Introduction

Development of Secure Software

Frank Piessens

Cyber security / computer security

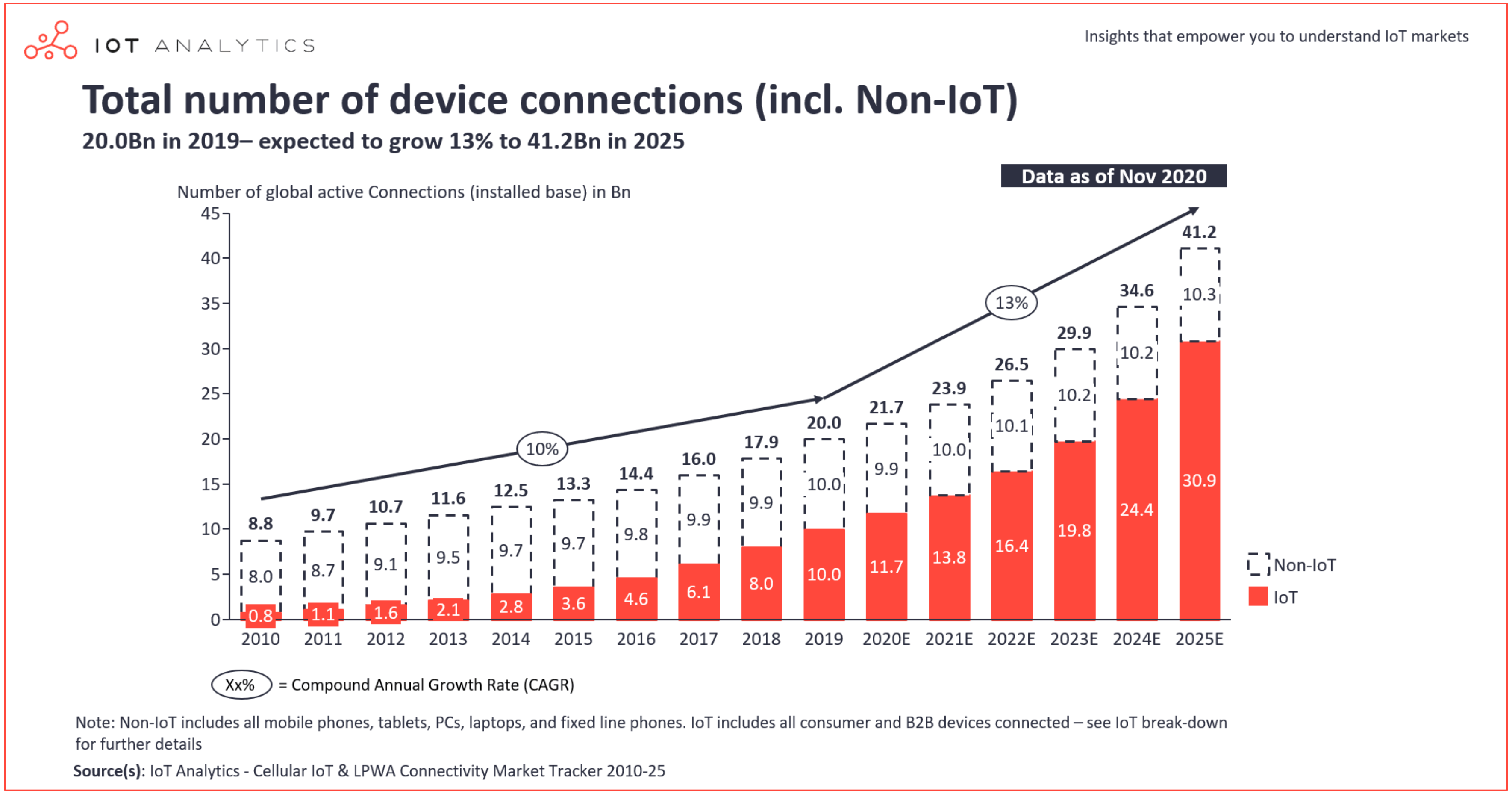
- The art, science and engineering of protecting computer-related **assets**
- Such assets include:
    - Data, information
    - Computer hardware, software or services
    - Electronic communication
    - Computer-controlled physical world devices
    - …
- Recent evolution of *cyberspace* has significantly increased the risk to such assets
- **Software security** is one of the key issues

Overview

- The evolution of cyberspace
- Examples of cybersecurity incidents
  - Malware, viruses, worms
  - Defacements
  - Jailbreaking, rooting
  - Data leaks
  - Online scams
- What are the underlying causes?
- Conclusion

The evolution of cyberspace

- More and more devices are connected to the Internet



IOT ANALYTICS

Insights that empower you to understand IoT markets

Total number of device connections (incl. Non-IoT)

20.0Bn in 2019– expected to grow 13% to 41.2Bn in 2025

Data as of Nov 2020

= Compound Annual Growth Rate (CAGR)

Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Source(s): IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker 2010-25

The evolution of cyberspace

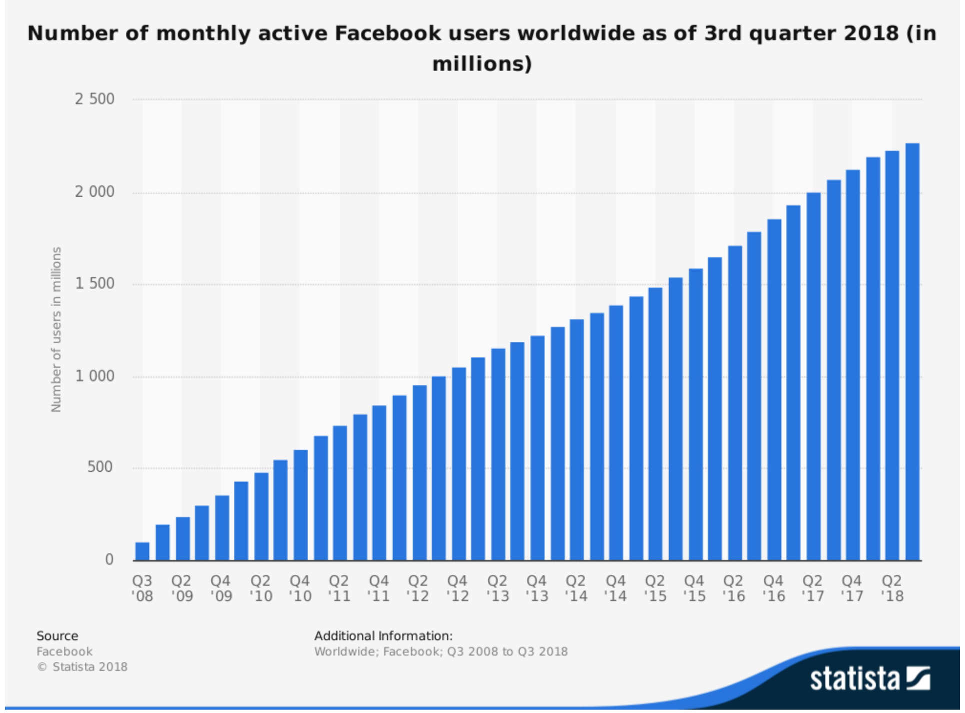
- More and more devices are connected to the Internet
- These devices run more and more software
  - Estimated lines of code:
    - Very first Unix: 2.5K (1970)
    - Space Shuttle: 400K (1981)
    - MS Windows:
      - Windows 3.1: 3M (1992)
      - Windows 95: 11M (1995)
      - Windows 7: 40M (2009)
    - Android (2010): 12M
    - Debian/GNU Linux
      - Debian 2 (1998): 35M
      - Debian 3 (2002): 140M
      - Debian 8 (2015): 850M
      - Debian 11 (2021): 1240M
    - Google online services (2015): 2000M

Sources:

https://github.com/dspinellis/unix-history-repo/tree/Research-V1-Snapshot-Development
https://www.nasa.gov/mission_pages/shuttle/flyout/flyfeature_shuttlecomputers.html
https://www.nytimes.com/1995/07/31/business/microsoft-s-mobilization-overview-windows-of-opportunity-for-microsoft.html
https://www.gubatron.com/blog/2010/05/23/how-many-lines-of-code-does-it-take-to-create-the-android-os/
https://sources.debian.org/stats/
https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place/

The evolution of cyberspace

- More and more devices are connected to the Internet
- These devices run more and more software
- Software applications can have billions of users



Number of monthly active Facebook users worldwide as of 3rd quarter 2018 (in millions)

Source
Facebook
© Statista 2018

Additional Information:
Worldwide; Facebook; Q3 2008 to Q3 2018

The evolution of cyberspace

- More and more devices are connected to the Internet
- These devices run more and more software
- Software applications can have billions of users
- Software applications and devices are automatically triggered
    - Business integration and application-to-application connections
    - IoT apps connect IoT devices to online services and social media
        - “Send me an e-mail whenever I park my car with a map where I am parked”

The evolution of cyberspace

- More and more devices are connected to the Internet
- These devices run more and more software
- Software applications can have billions of users
- Software applications and devices are automatically triggered
  - Business integration and application-to-application connections
  - IoT apps connect IoT devices to online services and social media
    - “Send me an e-mail whenever I park my car with a map where I am parked”
- The impact of software failures on our life grows more and more

Conclusions

- The ongoing trends of:
  - More computing devices,
  - with more and more software,
  - and more and more connectivity and users,
  - and an increasing impact on society and daily life

  lead to a substantial increase in risk
- The field of **cybersecurity** studies these risks and how to deal with them

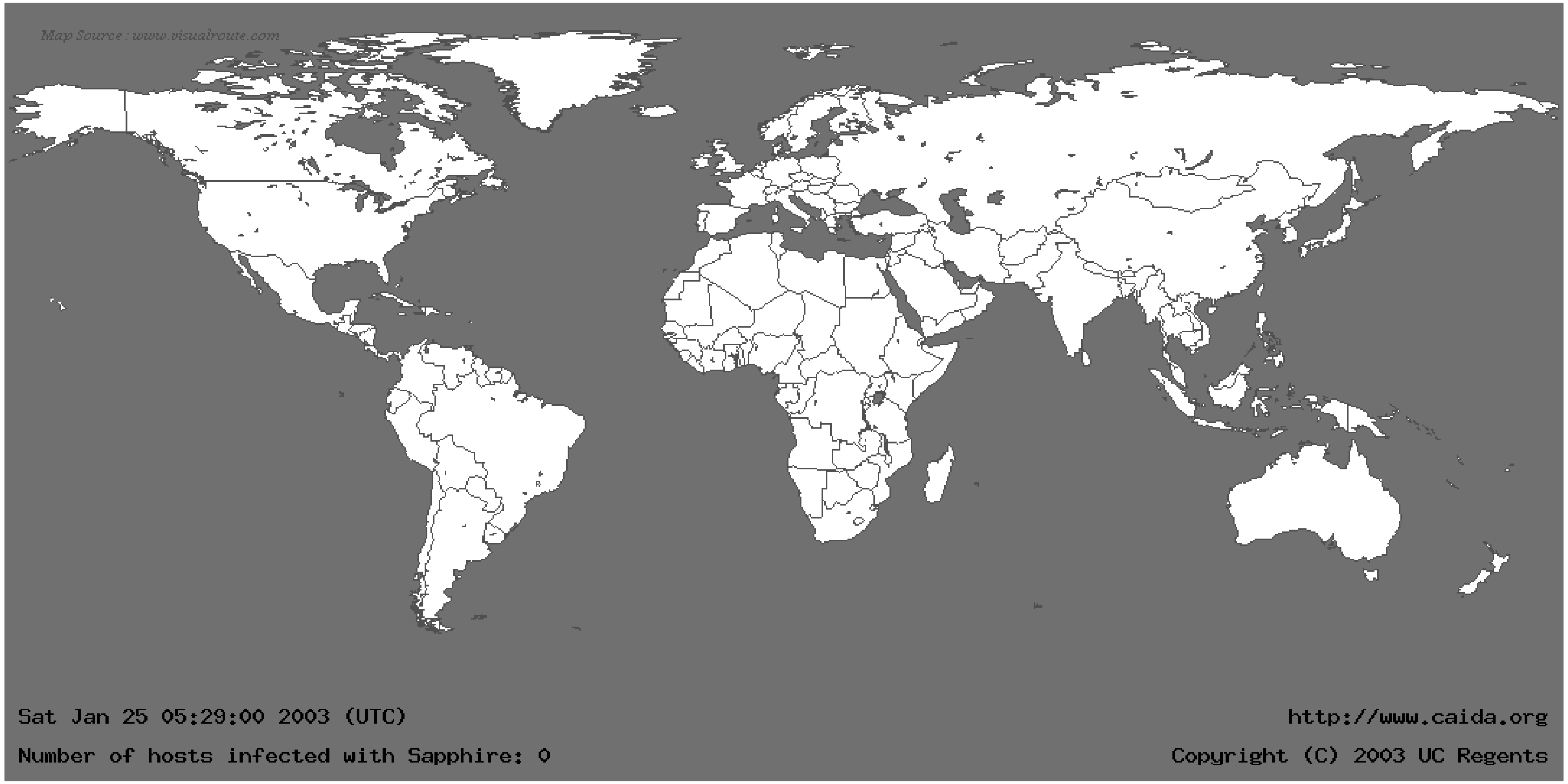
Overview

- The evolution of cyberspace
- Examples of cybersecurity incidents
  - Malware, viruses, worms
  - Defacements
  - Jailbreaking, rooting
  - Data leaks
  - Online scams
- What are the underlying causes?
- Conclusion

Example 1: Malware

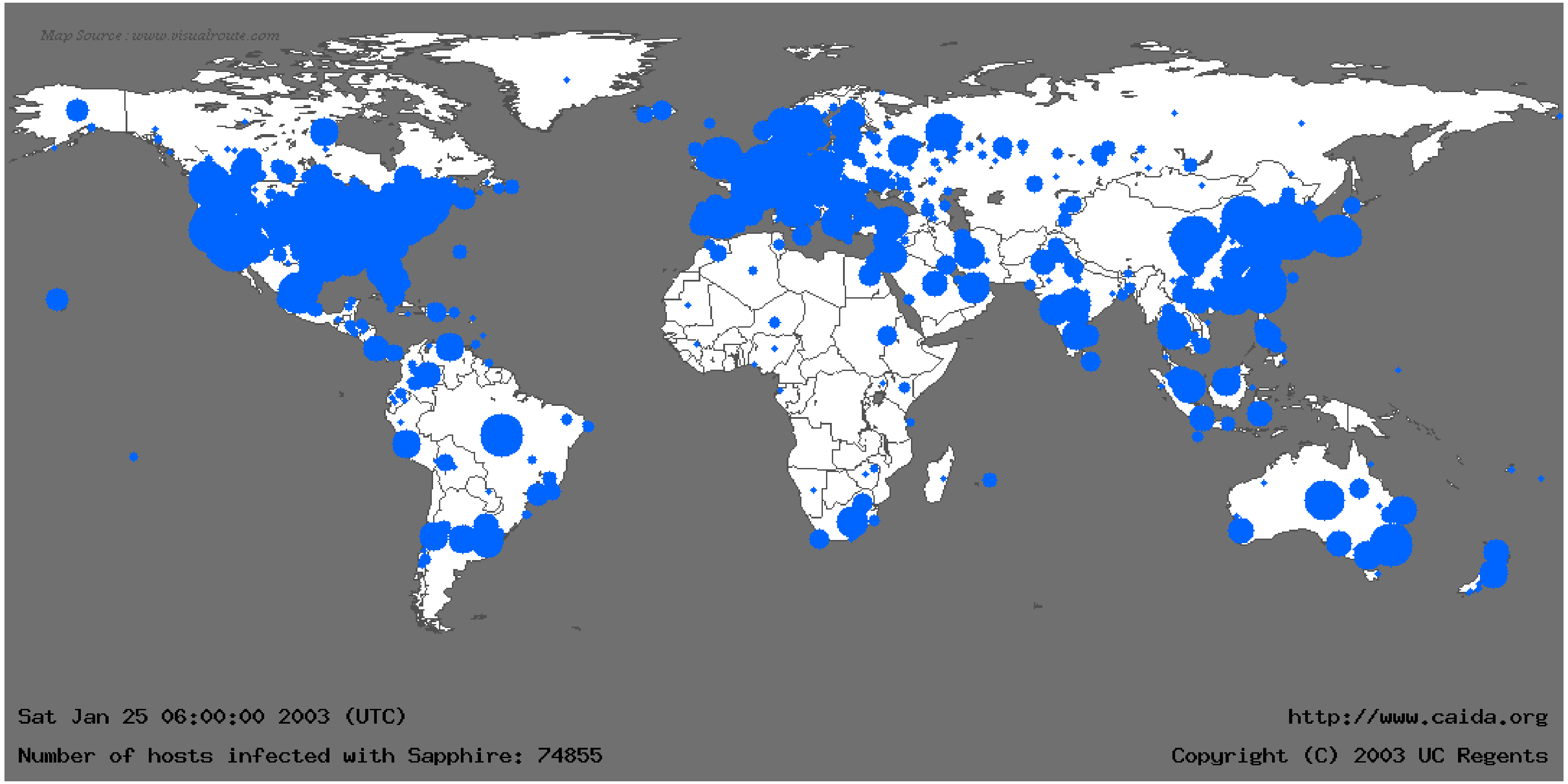
- Definitions:
    - **Virus:** Computer program (typically harmful) that can infect other programs. Viruses can replicate and spread to other machines through physical carriers (e.g., USB sticks, floppy disks) or over the network (e.g., e-mail viruses).
    - **Worm**: Self-replicating virus: no user action required to spread the infection
- Early history of malware:
    - First virus: 1982, Elk Cloner infects Apple II machines
    - First worm: 1988, Morris worm crashed 10% of the Internet

Slammer Worm (January 2003)


Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
http://www.caida.org
Number of hosts infected with Sapphire: 0
Copyright (C) 2003 UC Regents

Source: The Spread of the Sapphire/Slammer Worm, by David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver

Slammer Worm (January 2003)


Map Source : www.visualroute.com
Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

Source: The Spread of the Sapphire/Slammer Worm, by David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver

Stuxnet (2010)

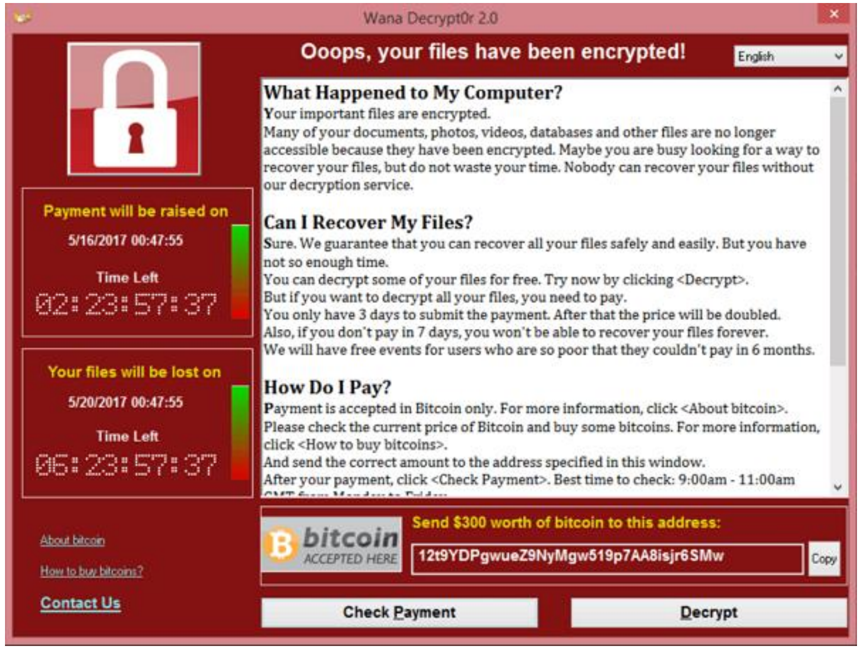
- Stuxnet is a computer worm used as a cyber-weapon by the Americans/Israelis:
  - The worm spread stealthily trying to reach one of Iran’s nuclear enrichment facilities
  - Once it reached the facility, it stealthily destroyed the centrifuges by manipulating their rotation speeds of the centrifuges
- Stuxnet showed how cyber-attacks could be used to do damage to physical infrastructure
- With the move to “internet-enable” industrial control systems and with the Internet-of-things, the reach of malware has expanded significantly

Malware: current trends

- Malware is developed by:
    - Criminals, for a variety of purposes:
        - Stealing banking credentials, sending spam, ransomware, denial-of-service attacks, crypto-mining, …
        - Creation of botnets that can be “rented” on underground markets
    - Nation states, for:
        - Collecting intelligence
        - Cyber-offensive operations
- Some important recent incidents:
    - Malware developed by the NSA, and leaked by Russian(?) hackers is used by other actors:
        - Wannacry (May 2017): likely North Korea, ransomware(?)
        - NotPetya (June 2017): most expensive cyber-attack so far, a Russian attack on Ukraine
- **Supply chain attacks** further increase the scale and reach of malware
    - Attacks where the attacker compromises a component provided to the victim by a third-party
        - E.g., the SolarWinds hack in 2020

Ransomware (data from 2019)

- 60 out of 100 Belgian companies polled were affected by a ransomware attack
- Average cost of recovering from an attack was estimated at $760.000
- Approx. one quarter of victims pays the ransom
- Sources:
  - https://cybersecurity-bites.be/ict-beheer/anatomie-van-een-ransomware-aanval/
  - https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

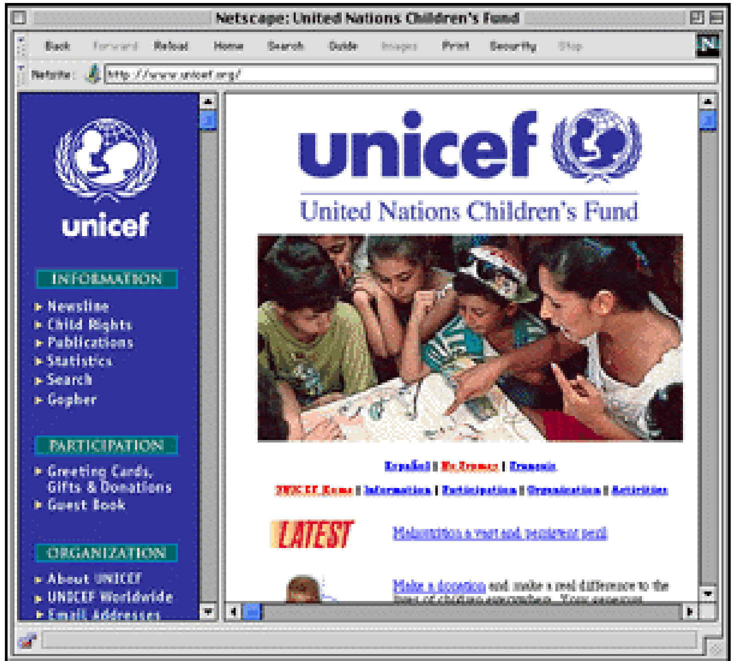
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

The SolarWinds hack (2020)

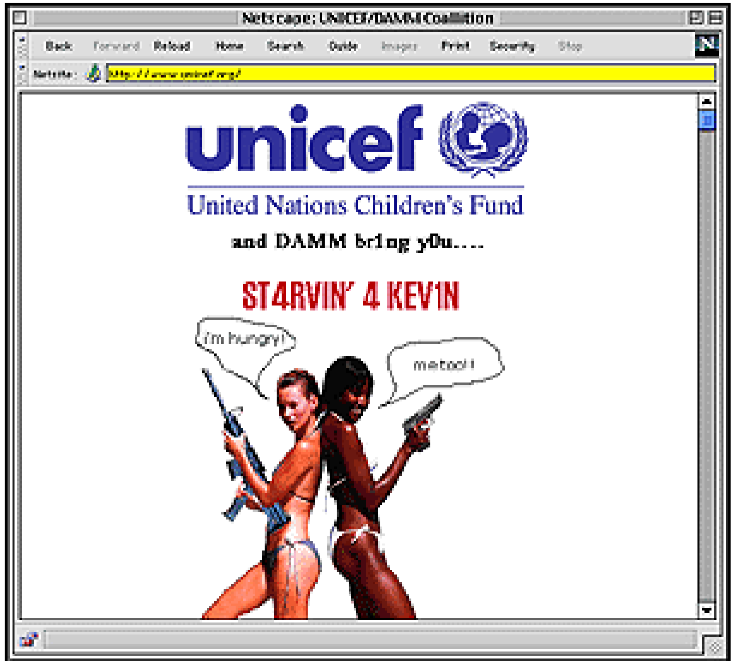
- Attackers compromised the build system of SolarWinds and planted a **Trojan** in network monitoring software developed by SolarWinds
- The trojanized software was distributed through the software updating mechanism to clients, where it could access confidential data
    - Among the victims were the US federal government, NATO and the European Parliament
    - The hackers had access to victim data for several months
- The attack is believed to be a foreign nation attack, most likely performed by the Russians
- More information:
    - https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

Example 2: Defacements

- A defacement is an attack where the attacker modifies the appearance of a web site.
- Defacements are almost as old as the Web itself.
- Example: Unicef defacement (Jan 1998):

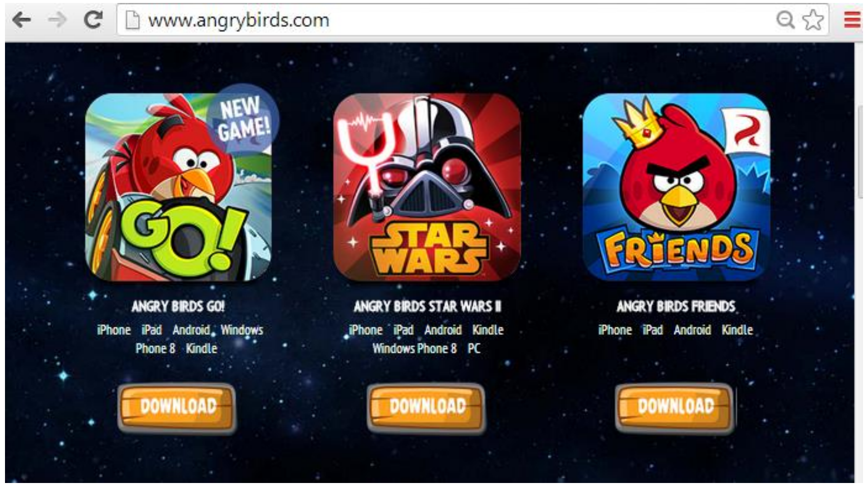

Netscape: United Nations Children's Fund
Back
Forward
Reload
Home
Search
Guide
Images
Print
Security
Stop
Netsite:
http://www.unicef.org/
unicef
United Nations Children's Fund
INFORMATION
Newsline
Child Rights
Publications
Statistics
Search
Gopher
PARTICIPATION
Greeting Cards, Gifts & Donations
Guest Book
ORGANIZATION
About UNICEF
UNICEF Worldwide
Email Addresses
Español | En Français | Français
UNICEF Home | Information | Participation | Organization | Activities
LATEST
Malnutrition: a vast and persistent peril

Make a donation and make a real difference to the lives of children everywhere. Your generous

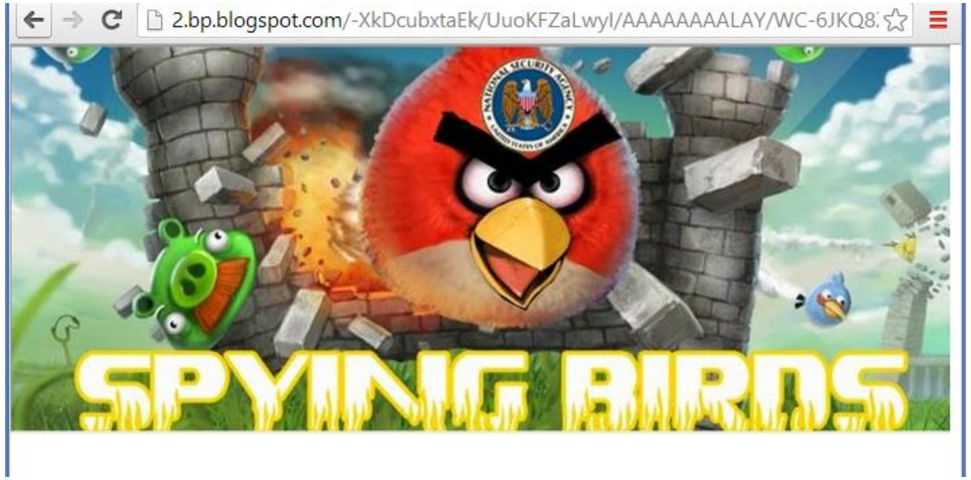


Defacements are still going strong

- After Ed Snowden's revelation in 2013 that NSA and GCHQ take advantage of smartphone apps

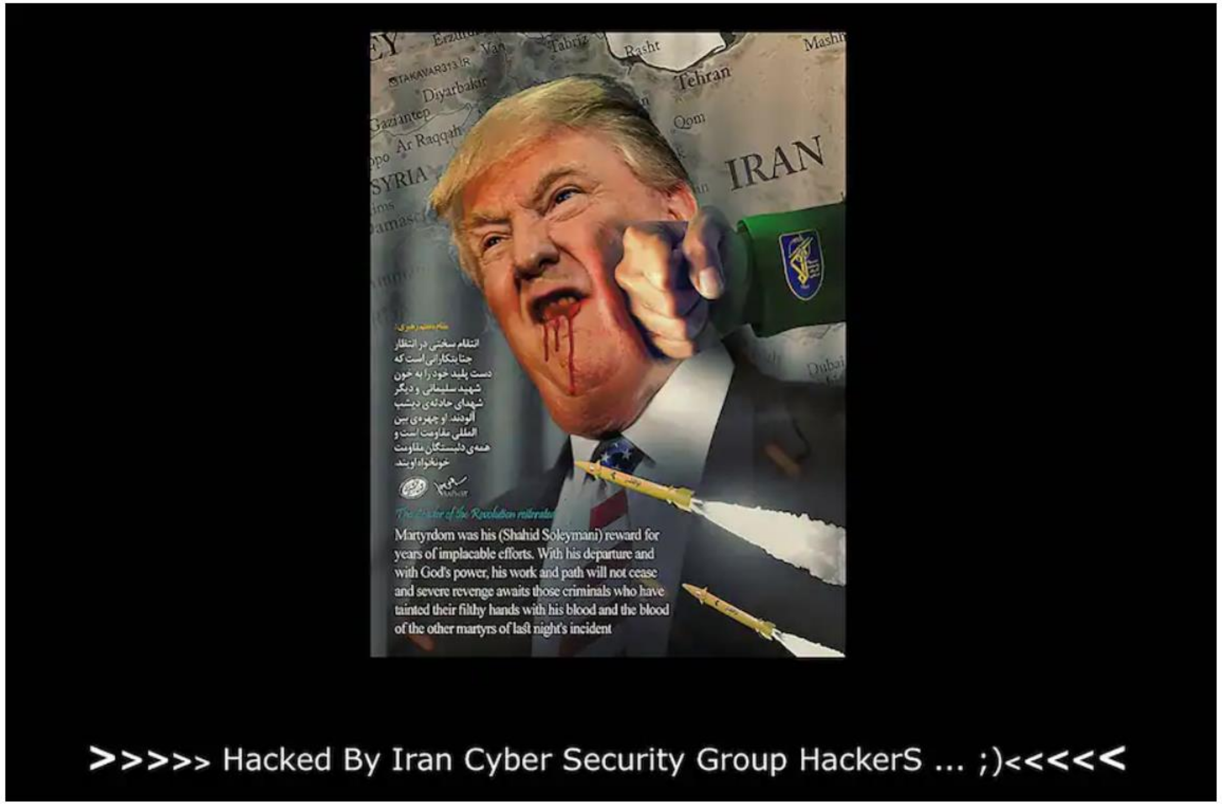


⇨


2.bp.blogspot.com/-XkDcubxtaEk/UuoKFZaLwyl/AAAAAAAALAY/WC-6JKQ8
SPYING BIRDS

Defacements are still going strong

- Jan 2020, after the US takes out general Soleimani



پیام مهم رهبری:

انتقام سختی در انتظار
جنایتکارانی است که
دست پلید خود را به خون
شهید سلیمانی و دیگر
شهدای حادثه‌ی دیشب
آلودند. او چهره‌ی بین
المللی مقاومت است و
همه‌ی دلبستگان مقاومت
خونخواه اویند.

The Leader of the Revolution reiterated

Martyrdom was his (Shahid Soleymani) reward for years of implacable efforts. With his departure and with God's power, his work and path will not cease and severe revenge awaits those criminals who have tainted their filthy hands with his blood and the blood of the other martyrs of last night's incident

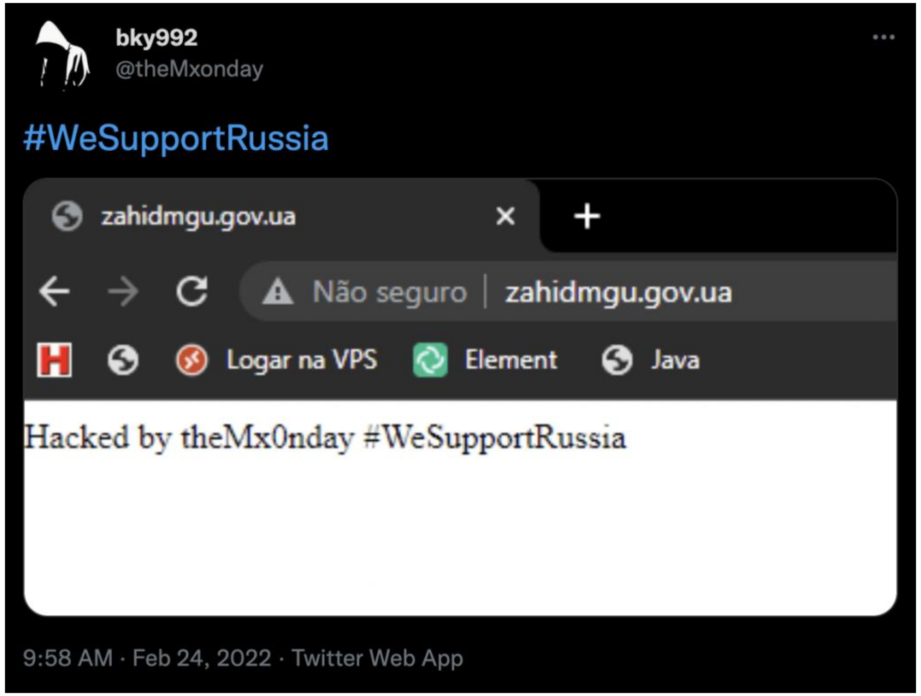
>>>>> Hacked By Iran Cyber Security Group HackerS ... ;)<<<<<

This image taken Saturday shows the U.S. Federal Depository Library Program's website after a group claiming to be hackers from Iran breached it and posted messages vowing revenge for Washington's killing of top military commander Qasem Soleimani. (Federal Depository/AFP/Getty Images)

(Source: The Washington Post, Jan 6, 2020

Defacements are still going strong

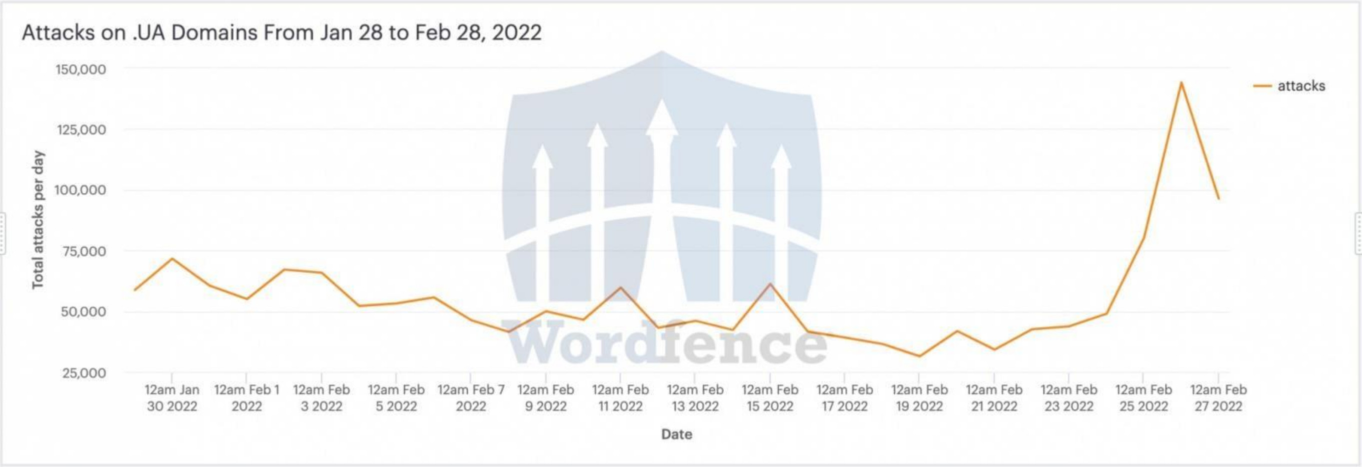
- Massive defacements accompanied the Russian invasion in Ukraine (Feb 24, 2022)


bky992
@theMxonday

#WeSupportRussia

Hacked by theMx0nday #WeSupportRussia

9:58 AM · Feb 24, 2022 · Twitter Web App



Source: https://www.bleepingcomputer.com/news/security/ukrainian-sites-saw-a-10x-increase-in-attacks-when-invasion-started/

Example 3: Jailbreaking / rooting

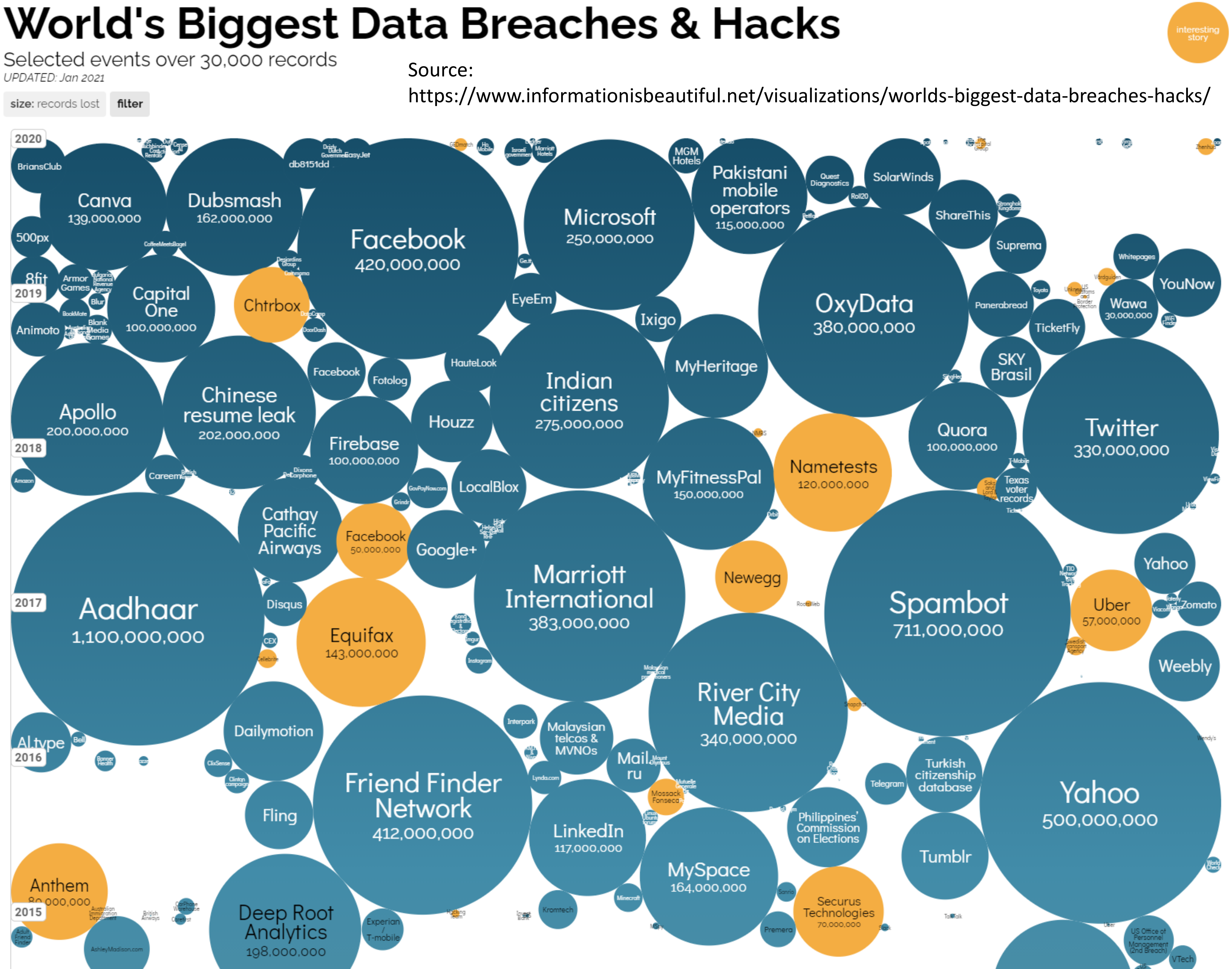
- Jailbreaking or rooting refers to the act of escalating privileges on a “closed” device such as a smartphone or game console
- Users of these devices do this to, for instance:
  - Remove restrictions on the telecom carrier they can use
  - Bypass DRM restrictions or censorship
  - Customize the device to an extent not allowed by the closed device
- Time-to-first-jailbreak for various devices ranges between 0 days and 100-200 days.

The 2011 Sony hack

- Sony attempts to limit jailbreaking of the PlayStation by suing George Hotz (who published jailbreaking code online)
- This move leads to a massive retaliation by the hacker community:
  - Anonymous launches a series of Denial-Of-Service attacks
  - Unknown hackers break into various Sony networks and steal millions of users personal information
  - Sony is forced to shut down the PlayStation network for days

Example 4: Large scale data leaks

- Security incidents where a large amount of confidential data leaks to unauthorized parties, for instance:
  - Stealing of account databases by hackers
    - E.g., Data (including hashed passwords) for billions (!) of accounts were stolen from Yahoo in 2013/2014
    - https://haveibeenpwned.com/
  - The Facebook / Cambridge Analytica scandal
    - A survey app developed by Cambridge Analytica harvested data about Facebook users (with consent) as well as from their friends (without consent)
    - This data was used to influence elections, including the presidential elections in the US and the Brexit vote in the UK



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Jan 2021

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's Biggest Data Breaches & Hacks

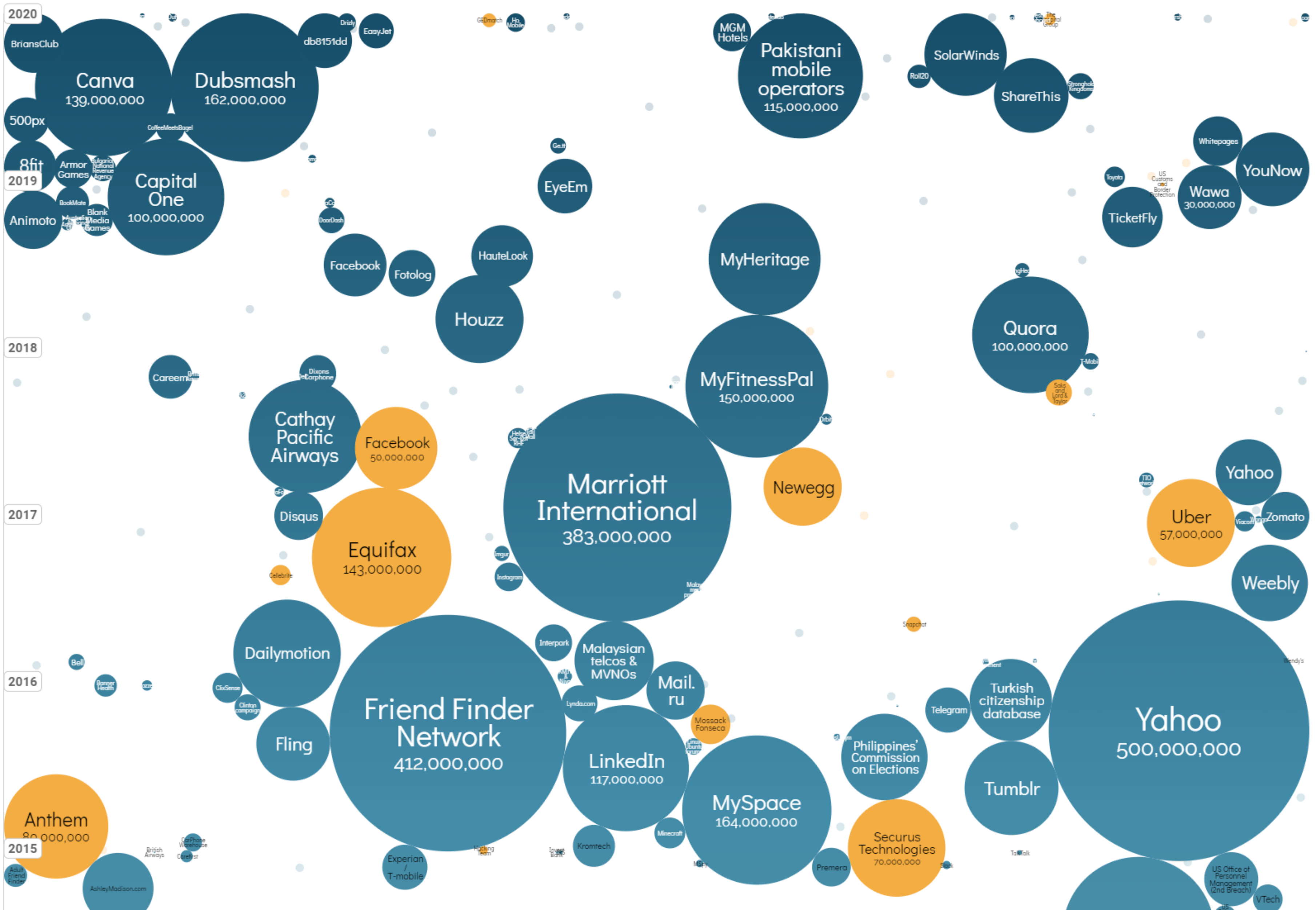
Selected events over 30,000 records

UPDATED: Jan 2021

size: records lost **filter:** hacked

interesting story

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Example 5: Online scams

- Phishing:
  - Stealing of credentials (usually for banking website) by means of mail and/or web site spoofing
  - See the Pano 2021 documentary:
    - https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/
- Catfishing:
  - Creating a fake profile on a social networking service to compromise other users of that service, e.g., to blackmail them later
  - Some famous cases of Belgian celebrities being catfished in 2020

Overview

- The evolution of cyberspace
- Examples of cybersecurity incidents
  - Malware, viruses, worms
  - Defacements
  - Jailbreaking, rooting
  - Data leaks
  - Online scams
- What are the underlying causes?
- Conclusion

Underlying causes

- We have discussed a wide range of examples of cybersecurity incidents
- Why can these incidents happen? What are the root causes? What are the weak links?
- Many answers are possible, but two weak links are widely acknowledged

Weak link 1 = People

- People are terrible from the point of view of security
    - Choice and management of passwords
    - Security configurations
    - Irresponsible behavior
    - Social engineering

Exploiting human weaknesses

2019 McAfee®
Most Dangerous Celebrities™

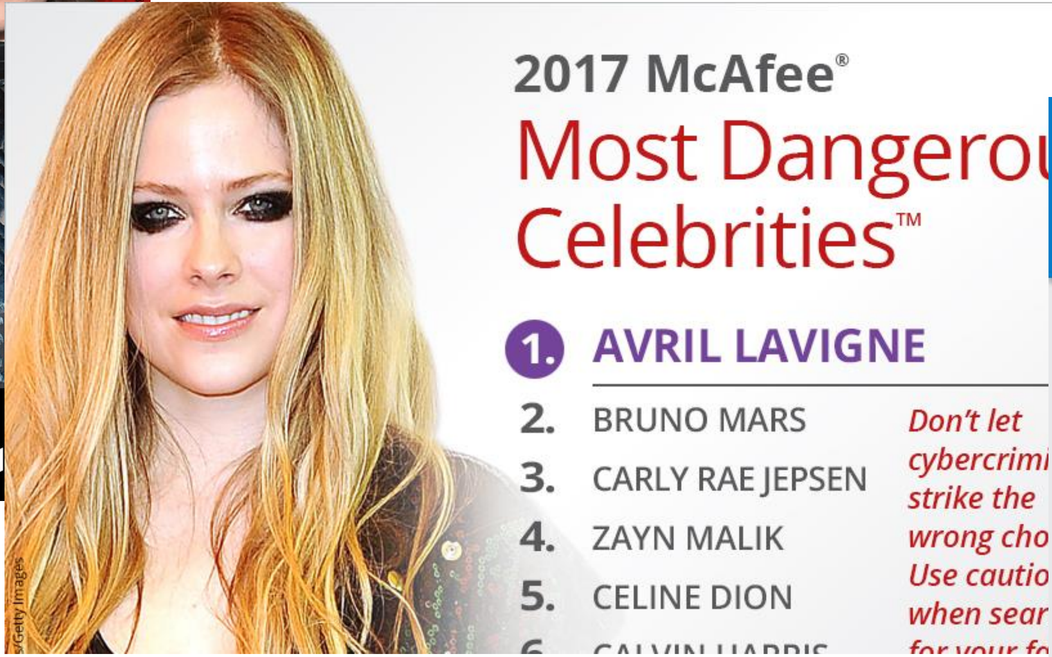
1 〉 ALEXIS BLEDEL
2 〉 James Corden
3 〉 Sophie Turner
4 〉 Anna Kendrick
5 〉 Lupita Nyong'o
6 〉 Jimmy Fallon
7 〉 Jackie Chan
8 〉 Lil Wayne
9 〉 Nicki Minaj
10 〉 Tessa Thompson

Cybercriminals love celebrities too. *Think before you click.*

Based on the percentage of sites identified in August 2019 by McAfee WebAdvisor as “risky” which are included in the search results for a celebrity’s name and commonly associated terms.

https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/most-dangerous-celebrities-2019/

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others. Copyright © 2019 McAfee LLC



2017 McAfee®
Most Dangerou
Celebrities™

1. AVRIL LAVIGNE
2. BRUNO MARS
3. CARLY RAE JEPSEN
4. ZAYN MALIK
5. CELINE DION
6. CALVIN HARRIS

Don't let cybercrimi strike the wrong cho Use cautio when sear for your fa

2020 McAfee®
Most Dangerous Celebrities™

Anna Kendrick
2. Sean Combs
3. Blake Lively
4. Mariah Carey
5. Justin Timberlake
6. Taylor Swift
7. Jimmy Kimmel
8. Julia Roberts
9. Kate McKinnon
10. Jason Derulo

Cybercriminals love celebrities too. *Think before you click.*

Based on the percentage of sites identified in August 2020 by McAfee WebAdvisor as "risky" which are included in the search results for a celebrity's name and commonly associated terms.

https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/most-dangerous-celebrities-2020/

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others. Copyright © 2020 McAfee LLC

McAfee

2015 Most Dangerous Celebrities™

1 Armin van Buuren
2 Luke Bryan
3 Usher
4 Britney Spears
5 Jay Z
6 Katy Perry
7 Amy Schumer
8 Betty White
9 Lorde
10 Nina Dobrev

You're not the only one who loves news about today's stars.

Cybercriminals often use stars' popularity in search results to expose you to malware.

intel Security

Logan Fazio/Getty Images

Based on the percentage of sites identified by McAfee® WebAdvisor as 'risky' which are included in the search results for a celebrity's name and commonly associated terms.

Exploiting human weaknesses

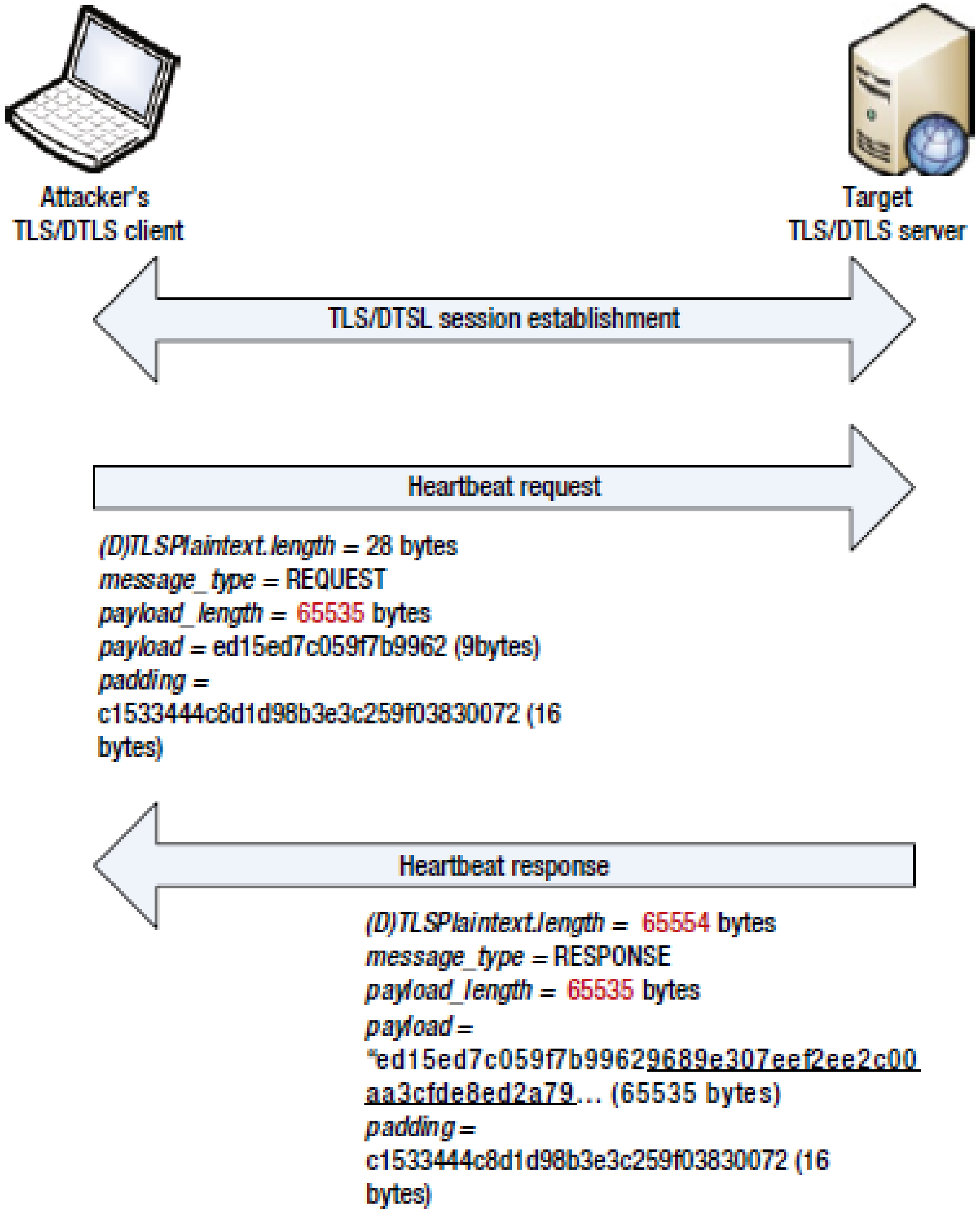
- A good way to break into a large organization’s network is to compromise key technical people (system administrators)
  - Getting their credentials
  - Getting them to do your bidding
- This can be achieved in many ways
  - Spear-phishing
    - Phishing attack tuned to a specific target
  - Bribing
  - Blackmail
  - …

Weak link 2 = software

- Software vulnerability =
  - A defect in software code (a bug) that can be exploited by an attacker to break some security objective of the software
- Around 100.000 such vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) list:
  - Buffer overflows, SQL injection, cross-site scripting, race conditions, side-channel vulnerabilities, information leaks, incomplete access mediation, cross-site scripting, double free, . . .

Example: memory management vulnerabilities

- (aka: memory safety vulnerabilities)
- Some programming languages do not check the validity of memory accesses, and hence buggy programs can read or write memory areas they are not supposed to access
- Heartbleed (2014) was such a bug in OpenSSL, a popular cryptographic library
- Attackers could trigger out-of-bound reads, that could potentially leak cryptographic key material



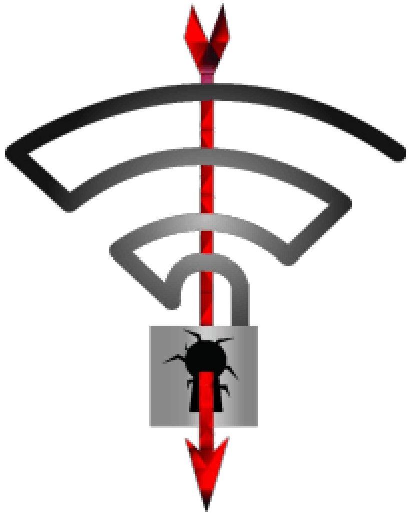
(D)TLSPlaintext.length = 28 bytes
message_type = REQUEST
payload_length = 65535 bytes
payload = ed15ed7c059f7b9962 (9bytes)
padding =
c1533444c8d1d98b3e3c259f03830072 (16
bytes)

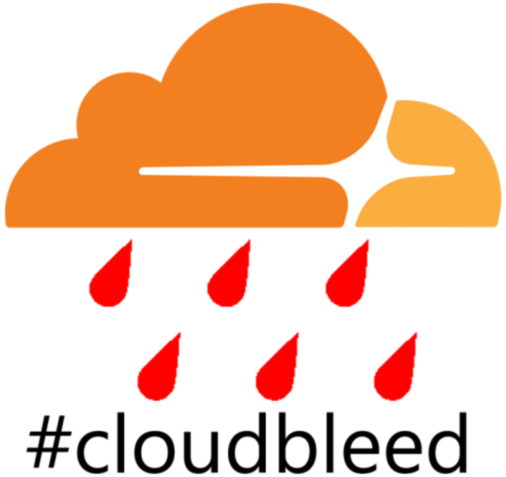
(D)TLSPlaintext.length = 65554 bytes
message_type = RESPONSE
payload_length = 65535 bytes
payload =
"ed15ed7c059f7b99629689e307eef2ee2c00
aa3cfde8ed2a79... (65535 bytes)
padding =
c1533444c8d1d98b3e3c259f03830072 (16
bytes)

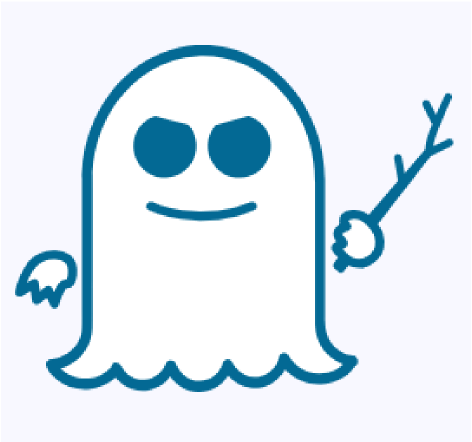
Source: Platform Embedded Security Technology Revealed (Xiaoyu Ruan)

Heartbleed initiated a trend of “marketing” vulnerabilities

STAGEFRIGHT







Example vulnerability: Android Stagefright

- A bug in the Android operating system
  - Discovered in 2015, affected more than a billion devices
  - Present since 2010
- On a vulnerable system:
  - An attacker can do anything on the phone, just by sending a malicious MMS message

Example: structured output generation vulnerabilities

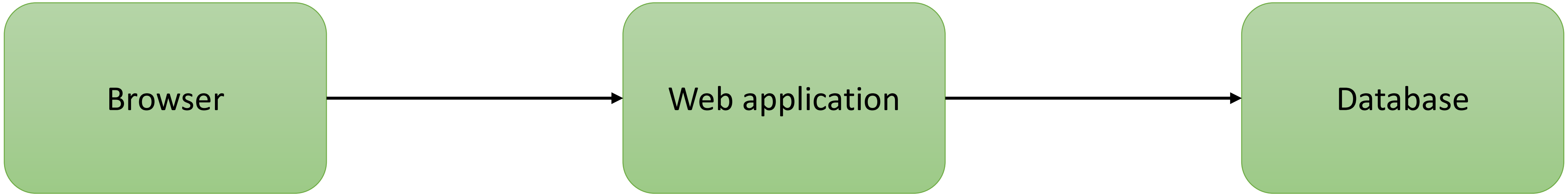
- (aka: injection vulnerabilities)
- Programs often construct structured output (e.g., SQL) using string concatenation
- When some of the strings can be chosen by an attacker, maliciously chosen values can change the structure of the output in unintended ways
- Examples: SQL injection, script injection (XSS), command injection, …

Software vulnerabilities and exploitation

- A single vulnerability can possibly give an attacker complete control over a system
    - “Hacking”, “Exploiting”, “Pwning”, … a system
- This is a significant contributor to risk in cybersecurity
    - Your phone can be turned into a monitoring device
    - Your PC can be turned into a cyberweapon in the hands of someone else

Example: SQL injection attack

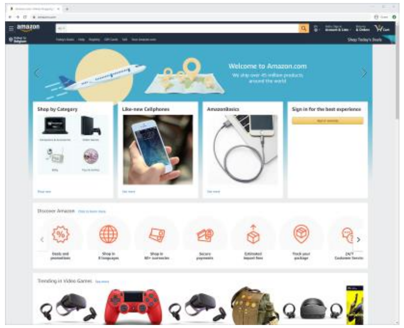
- How can simple “bugs” have such serious consequences?
- Let’s look at a “simple” class of vulnerabilities



Browser

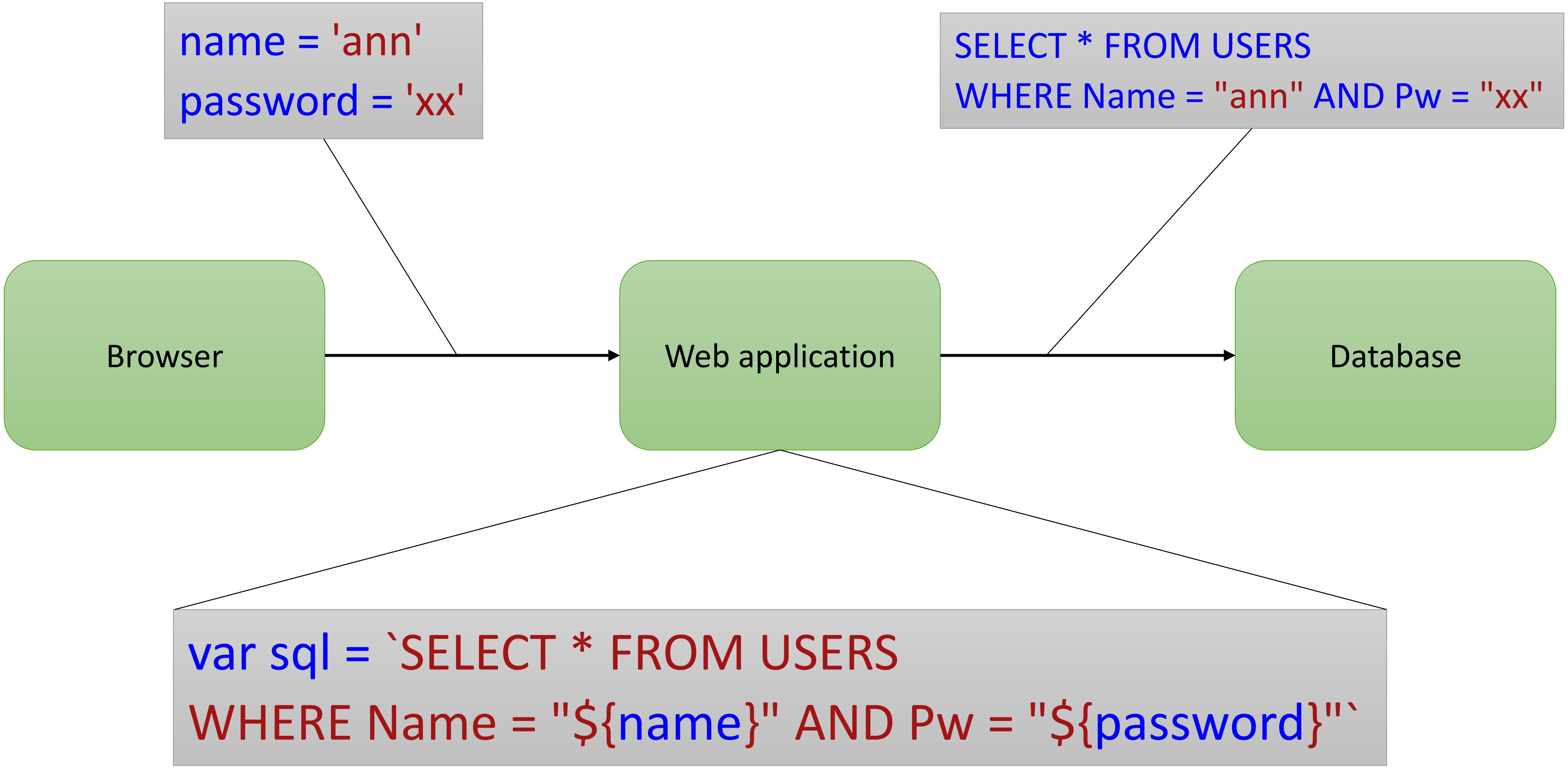
Web application

Database



“business logic”: software that determines how to respond to user input

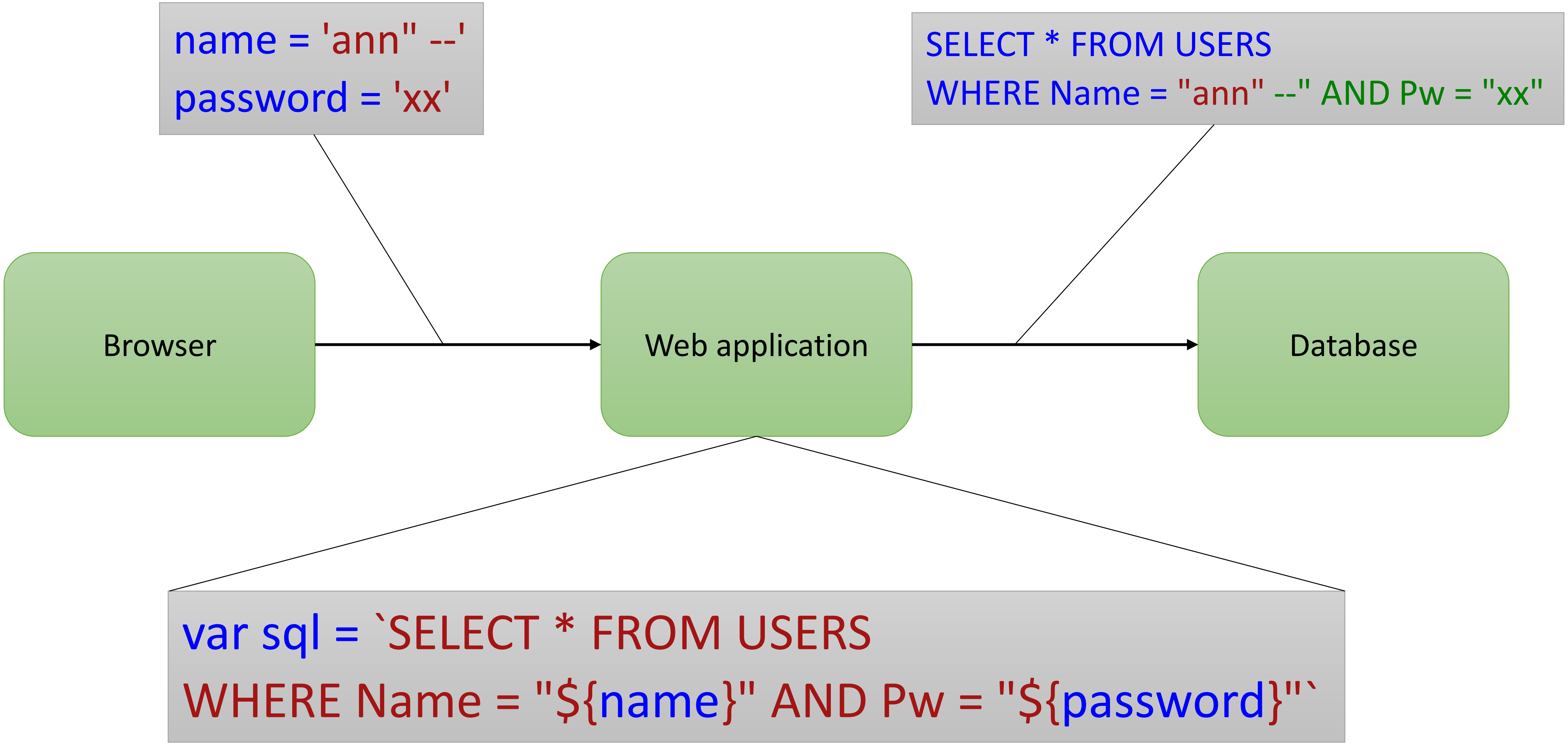
“persistent data”: tables with products, prices, customer information,…



```
name = 'ann'
password = 'xx'
```

```
SELECT * FROM USERS
WHERE Name = "ann" AND Pw = "xx"
```

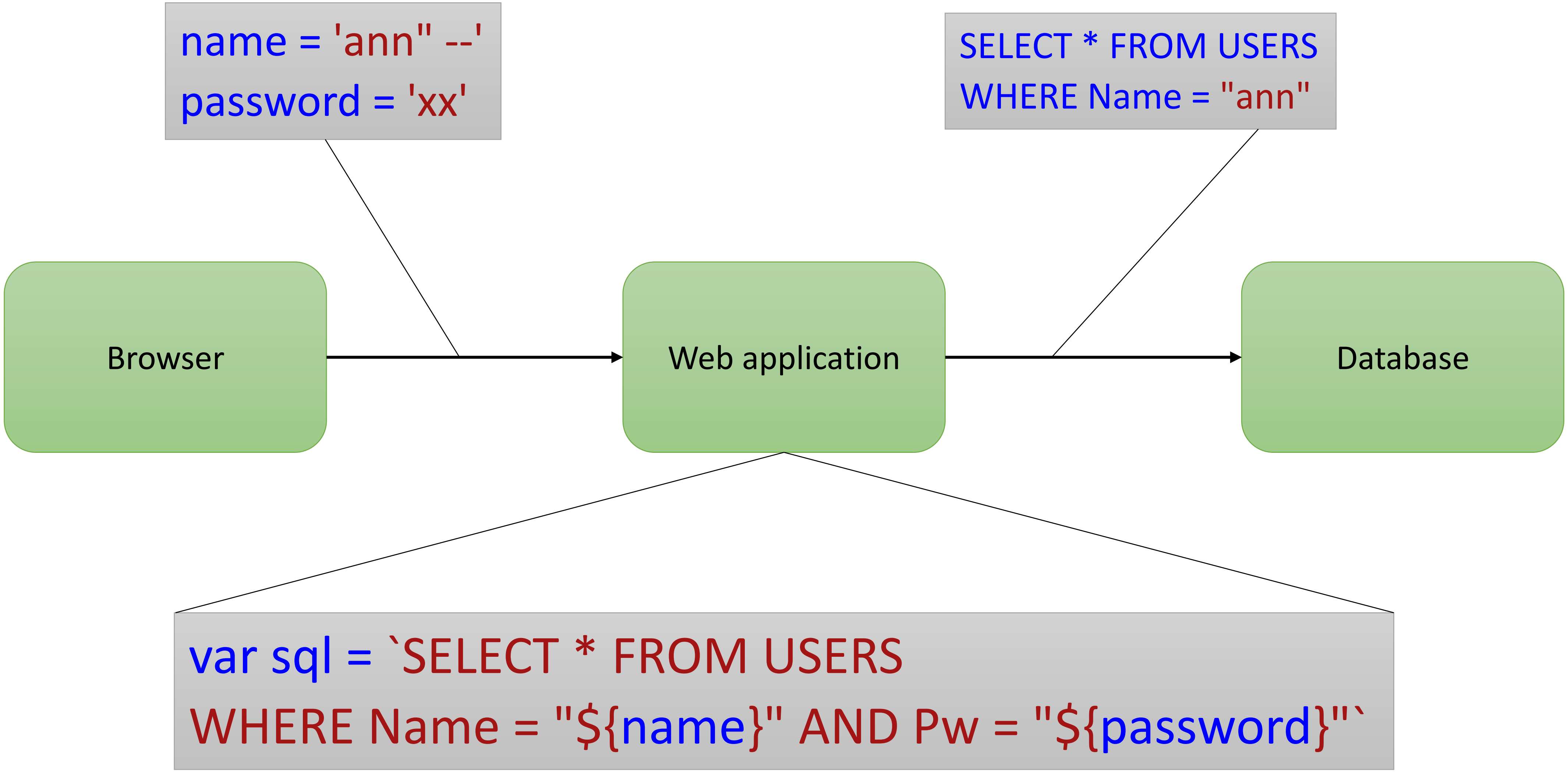
```
var sql = `SELECT * FROM USERS
WHERE Name = "${name}" AND Pw = "${password}"`
```



```
name = 'ann" --'
password = 'xx'
```

```
SELECT * FROM USERS
WHERE Name = "ann" --" AND Pw = "xx"
```

```
var sql = `SELECT * FROM USERS
WHERE Name = "${name}" AND Pw = "${password}"`
```



```
name = 'ann" --'
password = 'xx'
```

Browser

Web application

Database

```
SELECT * FROM USERS
WHERE Name = "ann"
```

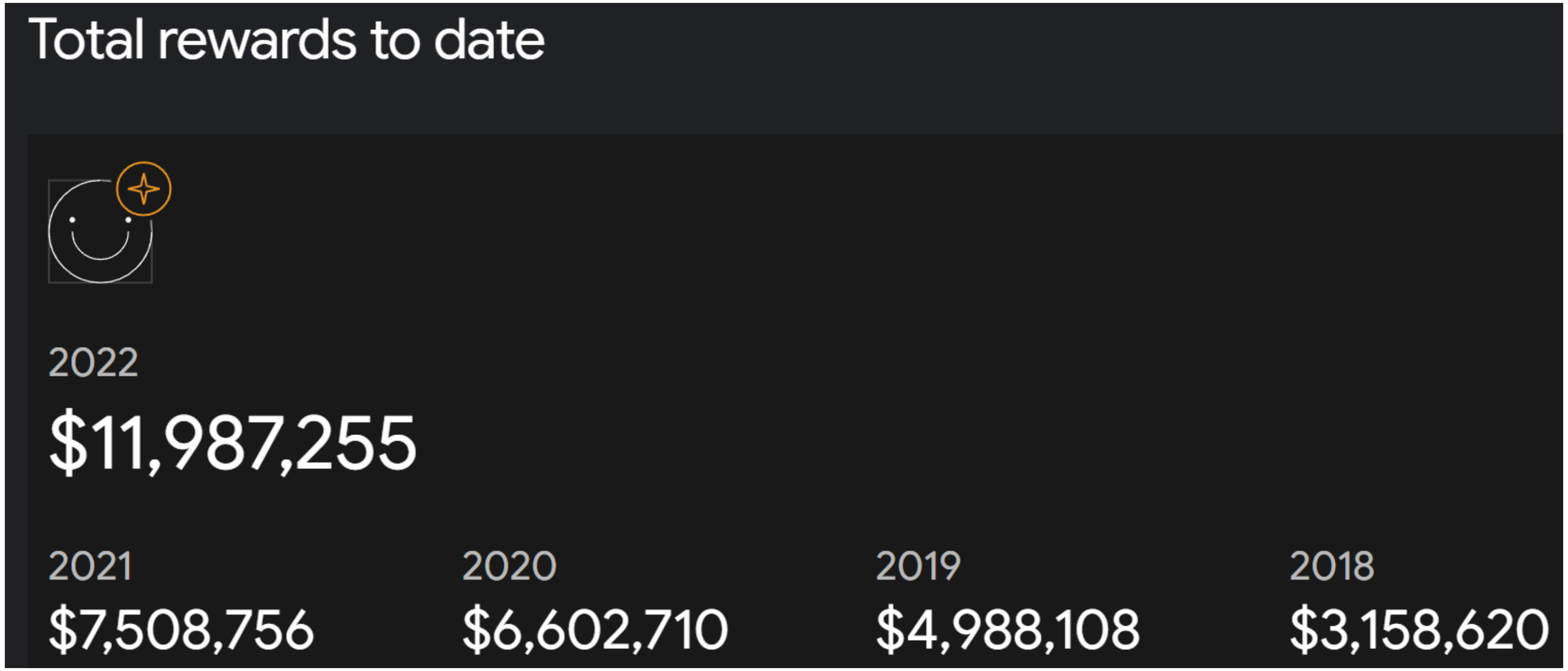
```
var sql = `SELECT * FROM USERS
WHERE Name = "${name}" AND Pw = "${password}"`
```

Zero-day vulnerabilities

- A **zero-day vulnerability** is a vulnerability in a hardware/software product that the manufacturer of the product is not aware of
- A zero-day in a widely used system is dangerous and powerful: it can be used to break into and control that system
- Consequently, these vulnerabilities have also become very valuable to various stakeholders:
  - Law enforcement / intelligence services: to get access to intelligence on criminals or other nations
  - The military: as cyberweapons
  - Criminals: to build malware
- What to do if you find one?

Sell it to manufacturer: Bug bounty programs

- E.g., Google Bug Hunters program:



Total rewards to date

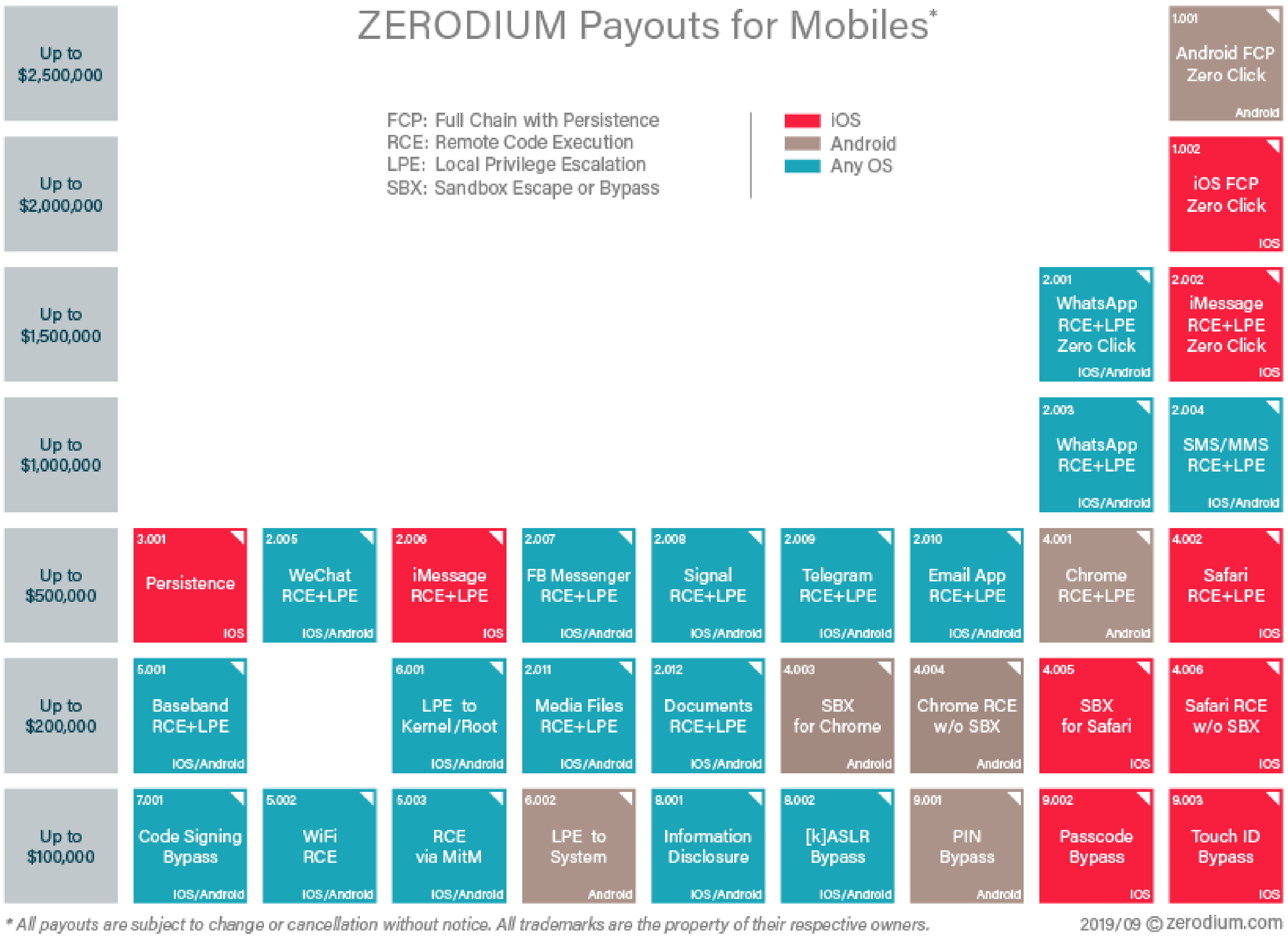
2022

$11,987,255

2021	2020	2019	2018
$7,508,756	$6,602,710	$4,988,108	$3,158,620

- Brokers make it easy to enter such bug bounty programs:
  - https://www.intigriti.com/
  - https://www.hackerone.com/

Sell it as a weapon, e.g., Zerodium 2021



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
🟫 Android
🟦 Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

These practices raise interesting questions

- Is it legal to look for vulnerabilities?
  - It is important to find a good balance between:
    - Disallowing malicious attempts to break into a system
    - Supporting “ethical hacking”, the process of looking for vulnerabilities in systems and disclosing them to the system owner so they can be fixed
- Is it legal to sell functional exploits? Should it be?
  - At some level, a functional exploit is like a weapon
  - Both in the US and in Europe, the practice of selling exploits seems to be tolerated
- For background on the legal issues surrounding ethical hacking in Belgium:
  - https://cybersecurity-bites.be/cyberwijs/security-researching-of-ethisch-hacken-interessant-voor-uw-onderneming/

Overview

- The evolution of cyberspace
- Examples of cybersecurity incidents
  - Malware, viruses, worms
  - Defacements
  - Jailbreaking, rooting
  - Data leaks
  - Online scams
- What are the underlying causes?
- Conclusions

Conclusions

- Cybersecurity is a key concern for our always-online society
- Software vulnerabilities are an important underlying cause for cybersecurity failures
- The purpose of this course is to:
  - study these vulnerabilities in a number of important software systems
  - understand how to exploit these vulnerabilities
  - understand countermeasures that can be applied
- Recommended reading for a more systematic overview of the cyberthreat landscape:
  - Ross Anderson, Security Engineering (third edition), Chapter 2:
    - https://www.cl.cam.ac.uk/~rja14/Papers/SEv3-ch2-7sep.pdf

Practical organization of the course

- Theory:
  - Live lectures, with best-effort to record and post on Toledo
  - Mandatory and recommended reading material
  - Course Overview in Toledo summarizes all the material covered
- Project:
  - A “security game” where you practice some of the attack techniques we studied
- Grading:
  - Theory (15 out of 20 points): written closed-book exam
  - Project (5 out of 20 points): written report + oral defense