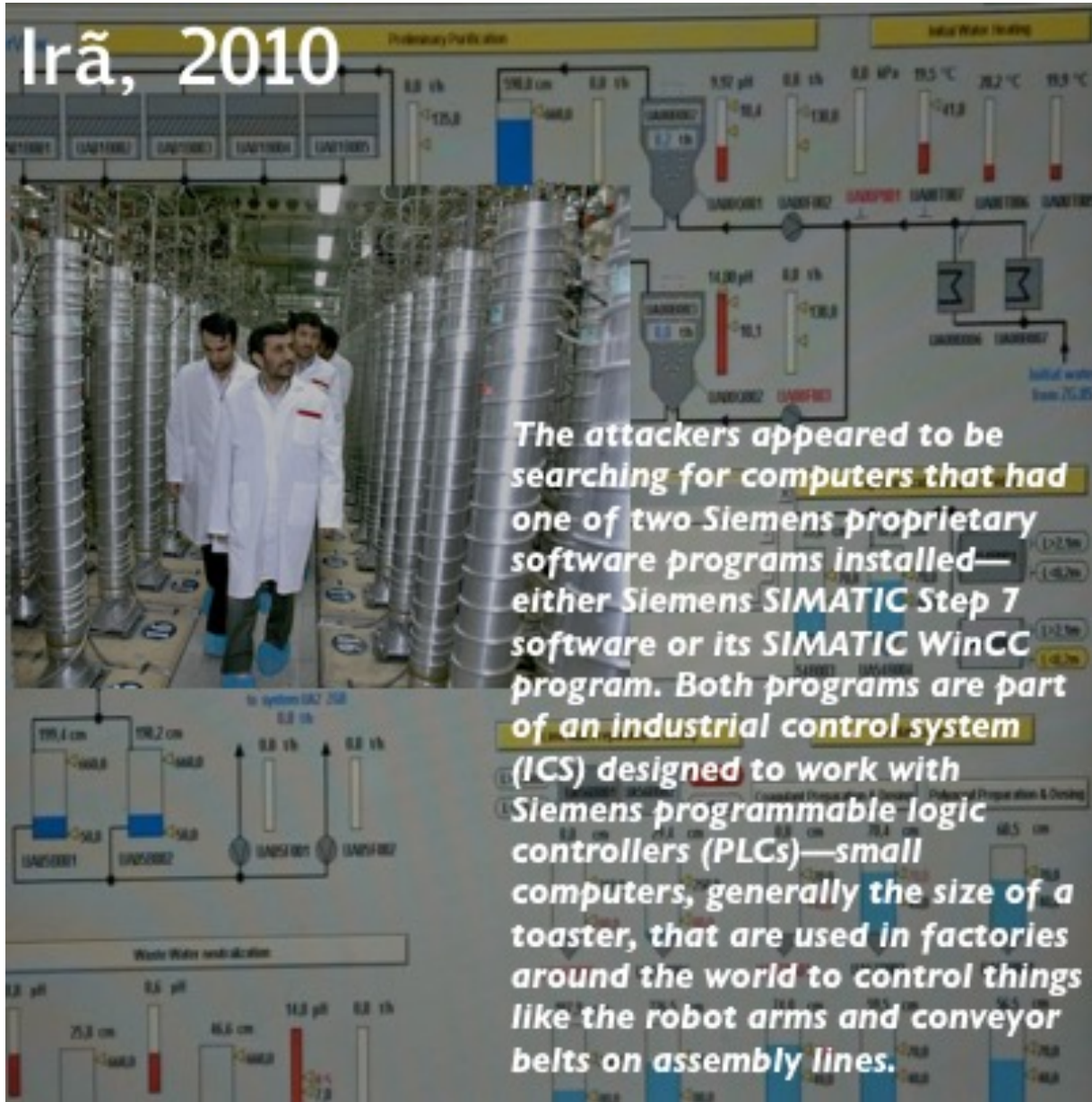
*The Mossad extracted evidence of the nuclear site from the computer of a Syrian official.*

PHOTOILLUSTRATION BY DAN WINTERS.

In the first days of March, 2007, agents from the Mossad, the Israeli intelligence agency, made a daring raid on the Vienna home of Ibrahim Othman, the head of the Syrian Atomic Energy Commission. Othman was in town attending a meeting of the International Atomic Energy Agency’s board of governors, and had stepped out. In less than an hour, the Mossad operatives swept in, extracted top-secret information from Othman’s computer, and left without a trace.



Irã, 2010



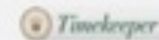
The attackers appeared to be searching for computers that had one of two Siemens proprietary software programs installed—either Siemens SIMATIC Step 7 software or its SIMATIC WinCC program. Both programs are part of an industrial control system (ICS) designed to work with Siemens programmable logic controllers (PLCs)—small computers, generally the size of a toaster, that are used in factories around the world to control things like the robot arms and conveyor belts on assembly lines.

Cyberwar

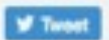
## The meaning of Stuxnet

A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar

Sep 30th 2010 | From the print edition



265



IT HAS been described as "amazing", "groundbreaking" and "impressive" by computer-security specialists. The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals (see [article](#)). It is designed to infect a particular configuration of a particular type of industrial-control system—in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target.

EUA, 2016



ANDY GREENBERG SECURITY 07.21.15 06:00 AM

# HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



# EUA/Alemanha, 2016



### Former Audi boss charged in VW dieselgate scandal

© 31 July 2015

Read emissions scandal



Rupert Stadler was arrested last year

German authorities have charged the former boss of Audi with fraud as part of an investigation into the VW emissions-cheating scandal.

# EUA, 2016

ECC

This Exhibit is SECRET//NOFORN

	FY 2011 <sup>1</sup> Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 - FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding (\$M)	290.6	275.4	--	275.4	234.9	--	234.9	-20.4	-7
Civilian FTE	144	143	--	143	141	--	141	-2	-1
Civilian Positions	144	143	--	143	141	--	141	-2	-1
Military Positions	--	--	--	--	--	--	--	--	--

<sup>1</sup>Includes several OCO funding. Totals may not add due to rounding.

Trapdoor

A → B ✓  
A ← \* B



HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition

The New York Times Search All NYTimes.com

**U.S.**

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

POLITICS | EDUCATION | TEXAS

## Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break. [Related Article](#)

[Excerpt from 2013 Intelligence Budget Request](#) | [Bulfinch Briefing Sheet](#)

This excerpt from the N.S.A.'s 2013 budget request outlines the ways in which the agency circumvents the encryption protection of everyday Internet communications. The Signal Enabling Project involves industry relationships, clandestine changes to commercial software to weaken encryption, and lobbying for encryption standards it can crack.

# EUA, 2016



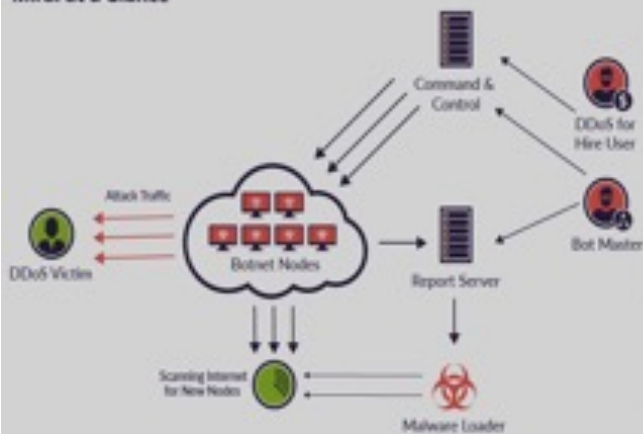
BIZ & IT

## DoS attack on major DNS provider brings Internet to morning crawl [Updated]

Dyn's US East region hit hardest in attack that affected Twitter, Reddit.

SEAN GALLAGHER - 10/21/2016, 11:59 AM

Mirai at a Glance

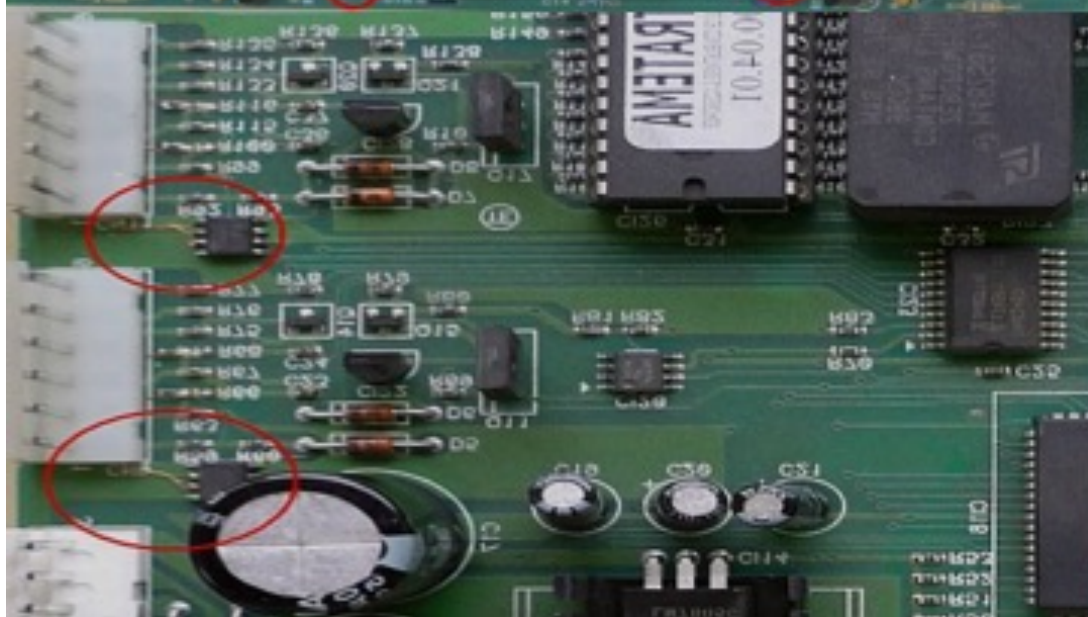
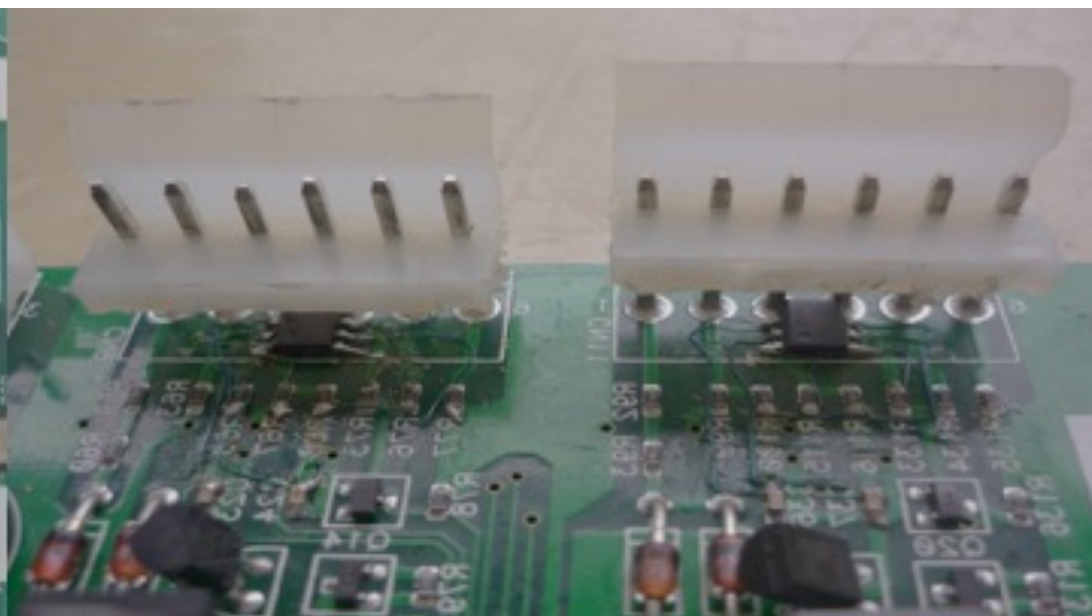


WikiLeaks  
Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point.  
2:09 PM - 21 Oct 2016



# Brasil, 2016

Os esquemas de fraude acompanharam o avanço da tecnologia, tornando-se mais sofisticados. Especialistas em informática violam o lacre da bomba e instalam um microprocessador (chip) que altera o seu giro e, conseqüentemente, o valor a ser pago.



**Quadrilhas usam chips para alterar volume em bombas de combustível**

Fiscalizações apontam aumento de fraudes

Ramona Oliveira  
28/06/2017 - 04:30 / Atualizado em 28/06/2017 - 08:28

# Ciber-Segurança versus Negócios

---

- Negócios
  - Objetivos palpáveis: lucro, crescimento, estratégia
  - Acessível a seres humanos "normais", "saudáveis" e "sociáveis"
  - Imagem clássica do executivo bem-sucedido
- Segurança/Tecnologia
  - Trabalho para gênios antissociais
  - Difícil compreensão para quem não é da área
  - Imagem clássica do nerd/geek



Imagem "clássica" de um ambiente de negócios...



Ambiente "tecnológico"...





## Pergunta "motivacional"


- Você já teve "vazados" dados pessoais?
  - Número do cartão de crédito
  - Informações médicas
  - Casos de propaganda direcionada

## Falácia dos dois “tipos” de organização

Existem dois “tipos” de organização:  
as que sofreram um vazamento de informações  
e as que ainda vão sofrer...



Falácia costuma ser estendida  
a todo tipo de ciberataque



## Vazamento de dados da Target

---

- Nov-Dez/2013: 40 milhões de números de cartão e 70 milhões de registros pessoais
- Queda de 40% nos lucros do 4º Tri
- Queda nas ações da empresa



May 26, 2017



## Cost of 2013 Target Data Breach Nears \$300 Million

With Latest Settlement, the Cost of the 2013 Target Data Breach Nears \$300 Million

Here is a list of settlements made as a result of the 2013 Target data breach:

- **\$10 million** paid in a class action lawsuit to affected consumers in March 2015.
- **\$19 million** paid to Mastercard in an April 2015 settlement.
- **\$67 million** paid to Visa in August 2015.
- **\$39.4 million** paid to banks and credit unions for losses and costs related to the breach, in a December 2015 settlement.
- And now **\$18.5 million** in this weeks settlement.

All those settlements total \$153.9 million dollars.

In Target's **2016 annual financial report** they reported that the total cost of the breach was:

**\$292 million dollars.**<sup>[1]</sup>





## Vazamento da Sony

- 11 de abril de 2011: dados de 77 milhões de contas vazados, incluindo cartões de crédito
- 171 milhões de dólares de custo total



# Sony PlayStation suffers massive data breach

Liana B. Baker, Jim Finkle

5 MIN READ



NEW YORK/BOSTON (Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

## Massive hack blows crater in Sony brand

By Julianne Peptone, staff reporter @CNBMoneyTech May 10, 2011 5:01 AM ET



NEW YORK (CNBMoney) — It's been a nightmarish three weeks for Sony, as it struggles to recover from massive hack attacks on three separate gaming systems it runs. Not only are the PlayStation, Qriocity and Sony online gaming networks still offline, but tens of millions of credit card numbers may have been stolen.

### NEWS

#### Technology

## Q&A: How does Sony breach affect customers?

3 May 2011



Sony has revealed that the personal information of millions of users on the PlayStation Network (PSN) and Sony Online Entertainment (SOE) system may have been stolen.

The online services hold a wealth of information on its users, including their name, home address, date of birth and credit card number.

Many users have expressed concern that they will now become the target of online fraud or e-mail scams.



# In Sony's 20th Breach In Two Months, Hackers Claim 177,000 Email Addresses Compromised



Andy Greenberg Forbes Staff

Security

Covering the worlds of data security, privacy and hacker culture.

Sony's unprecedented spree of security breaches in the last two months may be finally cooling off, as profit- and attention-seeking hackers move on to other vulnerable targets. But it's not quite over yet.



#### Business

## PlayStation Network breach will cost Sony \$171m

### And counting

By Dan Goodin 24 May 2011 at 05:00

12 SHARE



## The PlayStation Network breach (FAQ)

A rundown of what we know so far: how PSN got hacked, what Sony is doing about it, whether credit cards were stolen, and how the company is trying to regain the trust of its customers.

BY DAN GOODIN | MAY 24, 2011 5:00 AM EDT



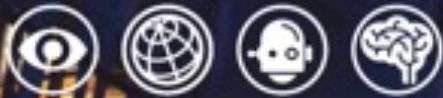
# Maiores Vazamentos da História Recente



# Custos do Cibercrime

- Estimativa de US\$445bi a US\$600bi (McAfee)
  - Em 2014, era de US\$345bi a US\$445bi
  - Significa quase 1% do PIB mundial (!)
- Custo anual estimado em US\$6tri em 2021 (Cybersecurity Ventures)
- Custo médio de ciberataques em US\$17,1mi (Accenture)
- Segunda fonte mundial de crimes e fraudes (PwC)

World (2017)  
80.738  
Trillion



## What are the most common types of reported economic *crime* and *fraud*?



Asset  
misappropriation  
45%

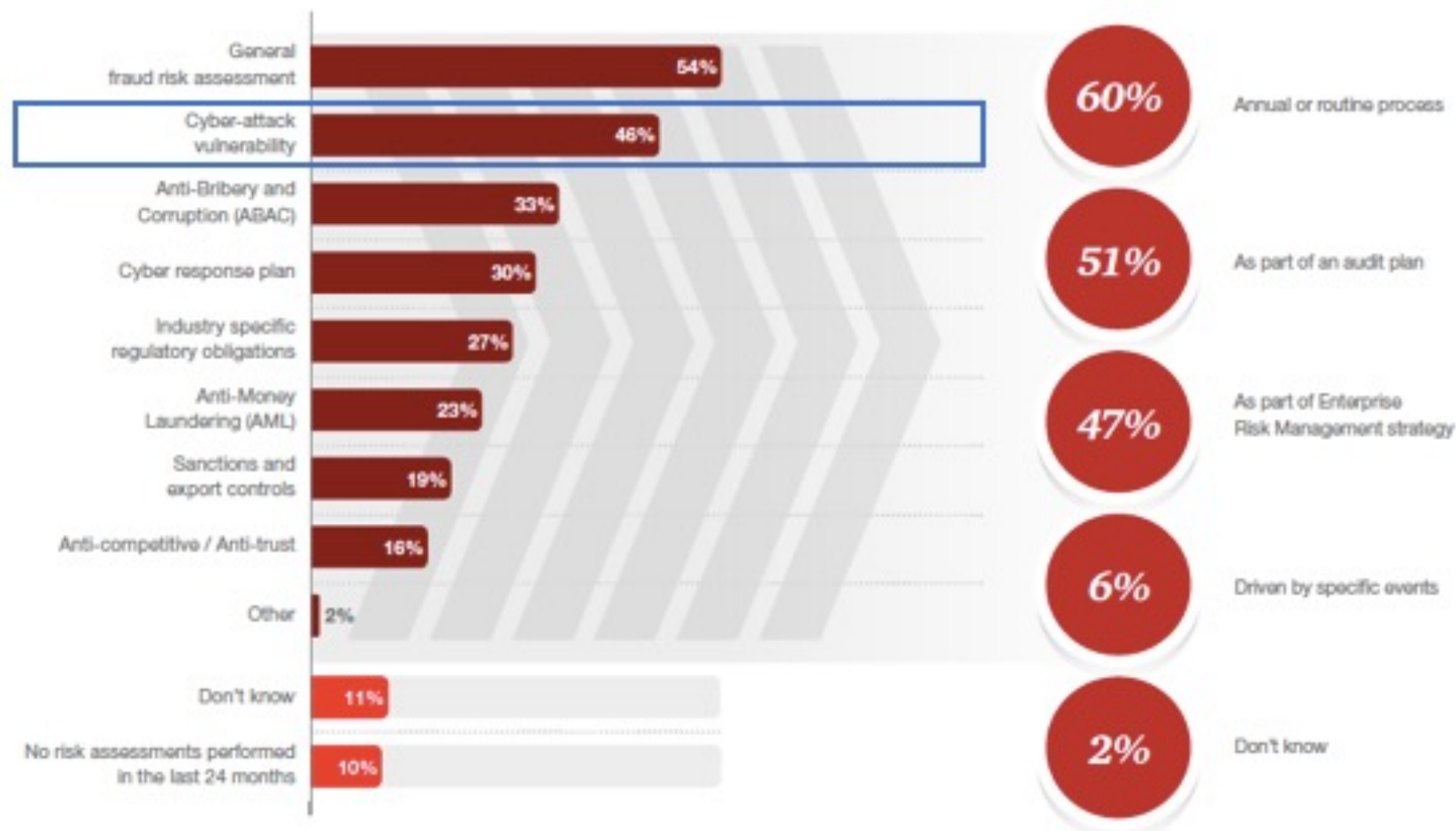


Cybercrime  
31%



Fraud committed  
by the consumer  
29%

**Exhibit 4: Less than half of all organisations have performed targeted risk assessments in the last 2 years**



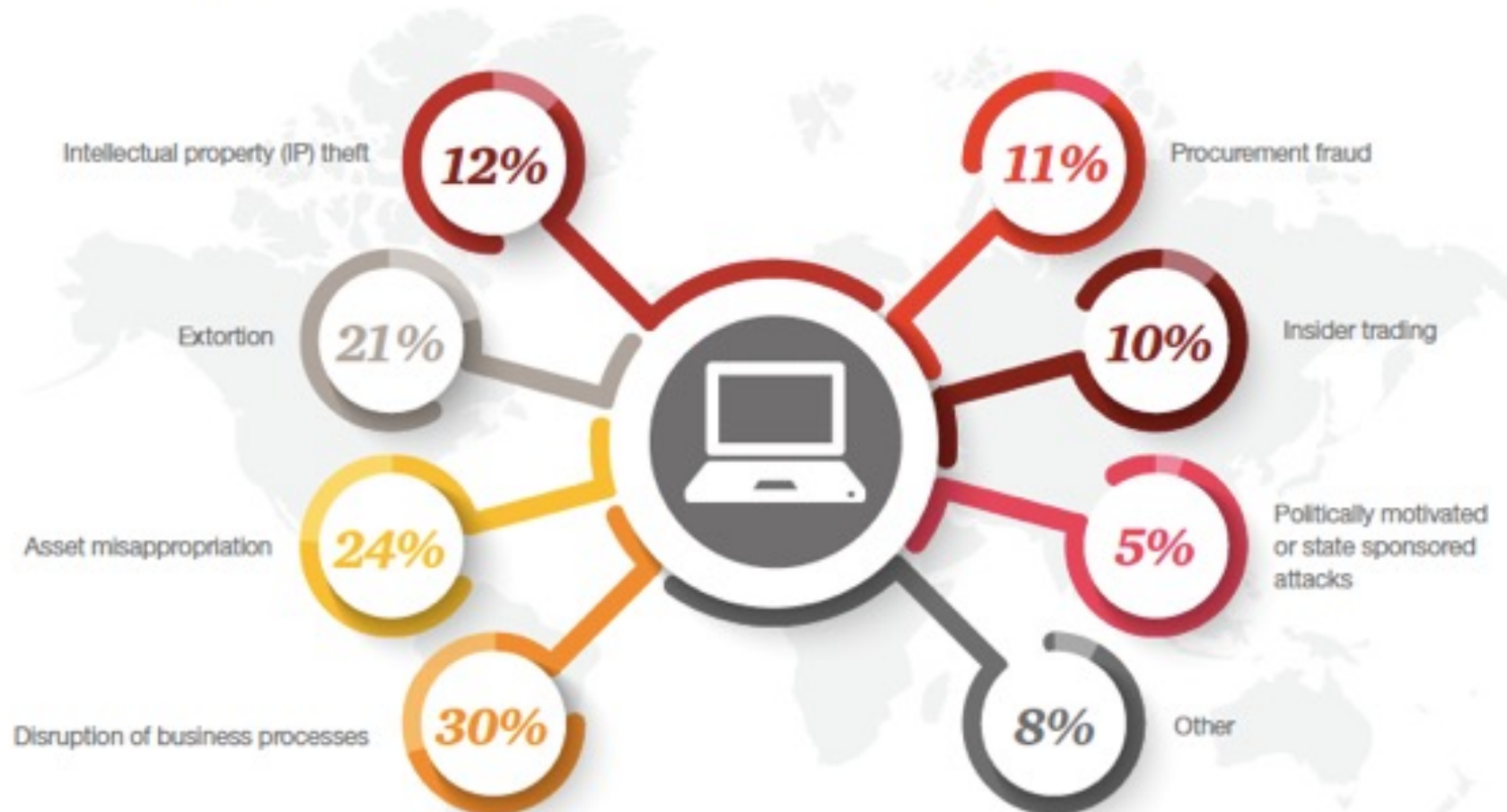
**Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?**

Source: PwC's 2018 Global Economic Crime and Fraud Survey

**Q. What prompted your organisation to perform a risk assessment?**

Source: PwC's 2018 Global Economic Crime and Fraud Survey

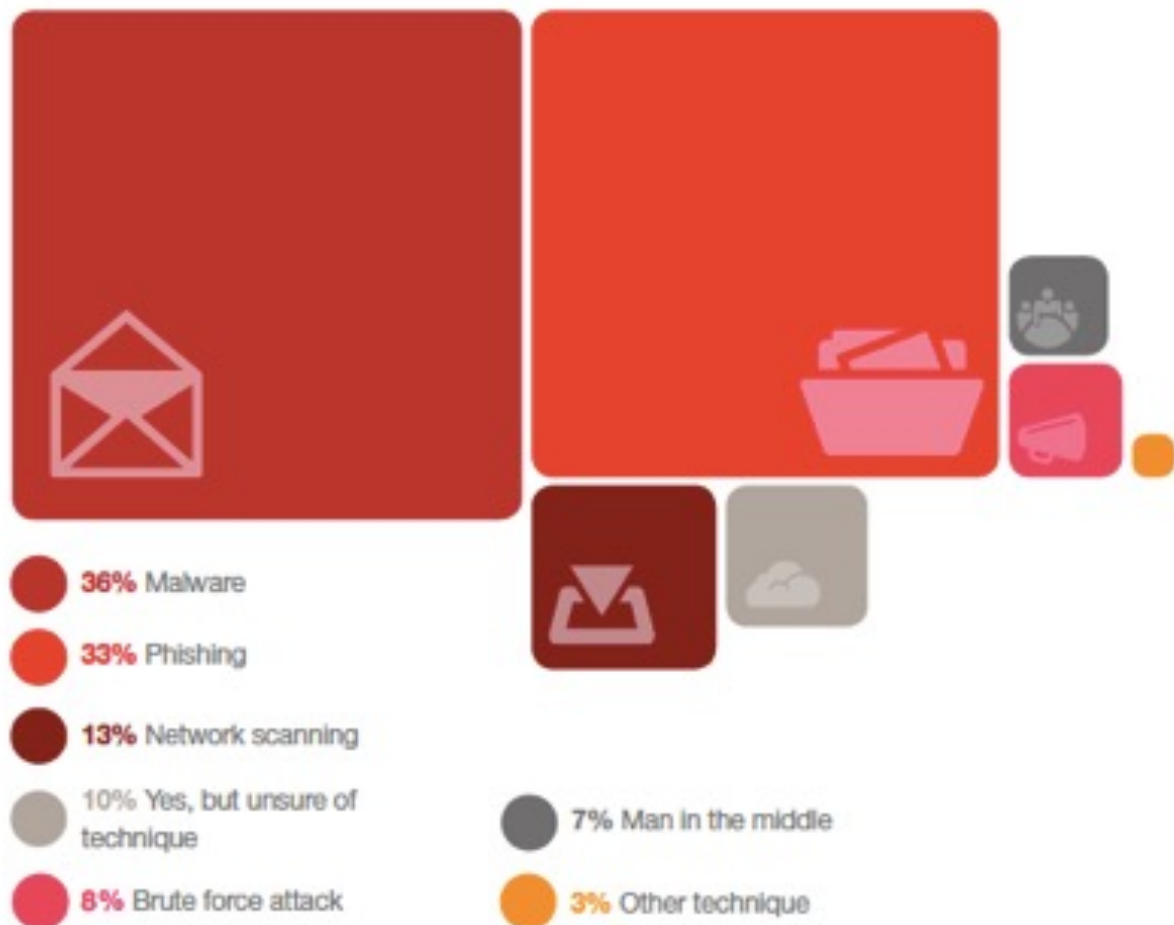
**Exhibit 17: Types of fraud that organisations were a victim of through a cyber-attack**



**Q. Which of the following types of fraud and/or economic crime was your organisation victim of through a cyber-attack?**

Source: PwC's 2018 Global Economic Crime and Fraud Survey

## Exhibit 18: Cyber-attack techniques used against organisations



Q. In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Over a third of all respondents have been targeted by cyber-attacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: 24% of respondents who were attacked suffered asset misappropriation and 21% were digitally extorted.



# Contents

---

## **6 Foreword**

---

## **8 Overview of economic crime**

---

## **14 Cybercrime**

---

- 15 A boundless threat
- 16 High-level statistics
- 18 Key insights
- 25 Key contacts

## **26 Ethics & compliance**

---

- 27 Aligning decision-making with values
- 28 High-level statistics
- 30 Key insights
- 39 Key contacts

## **40 Anti-money laundering**

---

- 41 Money laundering destroys value
- 42 High-level statistics
- 44 Key insights
- 51 Key contacts

## **52 Appendices**

---

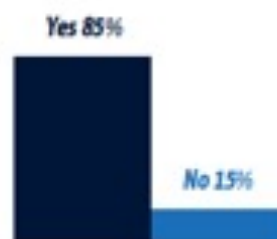
- 52 Participation statistics
- 54 Looking for more data?
- 55 Contributors

More than three in five board members say they are both significantly or very "satisfied" (64%) and "inspired" (65%) after the typical presentation by IT and security executives about the company's cyber risk.



yet the majority (85%) of board members believe that IT and security executives need to improve the way they report to the board.

Do you think IT and security executives need to improve the way they report to the board?



Board reconhece importância da Cibersegurança...  
...mas reports precisam melhorar

Even though 70% of board members surveyed report that they understand everything that they're being told by IT and security executives in their presentations



more than half (54%) agree or strongly agree that the data presented is too technical.

## How Boards of Directors Really Feel About Cyber Security Reports

Based on an Osterman Research survey



*The information that IT and security executives provide to the board is too technical*



Agree/Strongly Agree	54%
Neutral Or Nearly So	42%
Disagree/Strongly Disagree	4%

Despite 70% of board members indicating that they understand everything that they're being told by IT and security executives in their presentations, more than half (54%) also agree or strongly agree that reports are too technical. The contradiction shows while some board members think they understand the data presented to them, that may not necessarily be the case.

IT and security executives should not be surprised by the finding. Based on our previous survey, only one-third of IT and security executives believe the board comprehends the cyber security information they provide.

Some of the information that could be "too technical" for board members could be the top two featured in the most common types of information they say IT and security executives report. **According to board members, the top three common types of information reported include:**

1. A complete list of vulnerabilities within the organization,
2. Details on data loss, and
3. Downtime caused by data breach incidents.

Em resumo...  
ciber-  
segurança é  
questão de  
negócio

To whom does the CISO, CSO, or equivalent senior information security executive directly report?



CEO



Board of Directors



CIO  
(Chief Information Officer)



CSO  
(Chief Security Officer)



Chief Privacy Officer

Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 18, 2017.  
Base: 9,500 respondents

Riscos, riscos,  
riscos...

*On a scale of 1 to 7, what is the priority in addressing each of the following risks for the company, where 1 is "lowest priority" and 7 is "highest priority"?*



Cyber risks	5.60
Financial risks	5.54
Regulatory risks	5.40
Competitive risks	5.36
Legal risks	5.36

Ciber-  
segurança  
significa  
"negócios"

## Board Engagement, Comprehensive Data Policies Distinguish High-Performing Information Security Programs

Based on our analysis, there are two critical success factors present in organizations that adhere to security and privacy best practices:

- High levels of engagement and understanding by the board of directors regarding information security risks
- Having all five "core" information security policies in place

In other Protiviti research, we have observed this correlation between board engagement in information security and the overall security posture of the organization, including in our 2015 IT Security and Privacy Survey report.<sup>3</sup> Similarly, our results this year

show a notable difference between organizations that have all "core" information security policies in place — specifically, a records retention/destruction policy, a written information security policy, an acceptable use policy, a data encryption policy, and a social media policy — and those that do not; the former organizations demonstrate stronger information security practices overall.

Throughout our report, we compare the results from these two groups of companies that exhibit the above success factors (which we categorize as "top-performing organizations") with companies that do not exhibit them, and pinpoint notable gaps.

Ciber-  
segurança  
significa  
"negócios"

• • • *How engaged is your board of directors with information security risks relating to your business?*

	All respondents		Large Companies (≥ \$1B)		Small Companies (< \$1B)	
	Current	2015	Current	2015	Current	2015
High engagement and level of understanding by the board	33%	28%	37%	32%	26%	24%
Medium engagement and level of understanding by the board	37%	32%	37%	33%	39%	33%
Low engagement and level of understanding by the board	12%	15%	9%	11%	20%	19%
Don't know	18%	25%	17%	24%	15%	24%

• • • *Which of the following policies does your organization have in place? (Multiple responses permitted)*

	All respondents		Large Companies (≥ \$1B)		Small Companies (< \$1B)	
	Current	2015	Current	2015	Current	2015
Acceptable use policy	80%	77%	82%	82%	77%	72%
Record retention/destruction policy	78%	74%	81%	80%	72%	71%
Data encryption policy	70%	67%	77%	79%	60%	58%
Written information security policy (WISP)	69%	66%	72%	72%	65%	60%
Social media policy	59%	55%	61%	61%	53%	50%

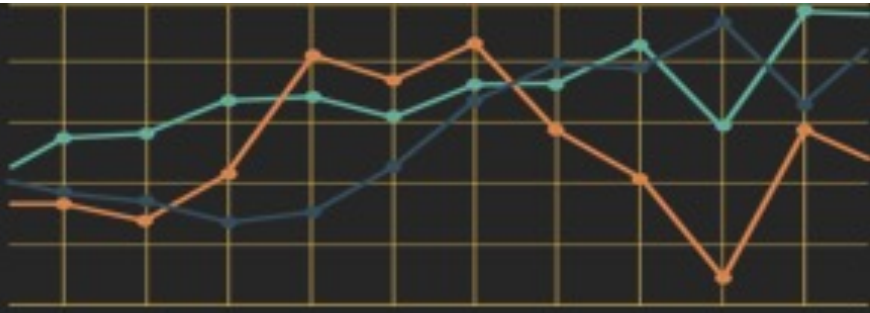
Objetivo, então, é...

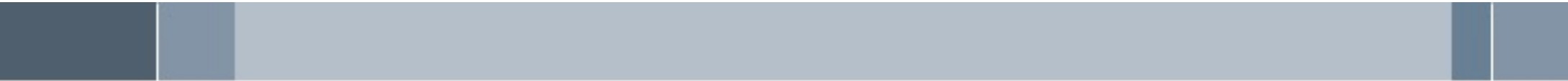




COMMUNICATION PROTECTION  
MEASURES RULES FIREWALL  
WEB LAYER **INTERNET** DOS INFORMATION  
SECURE SERVICES  
COMPUTER **SECURITY** TOKEN  
ANTIVIRUS FRAUD DATA  
MALICIOUS INTRUSION ATTACKS  
TRANSFER DDOS CONTROL  
PROTOCOL **NETWORK** ENCRYPTION  
VPN ACCESS  
BROWSER







# Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

## 1.2: Segurança e Sociedade





## Impacto da (falta de) segurança na Sociedade

- › Vazamento de informações sensíveis
- › Perdas Financeiras
- › Indisponibilidade e falhas de serviços relevantes
- › Segurança/Defesa Nacional
- › Exemplos de Ataques (e ataques e ataques e...)

## Yahoo says all three billion accounts hacked in 2013 data theft

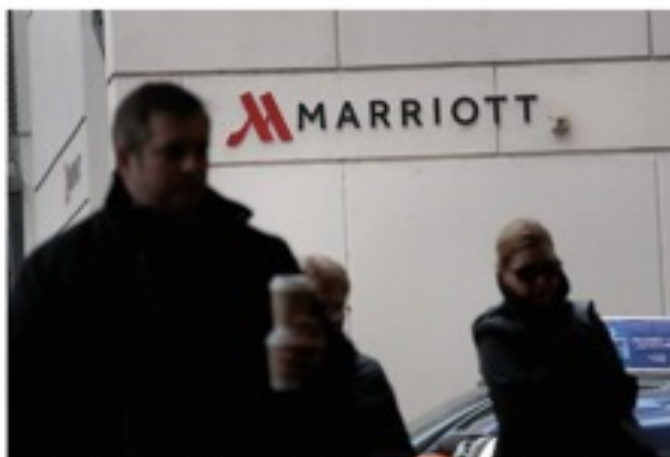
Jonathan Stempel, Jim Finkle

LINK READ

(Reuters) - Yahoo on Tuesday said that all 3 billion 2013 data theft, tripling its earlier estimate of the size in a disclosure that attorneys said sharply increased owner, Verizon Communications Inc (VZ.N).

The New York Times

## Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing



From the first revelation that the Marriott's computer systems had been breached, there was widespread suspicion that the hacking was part of a broad spy campaign to steal Americans' personal data. Scott Olson/Getty Images

By David E. Sanger, Nicole Perrotti, Glenn Thrush and Alan Rappeport

Dec. 11, 2016



## Equifax Data Breach Impacts 143 Million Americans



Lee Mathews Contributor

Security  
Observes, analyzes, and writes about tech. Generally in that order.

## Heartland Payment Systems Suffers Data Breach



Dave Lewis Contributor

cloud and enterprise security

# Vazamentos de Informações: Impactos a Privacidade e Confidencialidade...

Data Breach Nears \$300

of the 2013 Target Data Breach Nears \$300

NEWS

## Adult Friend Finder confirms data breach 3.5 million records exposed

Hacker claiming responsibility has posted 3,526,458 records online

## eBay Suffers Massive Security Breach, All Users Must Change Their Passwords



Gordon Kelly Senior Contributor

I write about technology's biggest companies

TWEET THIS

- all eBay users to urgently change their passwords
- hackers gained access to information including eBay customers' names, their encrypted passwords, email, registered addresses, phone numbers and date of birth

## Sony PlayStation suffers massive data breach

Liana S. Baker, Jim Finkle

LINK READ



## AIDS Trojan or PC Cyborg Ransomware

The AIDS Trojan, also known as the PC Cyborg virus, was the first ever ransomware most of us ever had the opportunity to touch a computer in 1985.

### 'Aids' disk damages host

WASHINGTON, September 24 (AP) — A computer virus that has spread to at least 100,000 computers in the United States and other countries has been identified as the AIDS Trojan, a computer virus that is believed to have been created by a person who used the name AIDS.

The AIDS Trojan is a computer virus that is believed to have been created by a person who used the name AIDS. It is a computer virus that is believed to have been created by a person who used the name AIDS.



Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: 85595756-2895577-

The price of 365 user applications is \$25289. The price of a lease for the lifetime of your hard disk is \$25378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$289 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P. O. Box 87-17-94, Panama 3, Panama.

Press ENTER to continue

## CryptoWall Ransomware raised \$325 Million in Revenue for its Developer

October 30, 2015 Mohit Kumar

# CRYPTOWALL RANSOMWARE

## Ransomware: impactos a financeiros...

to raise more than 325 million (325 million) in this past year alone.



- You should register Bitcoin wallet [click here for more information with pictures]
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day. Here are our recommendations:
  - LocalBitcoins.com (USA) - Buy Bitcoins with Western Union
  - Coinbase.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order, In NYC: Bitcoin ATM, In Person
  - LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
  - Bitdirect.eu - THE BEST FOR EUROPE
  - cryptos.com - Another fast way to buy bitcoins
  - Bitstamp.eu - Buy Bitcoins Instantly for Cash
  - How To Buy Bitcoins - An international directory of bitcoin exchanges.
  - Cash Into Coins - Buy on for cash.
  - CoinJar - CoinJar allows direct bitcoin purchases on their site.
  - Bitfury.com
  - Bitcoind.com
  - ZpZap - ZpZap is a global cash payment network enabling consumers to pay for digital currency.
- Send 1.75 BTC to Bitcoin address:
- Enter the Transaction ID and select amount.
 

Transaction ID:  1.75 BTC == 790.160

Note: Transaction ID - you can find in detailed info about transaction you made. (example 442146a2d64f2308000226c4005479a27c42675c9d2a0b11c441d2)
- Please check the payment information and click "PAY".

## 'Bad Rabbit' ransomware strikes Ukraine and Russia

Share

NO "BAD RABBIT" has been found where. see Russian websites, an airport in Ukraine & city, Kiev.

**BAD RABBIT**

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin address to transfer payment. The current price is on the right.

Time left before the price goes up

37:11:19

Price for decryption: 0.05

Enter your personal key or your assigned bitcoin address.

MUST READ: Microsoft: You're being less toxic online but bullying, harassment still rife

## New world record DDoS attack hits 1.7Tbps days after landmark GitHub outage

Memcached denial-of-service attacks are getting bigger by the day, according to new analysis.

By Liam Turgill March 6, 2017

Hacker News users [report](#) the following

- Twitter
- Etsy
- Github
- Soundcloud
- Spotify
- Heroku
- Pagerduty
- Shopify
- Intercom

PCWorld

NEWS REVIEWS HOW-TO VIDEO DEALS BUSINESS LAPTOPS SMARTPHONES HARDWARE SECURITY SOFTWARE GADGETS

Ads by Google

DDoS Attack

DDoS Spotify

A Security Guard

Home / Internet

UPDATED

## Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more

The sound of silence.



By Brad Chacos

Senior Editor, PCWorld OCT 21, 2016 3:04 PM PT

## Ataques DDoS: Impactos à disponibilidade...

## How a cyber attack transformed Estonia

By Damien McGuinness  
BBC News, Tallinn, Estonia

27 April 2017

Facebook Twitter Email Share



...the news - exactly 10 years ago Estonia  
e under attack from this modern form of

It is an event that still shapes the country today.

Head bowed, one fist clenched and wearing a World War Two Red Army uniform, the Bronze Soldier stands solemnly in a quiet corner of a cemetery on the edge of the Estonian capital Tallinn.

Flowers have been laid recently at his feet. It is a peaceful and dignified scene. But in April 2007 a row over this statue sparked the first known cyber-attack on an entire country.

The attack showed how easily a hostile state can exploit potential tensions within another society. But it has also helped make Estonia a cyber security hotshot today.

### From outrage to outrage

Unwelcomed by the Soviet authorities in 1947, the Bronze Soldier was originally called "Monument to the Liberators of Tallinn". For Russian speakers in Estonia he represents the USSR's victory over Nazism.

But for ethnic Estonians, Red Army soldiers were not liberators. They are seen as occupiers, and the Bronze Soldier is a painful symbol of half a century of Soviet oppression.

In 2007 the Estonian government decided to move the Bronze Soldier from the centre of Tallinn to a military cemetery on the outskirts of the city.

The decision sparked outrage in Russian-language media and Russian speakers took to the streets. Protests were exacerbated by false Russian news reports claiming that the statue, and nearby Soviet war graves, were being destroyed.

Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point.



0:00 PM - 21 Oct 2016

# Explosão na Sibéria (1982)

Cyberwar

War in the fifth c

Are the mouse and keyboard the new

Jul 1st 2010 | From the print edition



Sabotagem entre nações...

Guerra cibernética?

AT THE height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia. A missile being fired? A nuclear test? It was, it seems, an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA had tampered with the software so that it would "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds," according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, "was the most monumental non-nuclear explosion and fire ever seen from space."



...a cumplicidade dos  
...nos do norte, a CIA  
...inseriu um código  
...oso no software da  
...presa canadense."  
...ftware fez com que  
...uma extremidade da  
...bomba trabalhasse na  
...taxa máxima, enquanto  
...que na extremidade  
...oposta outra válvula  
...fechasse... maior  
...explosão não nuclear  
...já registrada..."



# Ataque a Fábrica na Síria (Orchard 2007)

ANNALS OF WAR

SEPTEMBER 17, 2012 ISSUE

## THE SILENT STRIKE

*How Israel bombed a Syrian na*

BY DAVID MAKOVSKY

*The Mossad extracted evidence of the nuclear site from the computer of a Syrian official.*

PHOTOILLUSTRATION BY DAN WINTERS.

In the first days of March, 2007, agents from the Mossad, the Israeli intelligence agency, made a daring raid on the Vienna home of Ibrahim Othman, the head of the Syrian Atomic Energy Commission. Othman was in town attending a meeting of the International Atomic Energy Agency's board of governors, and had stepped out. In less than an hour, the Mossad operatives swept in, extracted top-secret information from Othman's computer, and left without a trace.



## Guerra cibernética?



*"...the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar."<sup>2</sup>*



# Sabotagem ao Programa Nuclear Iraniano (2010)

Cyberwar

## The meaning of Stuxnet

A sophisticated "cyber-missile" highlights I

Sep 30th 2010 | From the print edition



IT HAS been described as "amazing", "groundbreaking" and "impressive" by computer-security specialists. The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals (see [article](#)). It is designed to infect a particular configuration of a particular type of industrial-control system—in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target.

## Guerra cibernética?

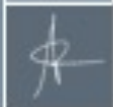


*The attackers appeared to be searching for computers that had one of two Siemens proprietary software programs installed—either Siemens SIMATIC Step 7 software or its SIMATIC WinCC program. Both programs are part of an industrial control system (ICS) designed to work with Siemens programmable logic controllers (PLCs)—small computers, generally the size of a toaster, that are used in factories around the world to*

# Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.3: Segurança e Tecnologia





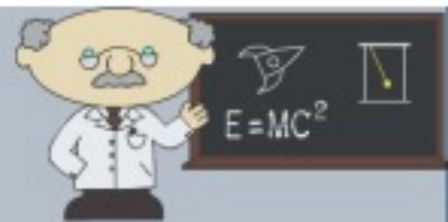
## Aspectos Técnicos de Segurança da Informação

- › Ferramentas e métodos para segurança
  - Criptografia
  - Arquiteturas e Protocolos
  - Autenticação
  - Controle de Acesso
  - IDS/IPS/FW/WAF/SIEM/Antivírus
  - Desenvolvimento Seguro e Segurança by Design
  - ...

...basicamente, a parte "didática" que vamos estudar nos livros

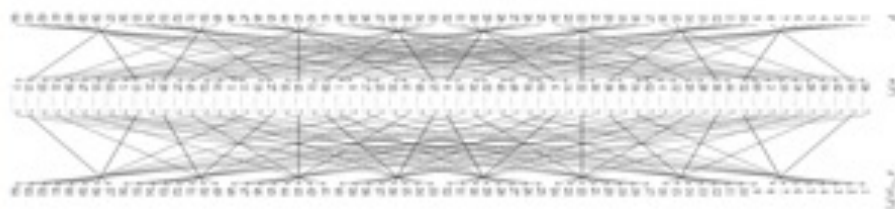
# Segurança da Informação, Parte 1: Motivação e Conceitos Básicos

1.4: Segurança e Ciência

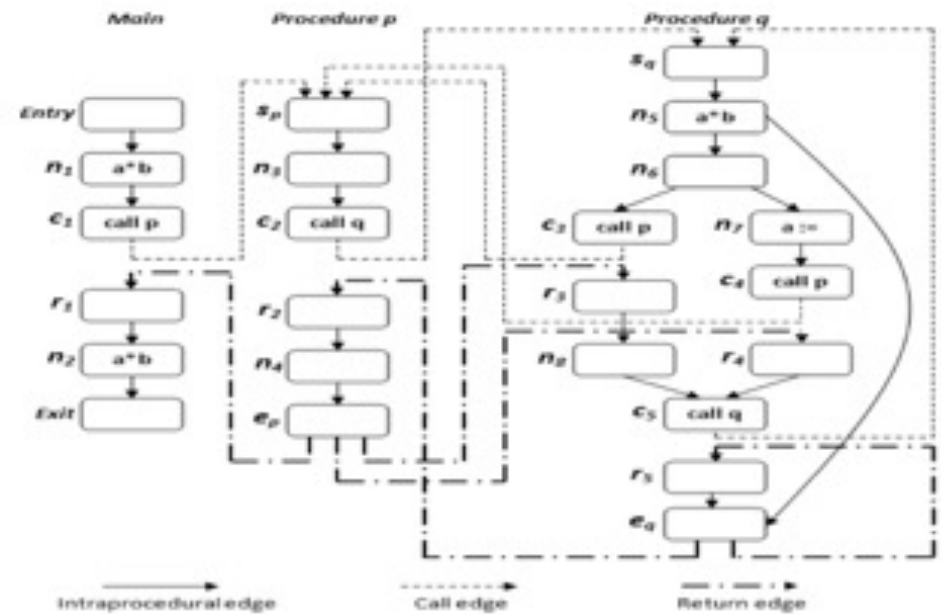
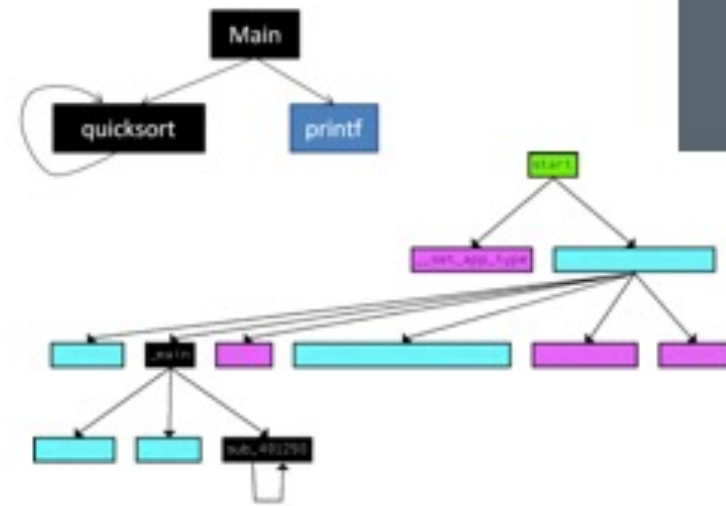
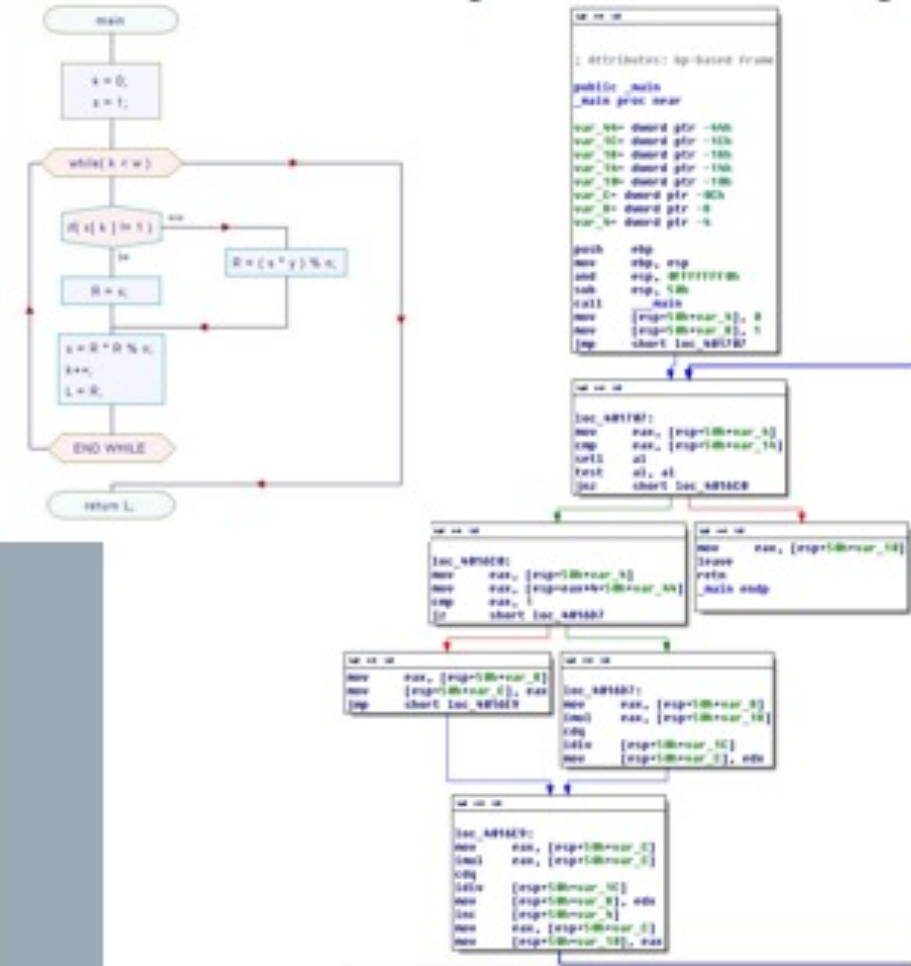




# Criptografia, protocolos e arquiteturas de segurança



# Análise de software, verificação/validação/testes

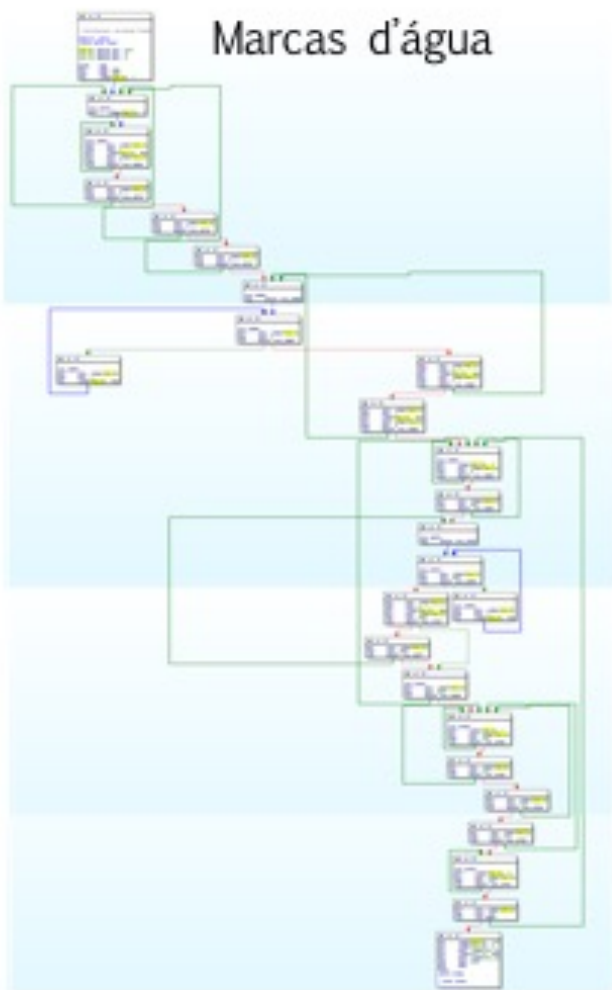


# Proteção de software

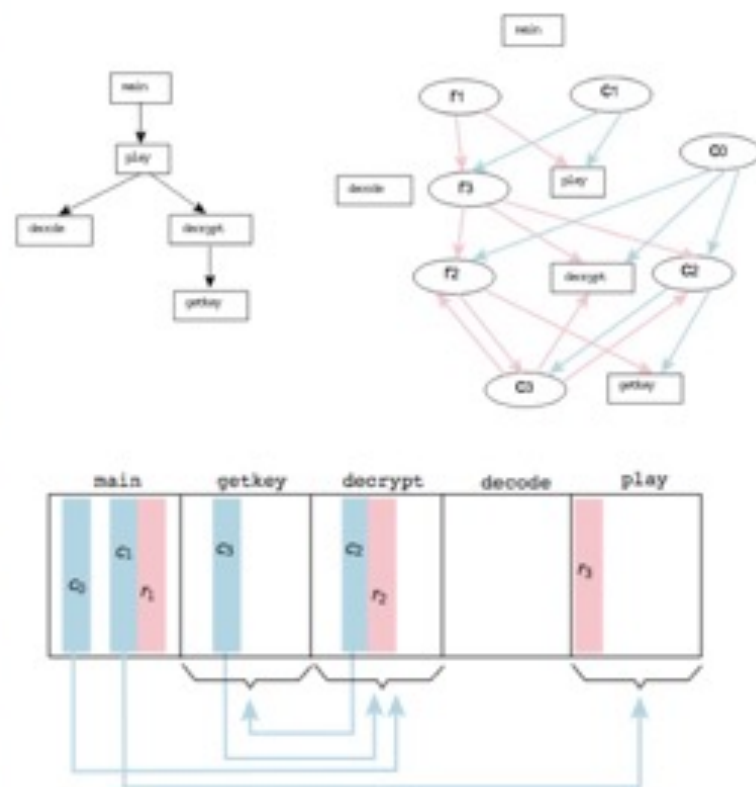
## Ofuscação



## Marcas d'água

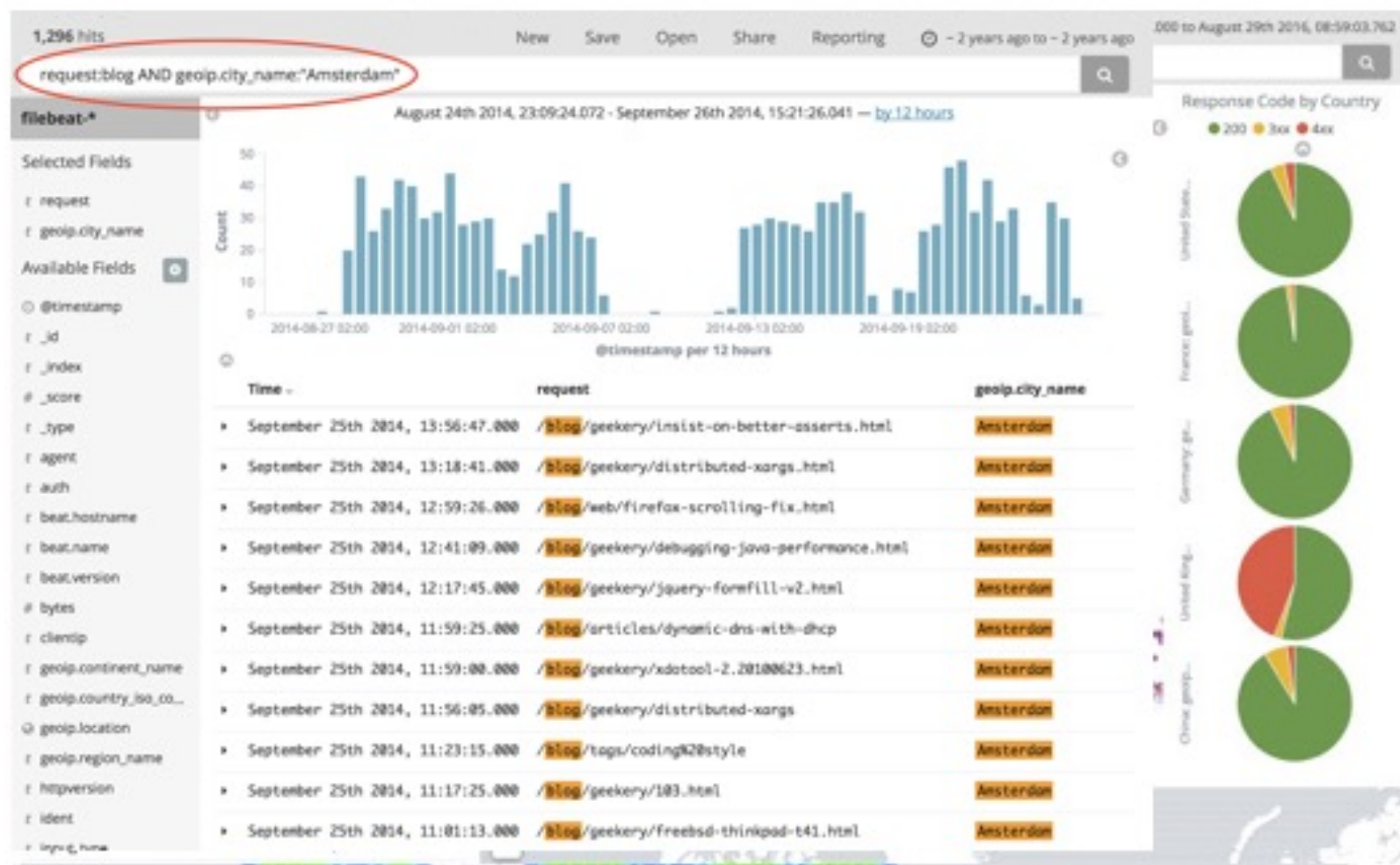


## Incorruptibilidade

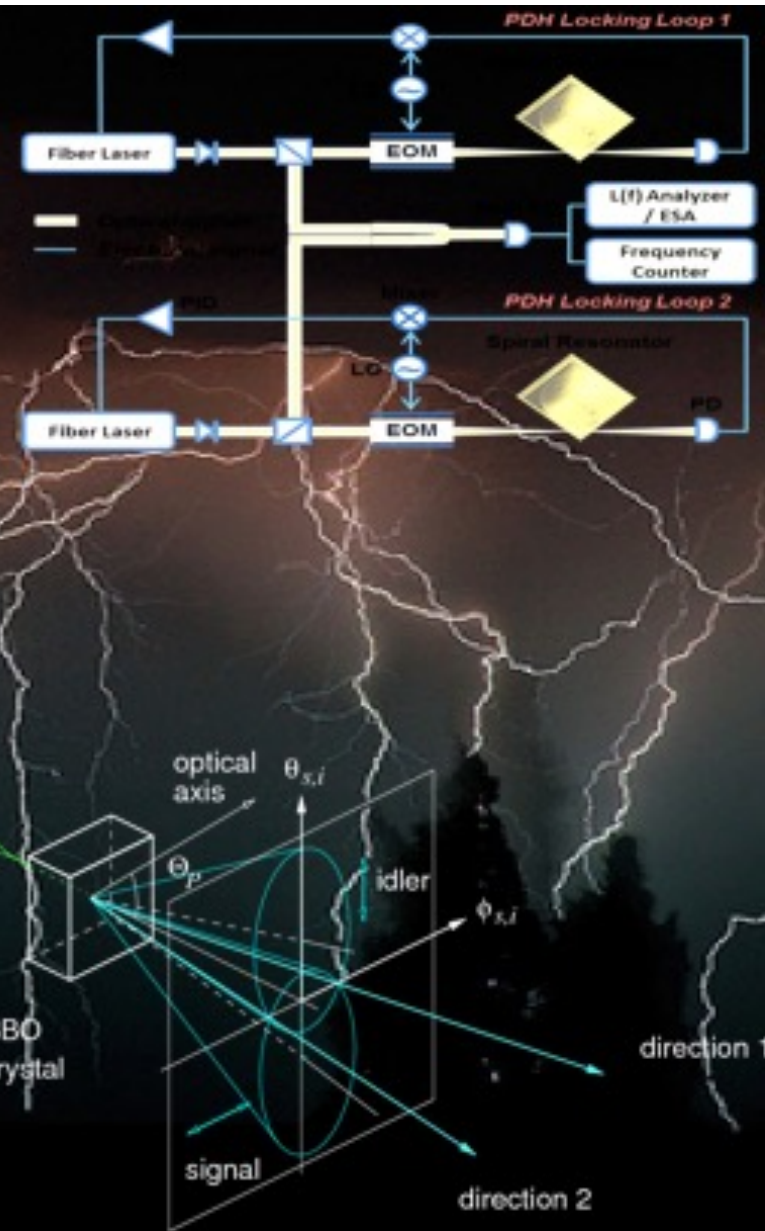




# Testes de Segurança Black-Box/comportamental

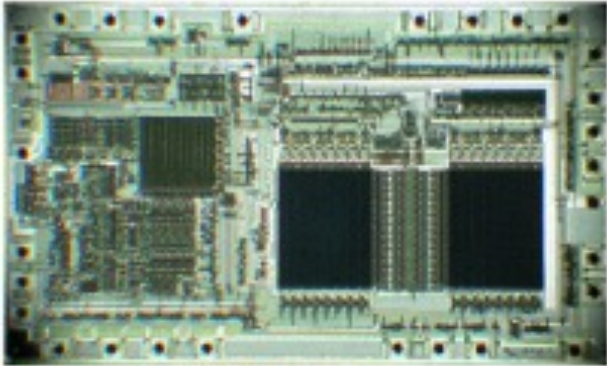
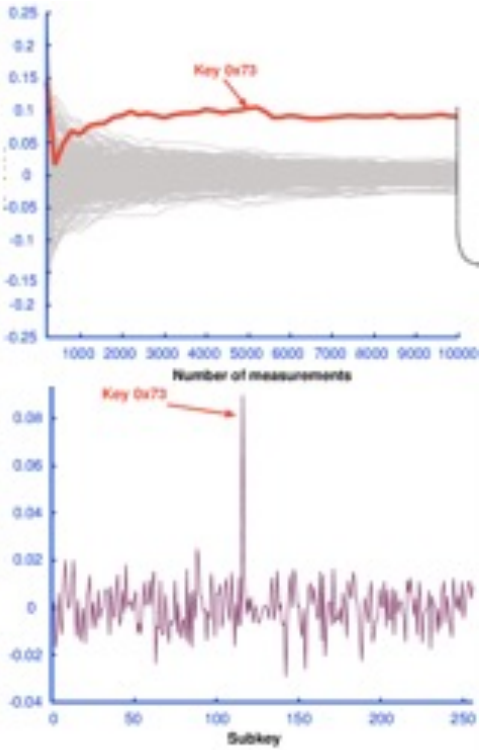


# Aleatoriedade

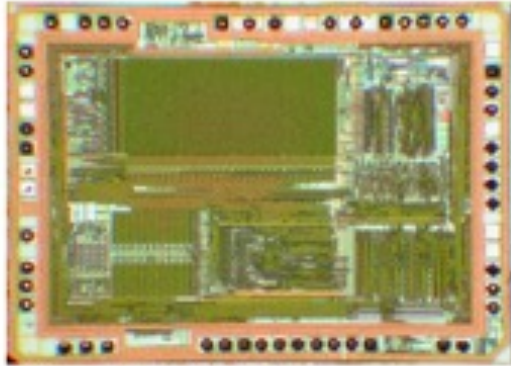




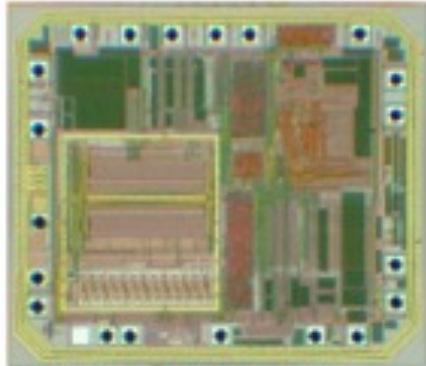
# Segurança da Hardware



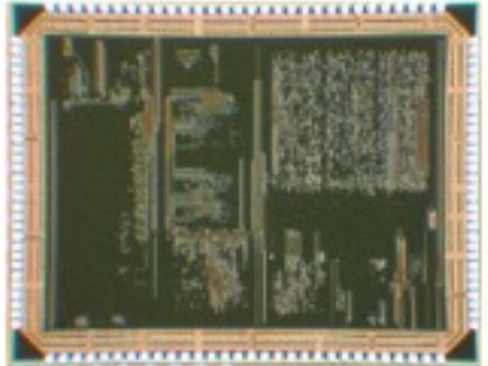
MC68HC705P6A, 1  $\mu\text{m}$



PIC16F77, 0.5  $\mu\text{m}$



MSP430F1121A, 0.35  $\mu\text{m}$



XAP Springbank, 0.18  $\mu\text{m}$



## Gestão de Riscos

