nic.br cgi.br cert.br

SECOMU 2021 – 51º Seminário de Computação na Universidade

CSBC 2021 – XLI Congresso da Sociedade Brasileira de Computação

19 de julho de 2021 | *Online*

cert.br

Computer Emergency Response Team Brazil

National CSIRT of Last Resort

Services Provided to the Community

Incident Management

- Coordination
- Technical Analysis
- Mitigation and Recovery Support

Situational Awareness

- Data Acquisition
  - Distributed Honeypots
  - SpamPots
  - Threat feeds
- Information Sharing

Knowledge Transfer

- Awareness
  - Development of Best Practices
  - Outreach
- Training
- Technical and Policy Advisory

Affiliations and Partnerships:

SEI Partner Network

Creation:

August/1996: CGI.br publishes a report with a proposed model for incident management for the country[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office) based on the report's recommendations[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The Brazilian Network Information Center

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

https://cert.br/about/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

The Lack of Privacy and Behavioral Control in a Surveillance Economy: Is Another World Possible?

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br nic.br cgi.br

Surveillance capitalism is an economic system
centered around the commodification of personal data
with the core purpose of profit-making.

The 2000s also saw the world's governments
putting in the effort to 'Master the Internet' (as the NSA put it) –
working out how to collect data at scale and index it,
just as Google does, to make it available to analysts.

Sources:
https://en.wikipedia.org/wiki/Surveillance_capitalism

Surveillance Capitalism and the Challenge of Collective Action, Shoshana Zuboff, January 24, 2019
https://doi.org/10.1177/1095796018819461

Chapter 2: Who is the Opponent?, Security Engineering 3rd Edition, 2020, Ross Anderson
https://www.cl.cam.ac.uk/~rja14/book.html

Lack of Privacy and Behavioral Control

How do we get there…

By design

Private Sector

- The business model depends on extracting intelligence from data and behavior (“surveillance capitalism/economy”)

Public Sector

- Data to inform or implement public policies, with varying motives
  - strategic and economic advantage
  - market competition
  - safety and health
  - terrorism and counterinsurgency
  - censorship and citizen control
  - maintenance of human rights

Due to carelessness, ignorance or incompetence

Poorly designed and implemented systems expose citizens to surveillance from companies, governments (local and foreign) and organized crime

- naïve assumptions
- no risk analysis
- no security engineering
- insecure coding
- lack of security lifecycle (patches, proper authentication, etc) specially in IoT, medical and SCADA systems

What is Privacy?

Privacy is the ability and/or right to protect your personal information and extends to the ability and/or right to prevent invasions of your personal space (the exact definition of which varies quite sharply from one country to another).

Confidentiality involves an obligation to protect some other person’s or organization’s secrets if you know them.

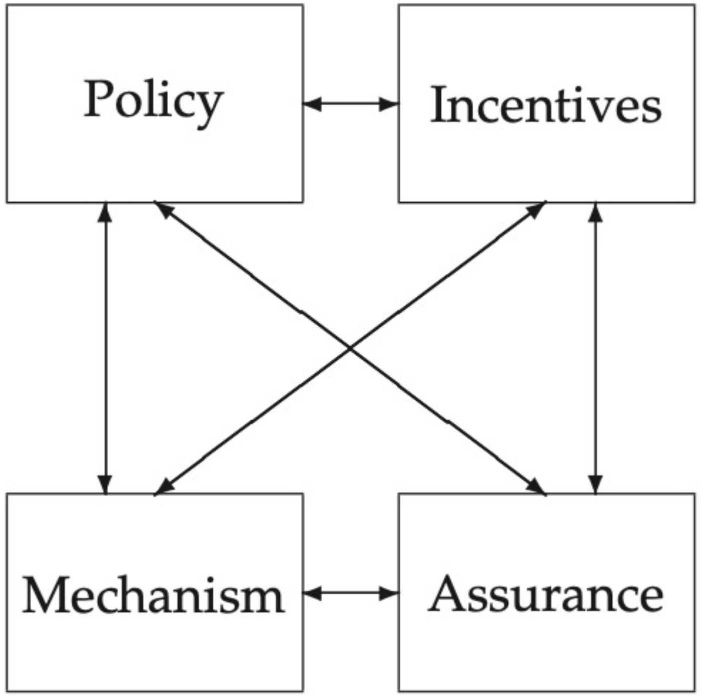
Secrecy is a technical term which refers to the effect of the mechanisms used to limit the number of principals who can access information, such as cryptography or computer access controls.

Source: Chapter 1: What is Security Engineering?, Security Engineering, 2nd Edition, 2008, Ross Anderson
https://www.cl.cam.ac.uk/~rja14/book.html

Data Protection is Key to Privacy and Depends on **Good Security Engineering**

Security engineering is about building systems to remain dependable in the face of malice, error, or mischance.

Good security engineering requires four things to come together. There's policy: what you're supposed to achieve. There's mechanism: the ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy. There's assurance: the amount of reliance you can place on each particular mechanism. Finally, there's incentive: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy.



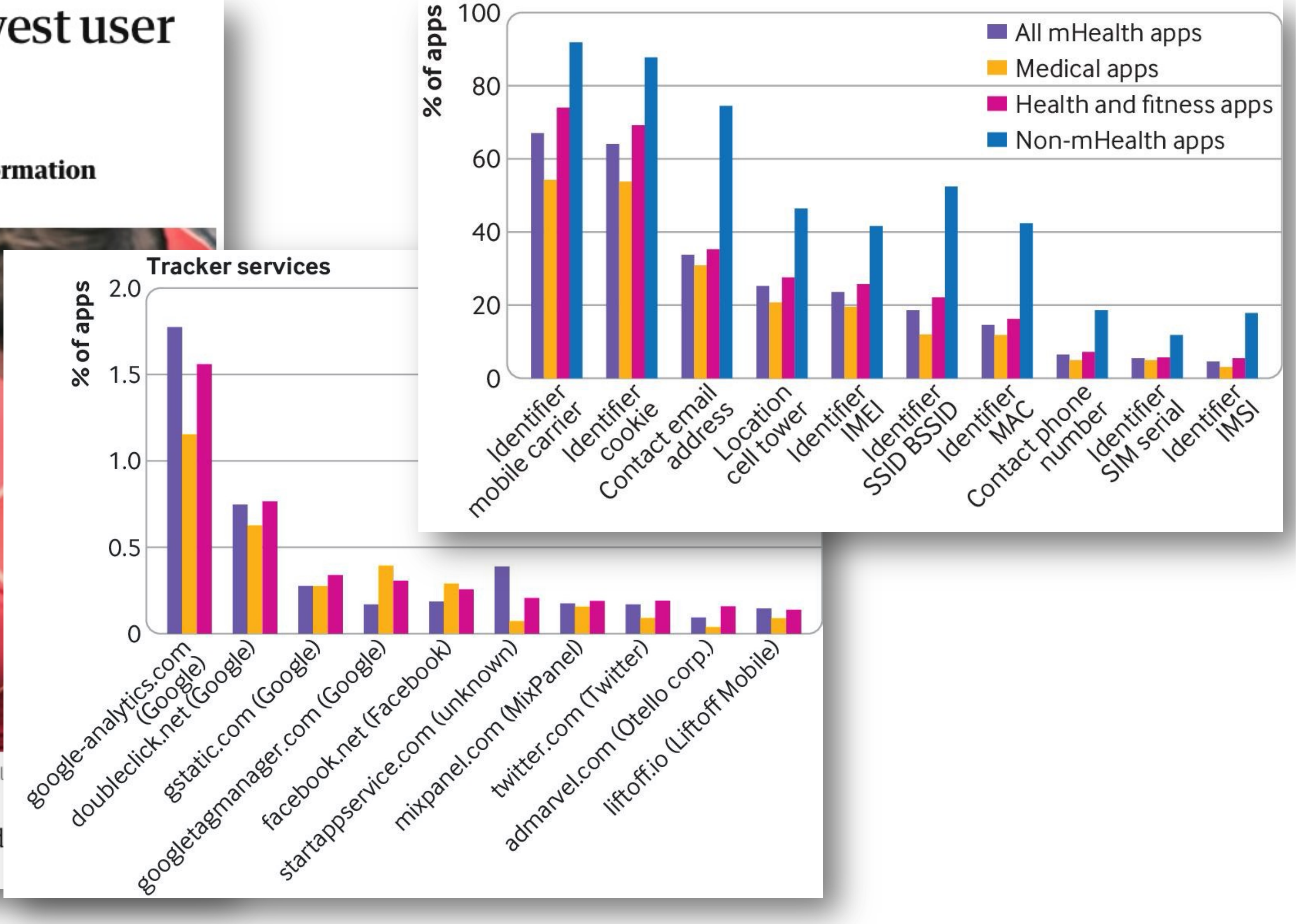
Source: Chapter 1: What is Security Engineering?, Security Engineering, 2nd Edition, 2008, Ross Anderson
https://www.cl.cam.ac.uk/~rja14/book.html

Nine out of 10 health apps harvest user data, global study shows

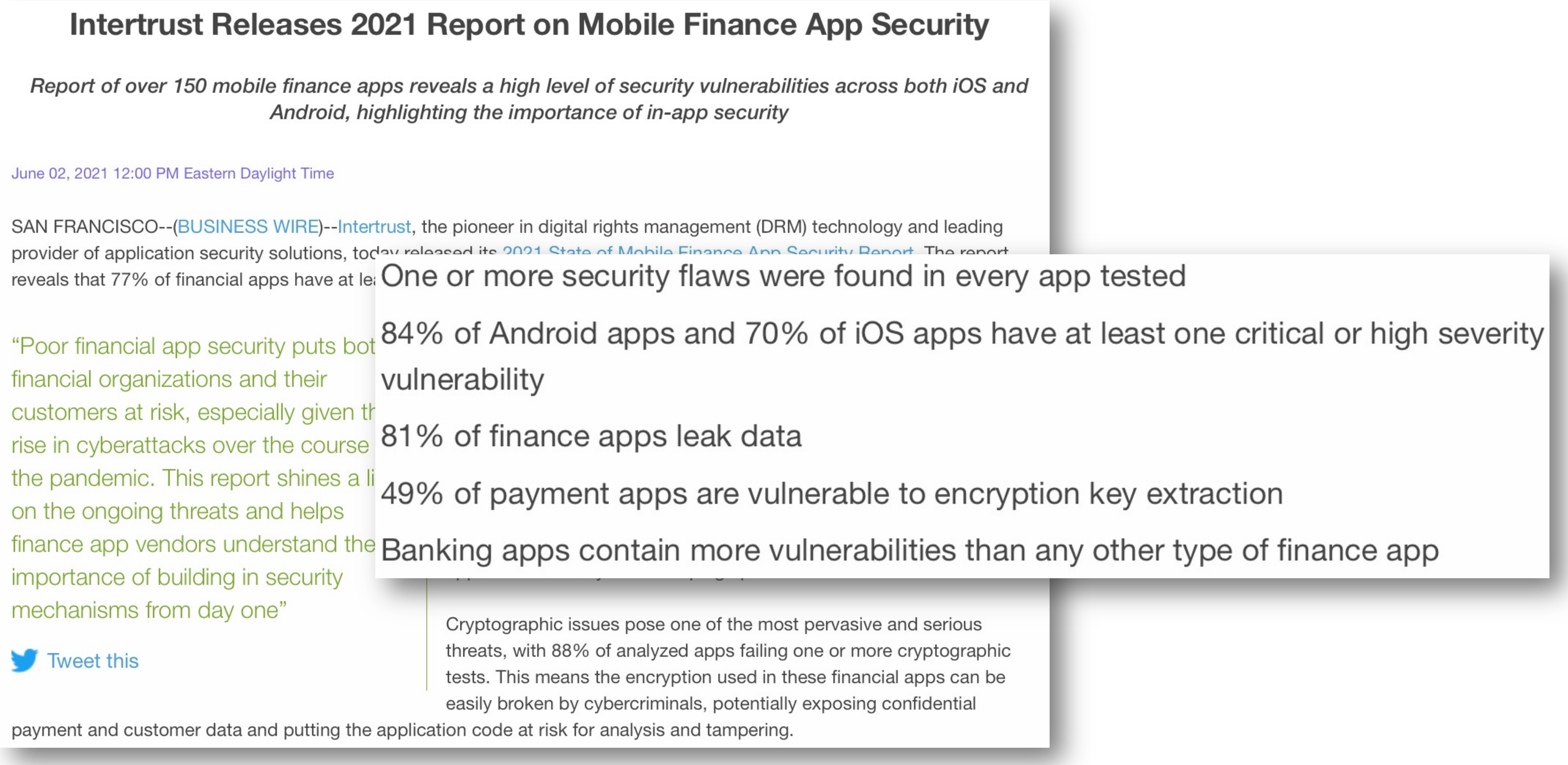
Analysis of 20,000 mobile apps that ask for sensitive information shows that some track users across different platforms

▲ Almost a third of health apps do not provide any sort of privacy statement on Googl
in the British Medical Journal reveals. Photograph: Alamy

Nine out of 10 mobile health apps collect and track user d
new global study.



Mobile health and privacy: cross sectional study, BMJ 2021; 373 doi: https://doi.org/10.1136/bmj.n1248
https://www.theguardian.com/technology/2021/jun/17/nine-out-of-10-health-apps-harvest-user-data-global-study-shows



Intertrust Releases 2021 Report on Mobile Finance App Security

Report of over 150 mobile finance apps reveals a high level of security vulnerabilities across both iOS and Android, highlighting the importance of in-app security

June 02, 2021 12:00 PM Eastern Daylight Time

SAN FRANCISCO--(BUSINESS WIRE)--Intertrust, the pioneer in digital rights management (DRM) technology and leading provider of application security solutions, today released its 2021 State of Mobile Finance App Security Report. The report reveals that 77% of financial apps have at le

"Poor financial app security puts bot
financial organizations and their
customers at risk, especially given th
rise in cyberattacks over the course
the pandemic. This report shines a li
on the ongoing threats and helps
finance app vendors understand the
importance of building in security
mechanisms from day one"

Tweet this

One or more security flaws were found in every app tested

84% of Android apps and 70% of iOS apps have at least one critical or high severity vulnerability

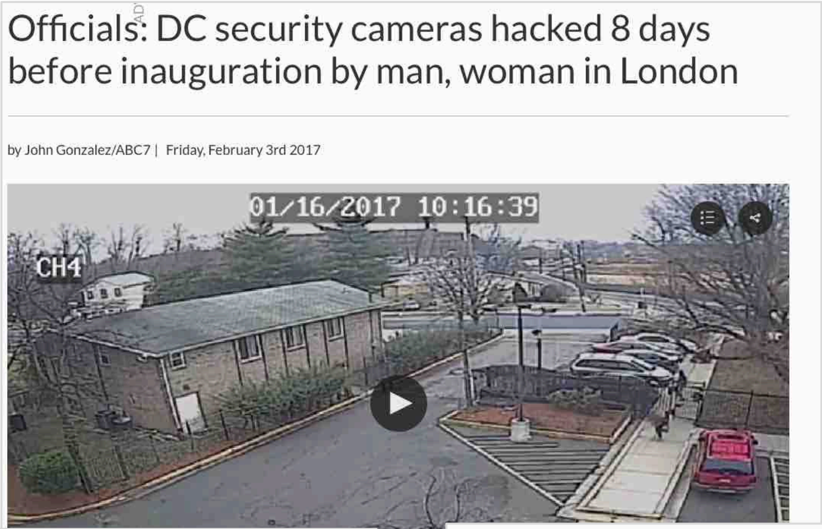
81% of finance apps leak data

49% of payment apps are vulnerable to encryption key extraction

Banking apps contain more vulnerabilities than any other type of finance app

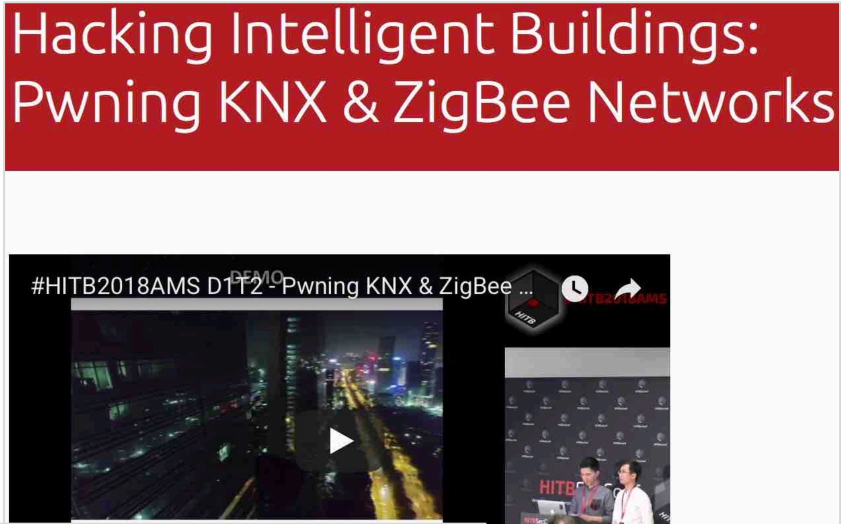
Cryptographic issues pose one of the most pervasive and serious threats, with 88% of analyzed apps failing one or more cryptographic tests. This means the encryption used in these financial apps can be easily broken by cybercriminals, potentially exposing confidential payment and customer data and putting the application code at risk for analysis and tampering.

https://www.businesswire.com/news/home/20210602005213/en/Intertrust-Releases-2021-Report-on-Mobile-Finance-App-Security

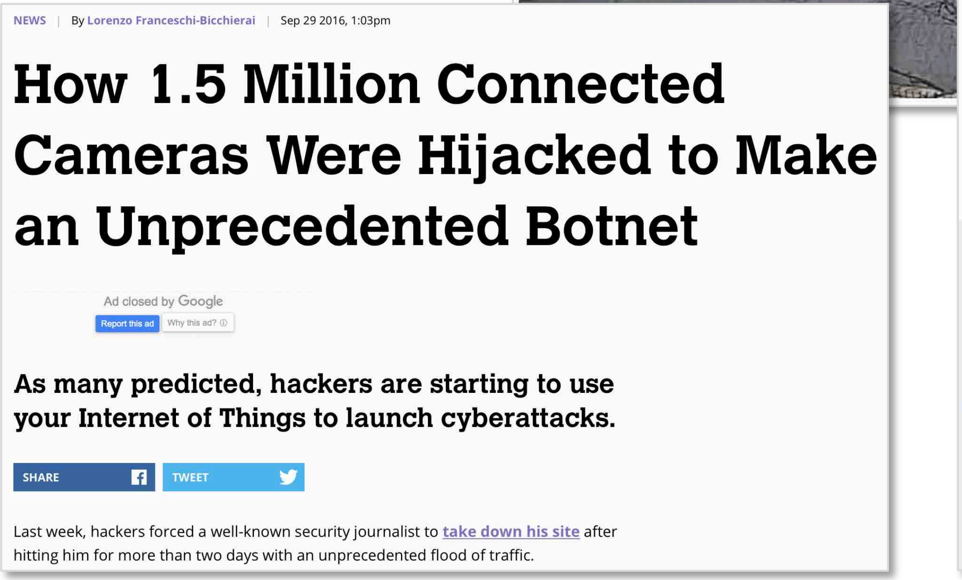


Officials: DC security cameras hacked 8 days before inauguration by man, woman in London

by John Gonzalez/ABC7 | Friday, February 3rd 2017



Hacking Intelligent Buildings: Pwning KNX & ZigBee Networks

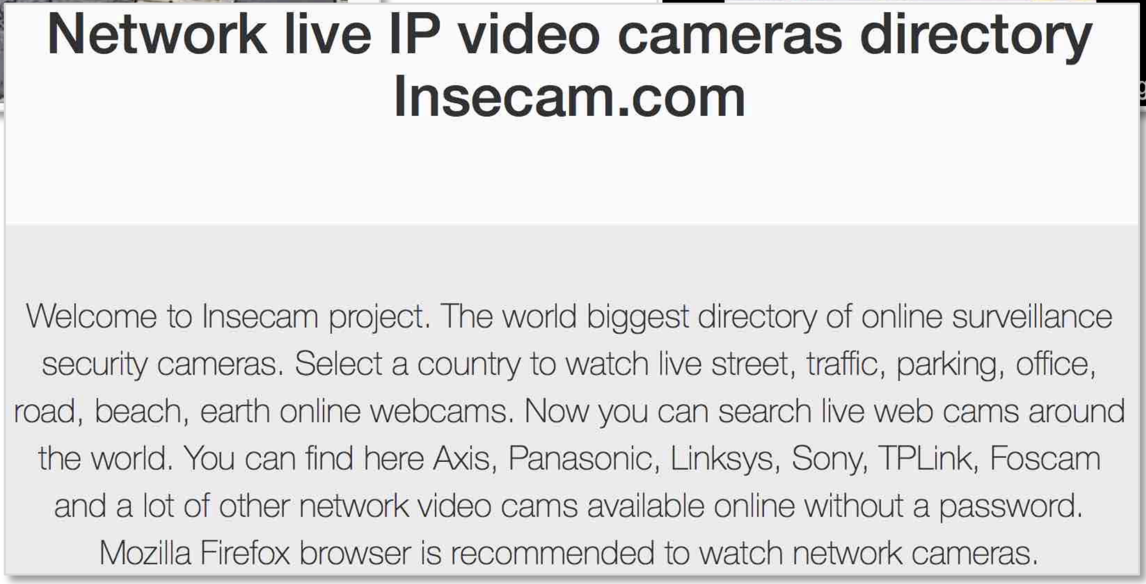


NEWS | By Lorenzo Franceschi-Bicchierai | Sep 29 2016, 1:03pm

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

As many predicted, hackers are starting to use your Internet of Things to launch cyberattacks.

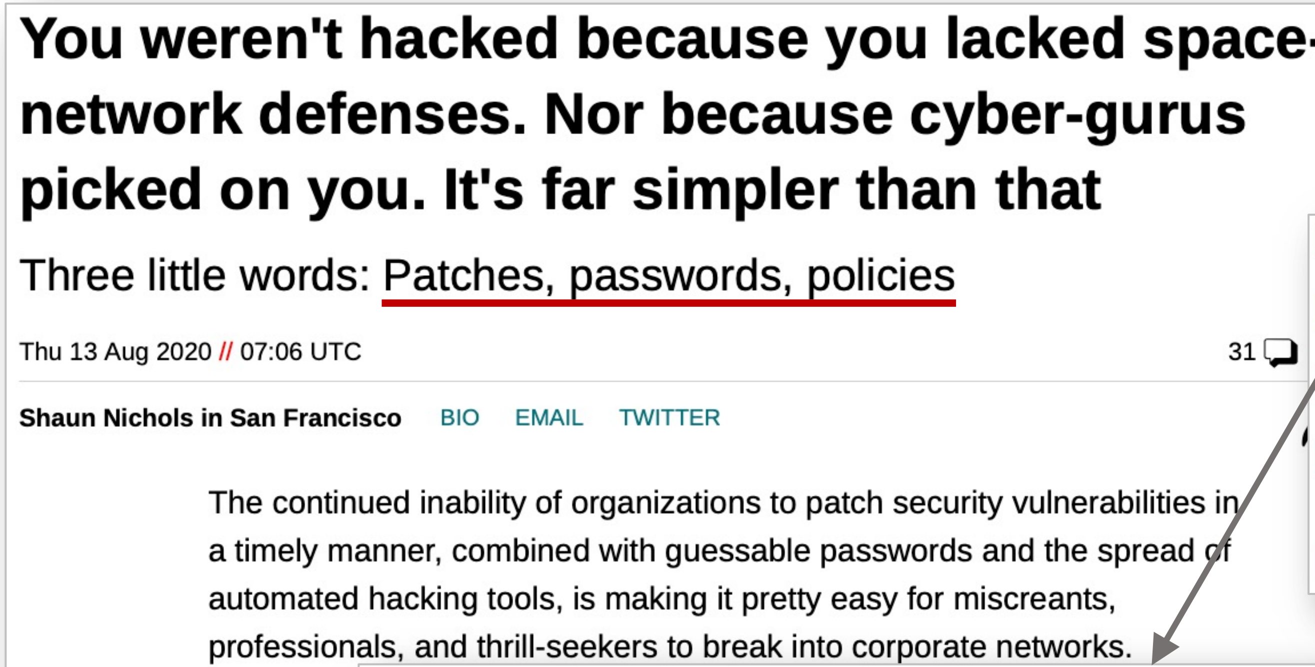
Last week, hackers forced a well-known security journalist to take down his site after hitting him for more than two days with an unprecedented flood of traffic.



Network live IP video cameras directory Insecam.com

Welcome to Insecam project. The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams. Now you can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other network video cams available online without a password. Mozilla Firefox browser is recommended to watch network cameras.

https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs
https://wjla.com/news/local/officials-dc-security-cameras-hacked-8-days-before-inauguration-by-man-woman-in-london
https://conference.hitb.org/hitbsecconf2018ams/sessions/hacking-intelligent-buildings-pwning-knx-zigbee-networks/
http://www.insecam.org



You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

Three little words: Patches, passwords, policies

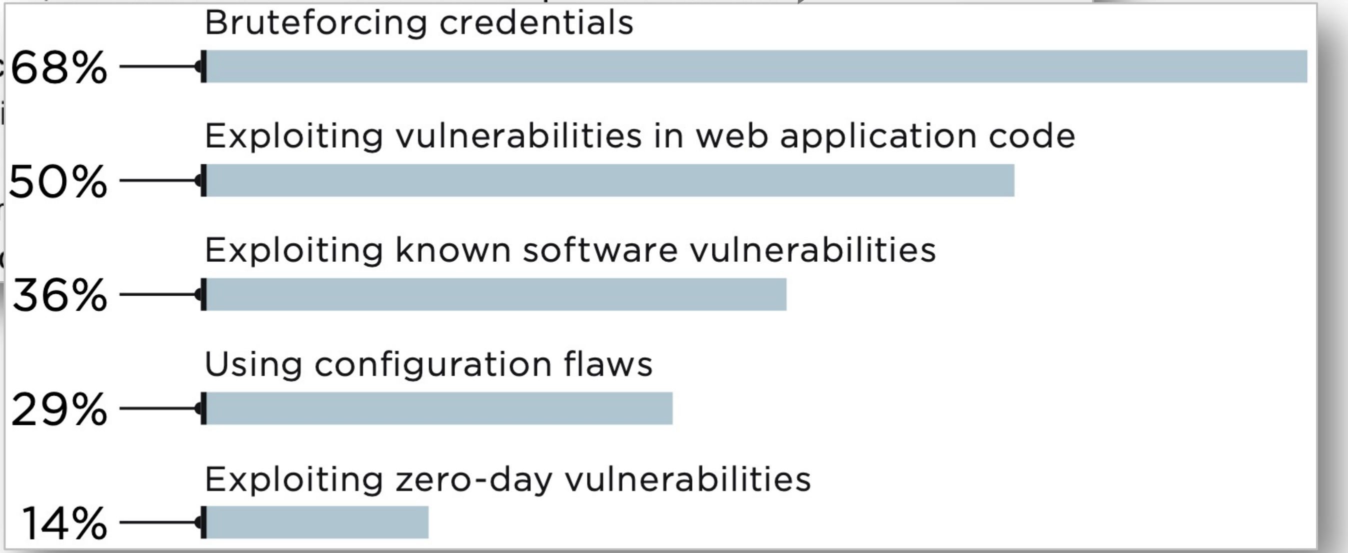
Thu 13 Aug 2020 // 07:06 UTC

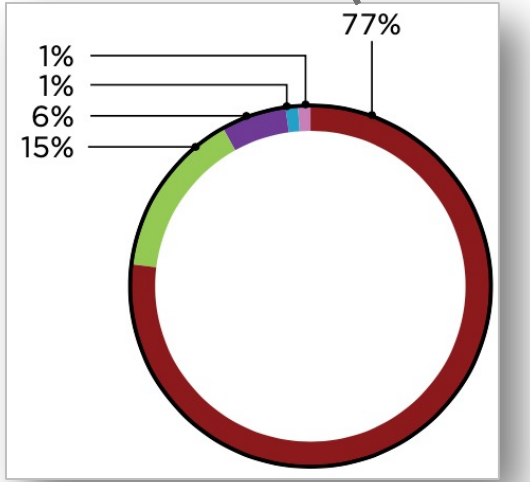
31

Shaun Nichols in San Francisco BIO EMAIL TWITTER

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

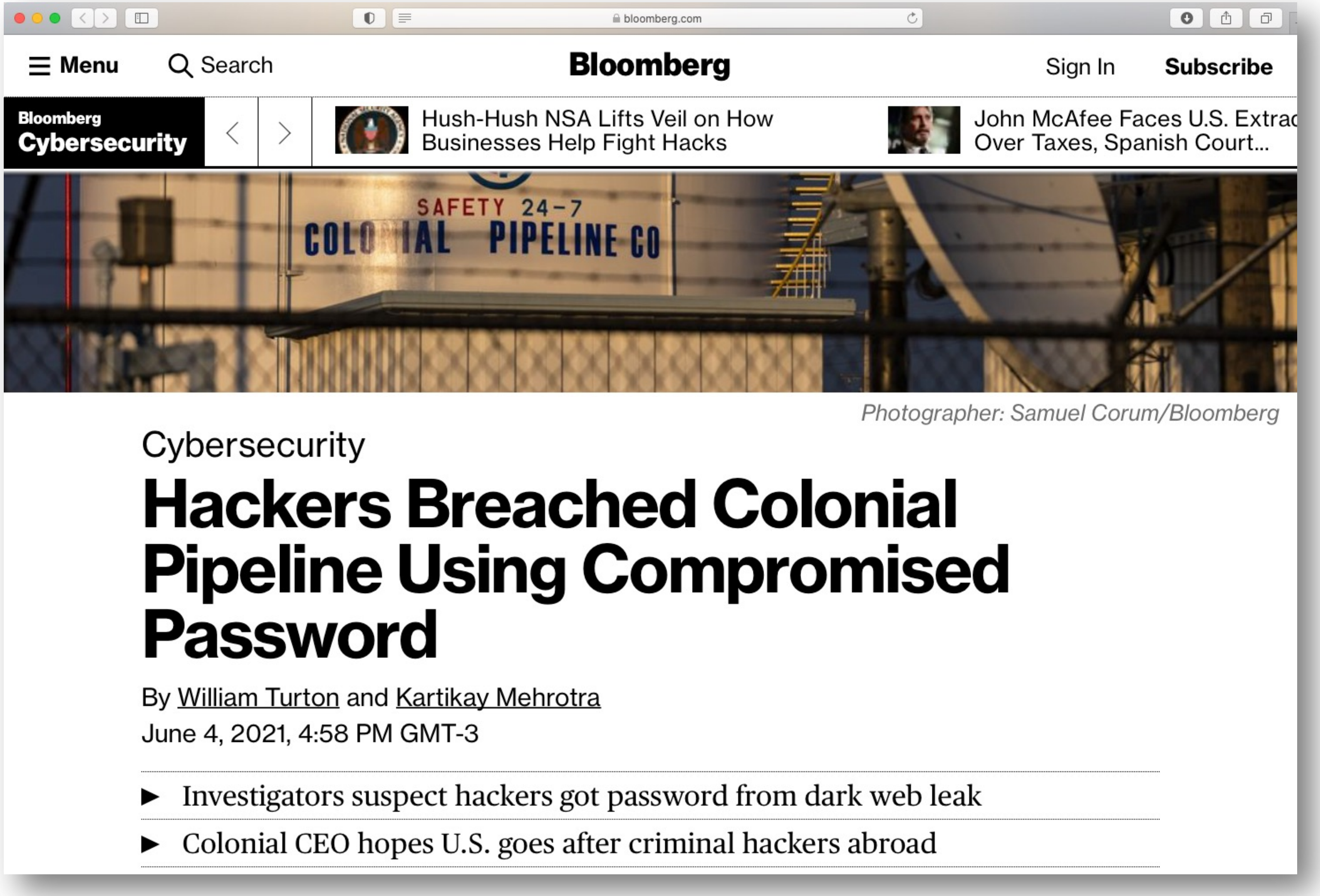
This is acc
Technologi
and found
its red tear
available t





- 🟥 Using web application protection vulnerabilities and flaws
- 🟩 Bruteforcing credentials used for accessing DBMS
- 🟪 Bruteforcing credentials for remote access services
- 🟦 Bruteforcing domain user credentials together with software vulnerabilities exploitation
- ▨ Bruteforcing credentials for the FTP server

https://www.theregister.com/2020/08/13/pentest_networks_fail/
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf



Hush-Hush NSA Lifts Veil on How Businesses Help Fight Hacks

John McAfee Faces U.S. Extrac Over Taxes, Spanish Court...

Photographer: Samuel Corum/Bloomberg

Cybersecurity

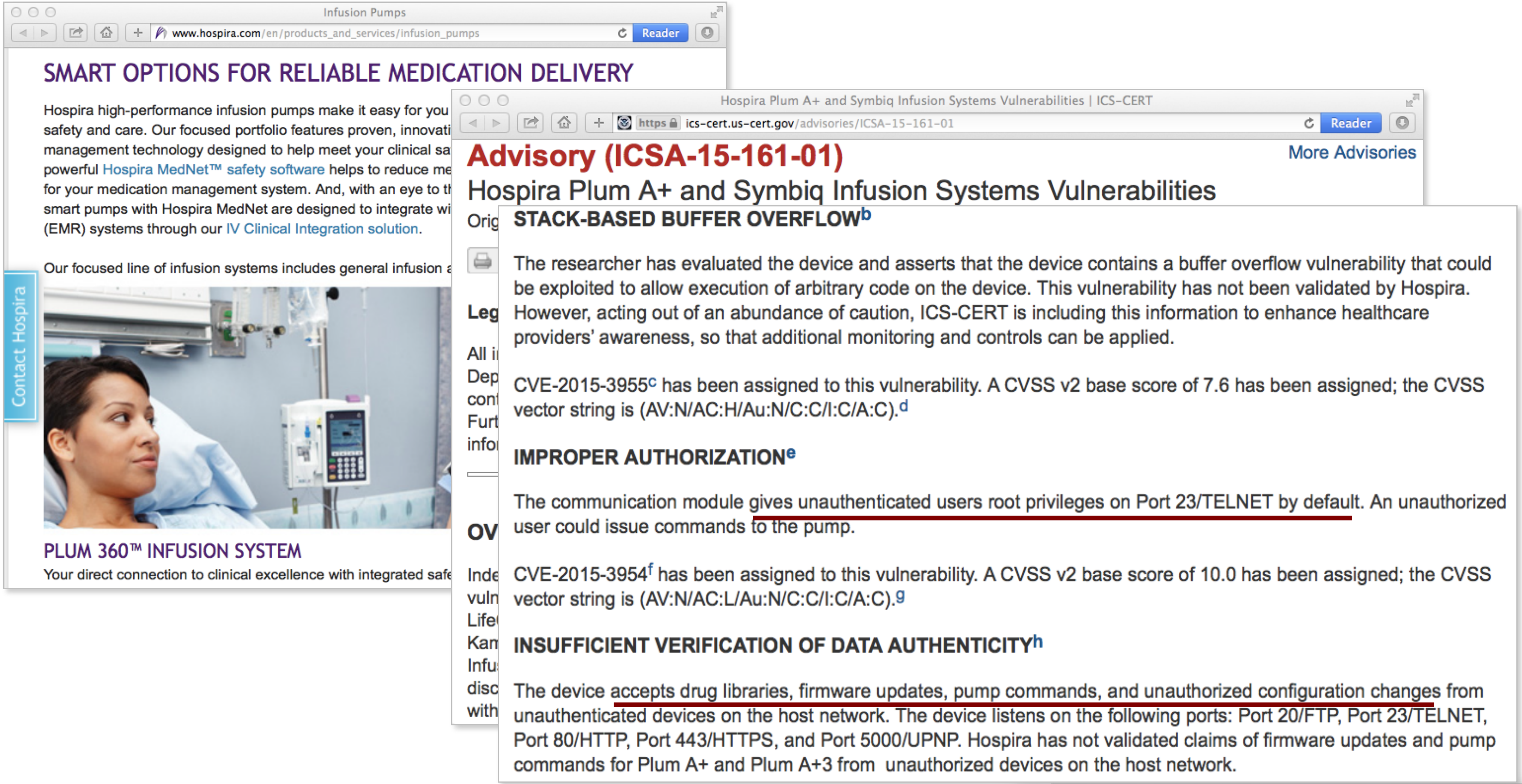
Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra

June 4, 2021, 4:58 PM GMT-3

- ▶ Investigators suspect hackers got password from dark web leak
- ▶ Colonial CEO hopes U.S. goes after criminal hackers abroad

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password



SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you
safety and care. Our focused portfolio features proven, innovati
management technology designed to help meet your clinical sa
powerful Hospira MedNet™ safety software helps to reduce me
for your medication management system. And, with an eye to th
smart pumps with Hospira MedNet are designed to integrate wi
(EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion a

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safe

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities | ICS-CERT
https ics-cert.us-cert.gov/advisories/ICSA-15-161-01
Reader
More Advisories

Advisory (ICSA-15-161-01)

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Orig

Leg

All i
Dep
con
Furt
info

OV

Inde
vuln
Life
Kan
Infu
disc
with

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

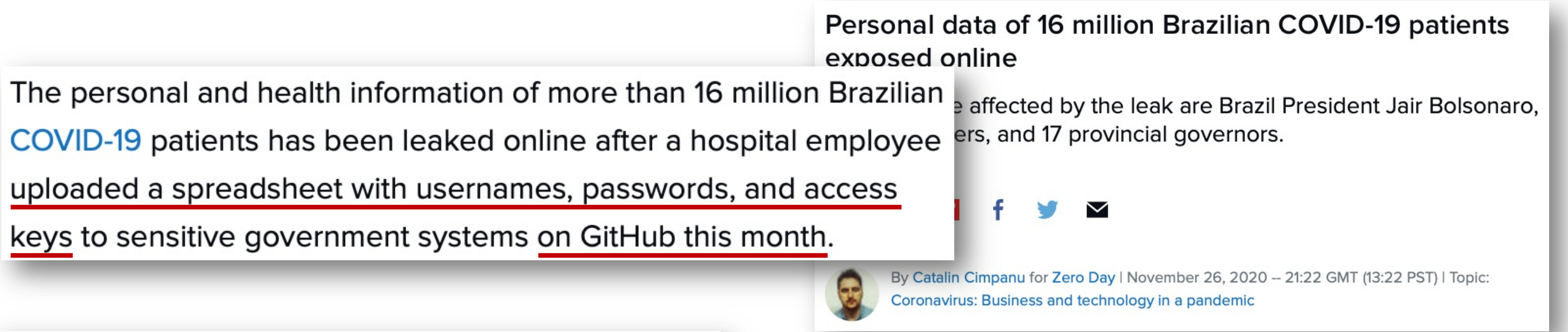
IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

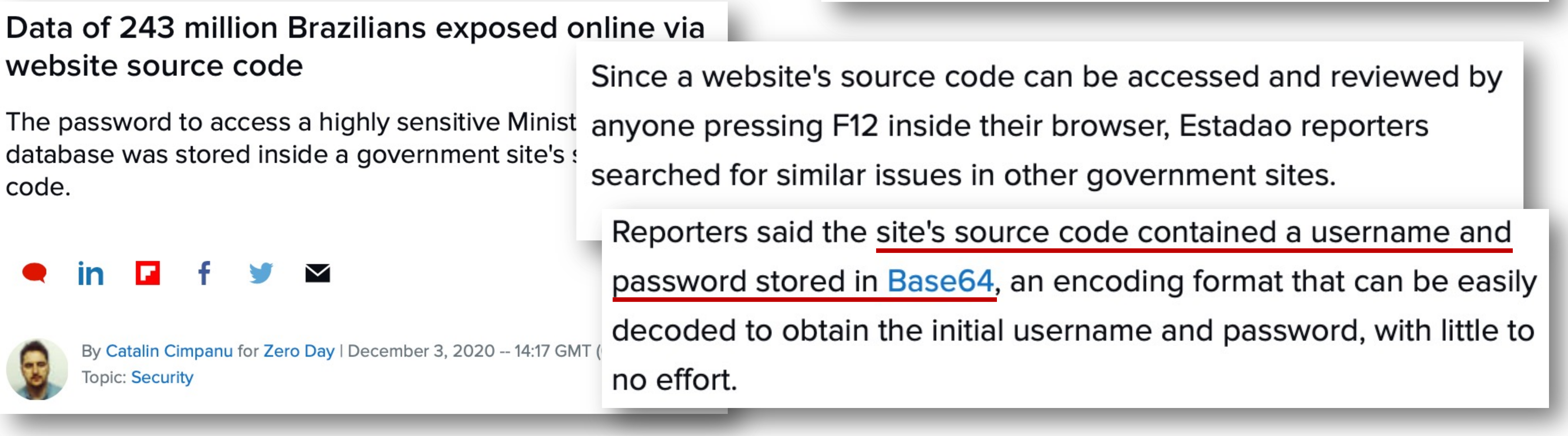


Personal data of 16 million Brazilian COVID-19 patients exposed online

The personal and health information of more than 16 million Brazilian COVID-19 patients has been leaked online after a hospital employee uploaded a spreadsheet with usernames, passwords, and access keys to sensitive government systems on GitHub this month.

e affected by the leak are Brazil President Jair Bolsonaro, ers, and 17 provincial governors.

By Catalin Cimpanu for Zero Day | November 26, 2020 -- 21:22 GMT (13:22 PST) | Topic: Coronavirus: Business and technology in a pandemic



Data of 243 million Brazilians exposed online via website source code

The password to access a highly sensitive Minist database was stored inside a government site's s code.

Since a website's source code can be accessed and reviewed by anyone pressing F12 inside their browser, Estadao reporters searched for similar issues in other government sites.

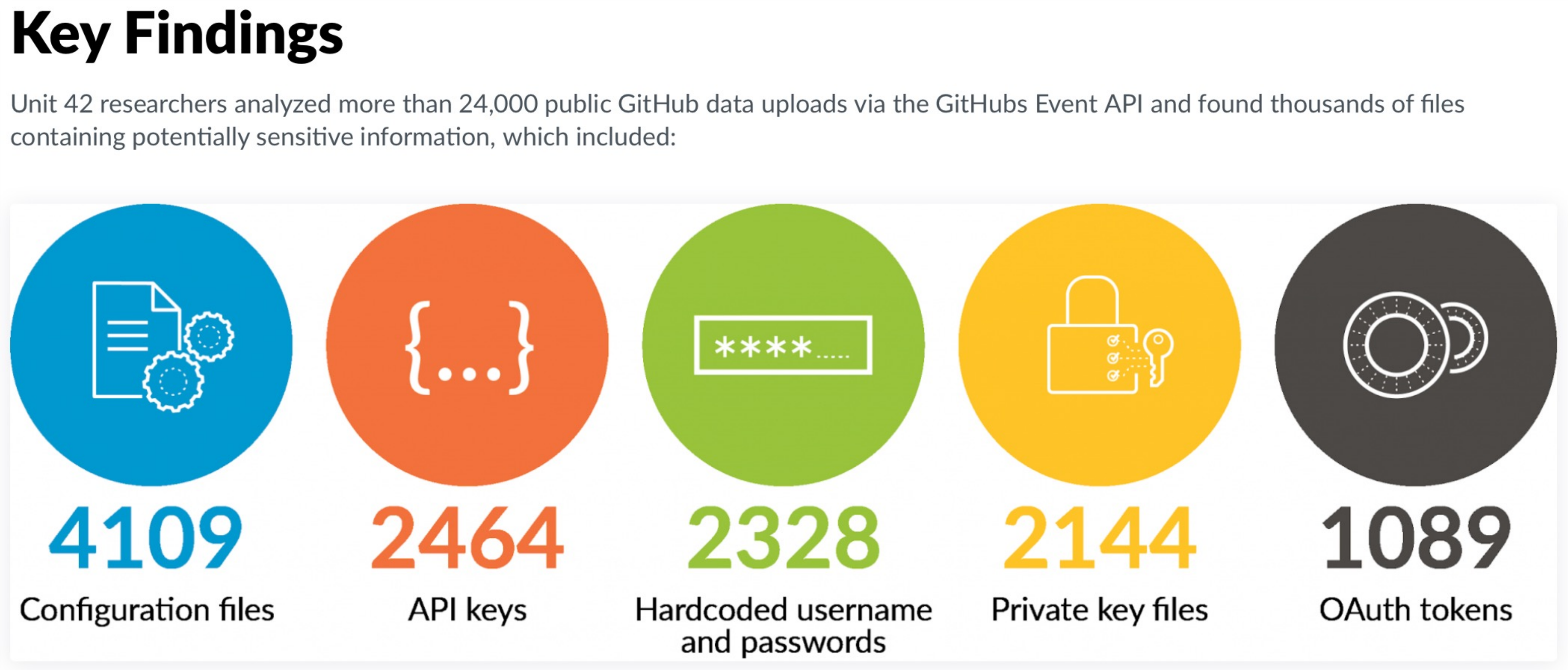
Reporters said the site's source code contained a username and password stored in Base64, an encoding format that can be easily decoded to obtain the initial username and password, with little to no effort.

By Catalin Cimpanu for Zero Day | December 3, 2020 -- 14:17 GMT (

Topic: Security

https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/
https://www.zdnet.com/article/data-of-243-million-brazilians-exposed-online-via-website-source-code/

GitHub as a Data Leak Source



Key Findings

Unit 42 researchers analyzed more than 24,000 public GitHub data uploads via the GitHubs Event API and found thousands of files containing potentially sensitive information, which included:

4109
Configuration files

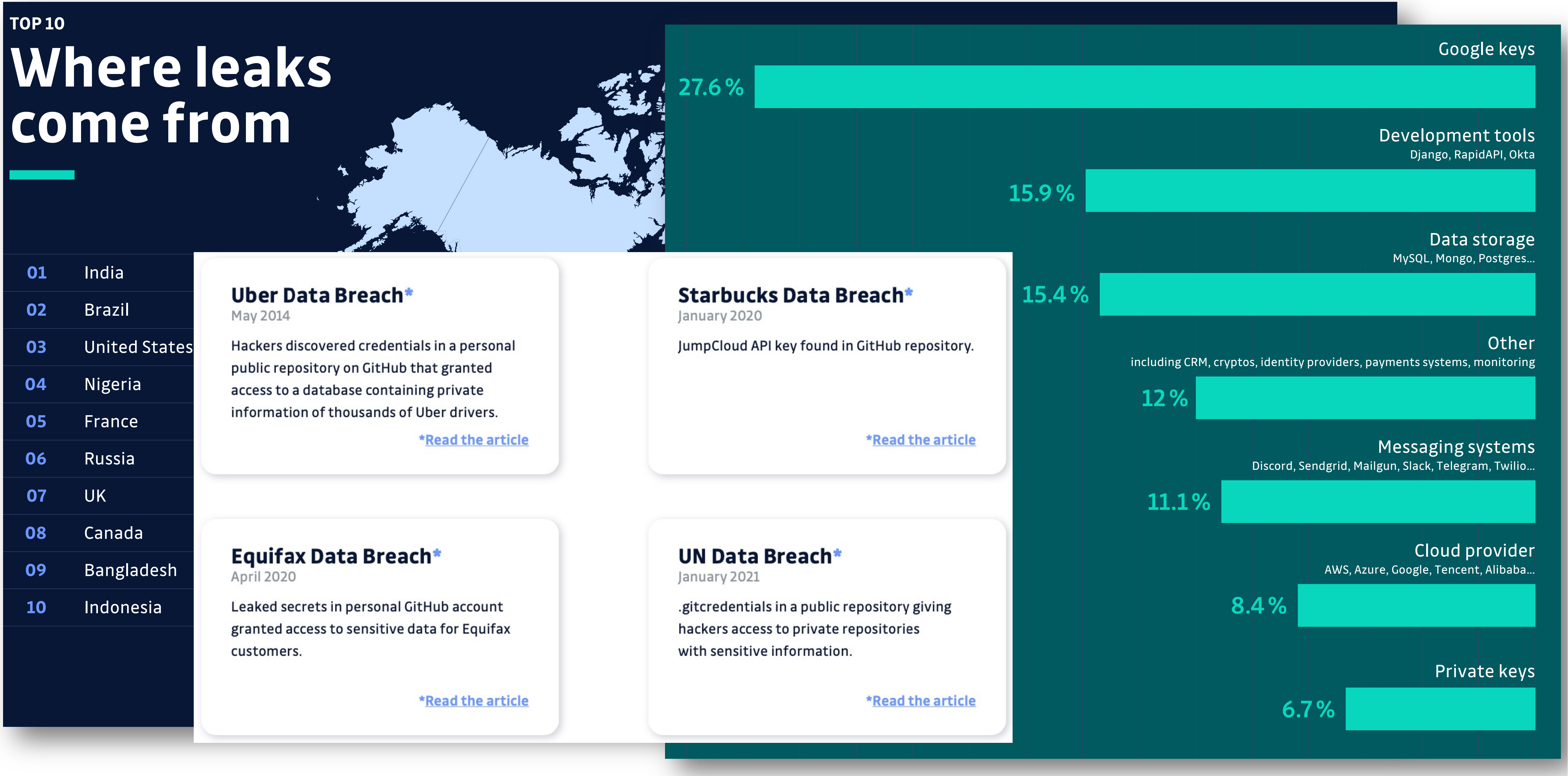
2464
API keys

2328
Hardcoded username and passwords

2144
Private key files

1089
OAuth tokens

https://unit42.paloaltonetworks.com/github-data-exposed/



TOP 10

Where leaks come from

01	India
02	Brazil
03	United States
04	Nigeria
05	France
06	Russia
07	UK
08	Canada
09	Bangladesh
10	Indonesia

Uber Data Breach*

May 2014

Hackers discovered credentials in a personal public repository on GitHub that granted access to a database containing private information of thousands of Uber drivers.

*Read the article

Starbucks Data Breach*

January 2020

JumpCloud API key found in GitHub repository.

*Read the article

Equifax Data Breach*

April 2020

Leaked secrets in personal GitHub account granted access to sensitive data for Equifax customers.

*Read the article

UN Data Breach*

January 2021

.gitcredentials in a public repository giving hackers access to private repositories with sensitive information.

*Read the article

Category	Share
Google keys	27.6 %
Development tools Django, RapidAPI, Okta	15.9 %
Data storage MySQL, Mongo, Postgres...	15.4 %
Other including CRM, cryptos, identity providers, payments systems, monitoring	12 %
Messaging systems Discord, Sendgrid, Mailgun, Slack, Telegram, Twilio...	11.1 %
Cloud provider AWS, Azure, Google, Tencent, Alibaba...	8.4 %
Private keys	6.7 %

State of Secrets Sprawl on GitHub - 2021: https://blog.gitguardian.com/state-of-secrets-sprawl-2021/

These later examples are not just “bad security”
No security mechanisms can cope with bad design/practices

STOP

- teaching security as a separate discipline
- teaching to build systems thinking only about fulfilling use cases
- thinking that someone or some security technology can fix it later
- building bad muscle memory on students
  - they will not easily change coding practices learnt at the University
  - they also need to learn how to use all tools and frameworks securely

FOCUS ON

- teaching that security is everyone’s responsibility
- thinking about abuse cases
  - attackers’ incentives
- permeating security in every discipline, specially
  - data science
  - software engineering and programming
- teaching critical thinking and skepticism

Final Thoughts

It is not because something can be done that it should be done

- always think about ethical and security considerations
- assume someone will try to abuse the technology you are creating

Always ask yourself: What could possibly go wrong?

Additional References

- Data Hemorrhage, Inequality, and You: How Technology and Data Flows are Changing the Civil Liberties Game (Slides and Video available)

  Shankar Narayan, Technology and Liberty Project Director, American Civil Liberties Union
  https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/narayan

- Security Engineering 3rd Edition, 2020, Ross Anderson

  Chapter 2: Who is the Opponent?

  Chapter 26: Surveillance or Privacy?
  https://www.cl.cam.ac.uk/~rja14/book.html

- The Second Crypto War—What's Different Now (Slides and Video available)

  Susan Landau, Bridge Professor of Cyber Security and Policy, Tufts University
  https://www.usenix.org/conference/usenixsecurity18/presentation/landau

- Addison-Wesley Software Security Series
  https://www.oreilly.com/library/view/software-security-building/0321356705/pr03.html

- Building Security In Maturity Model (BSIMM)
  https://www.bsimm.com/

- Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications
  https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Thank You

@ cristine@cert.br

@ incident notifications: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br