INTRODUCTION

MALWARE ANALYSIS AND INCIDENT FORENSICS
M.Sc. in Cyber Security

MALWARE ANALYSIS
M.Sc. in Engineering in Computer Science

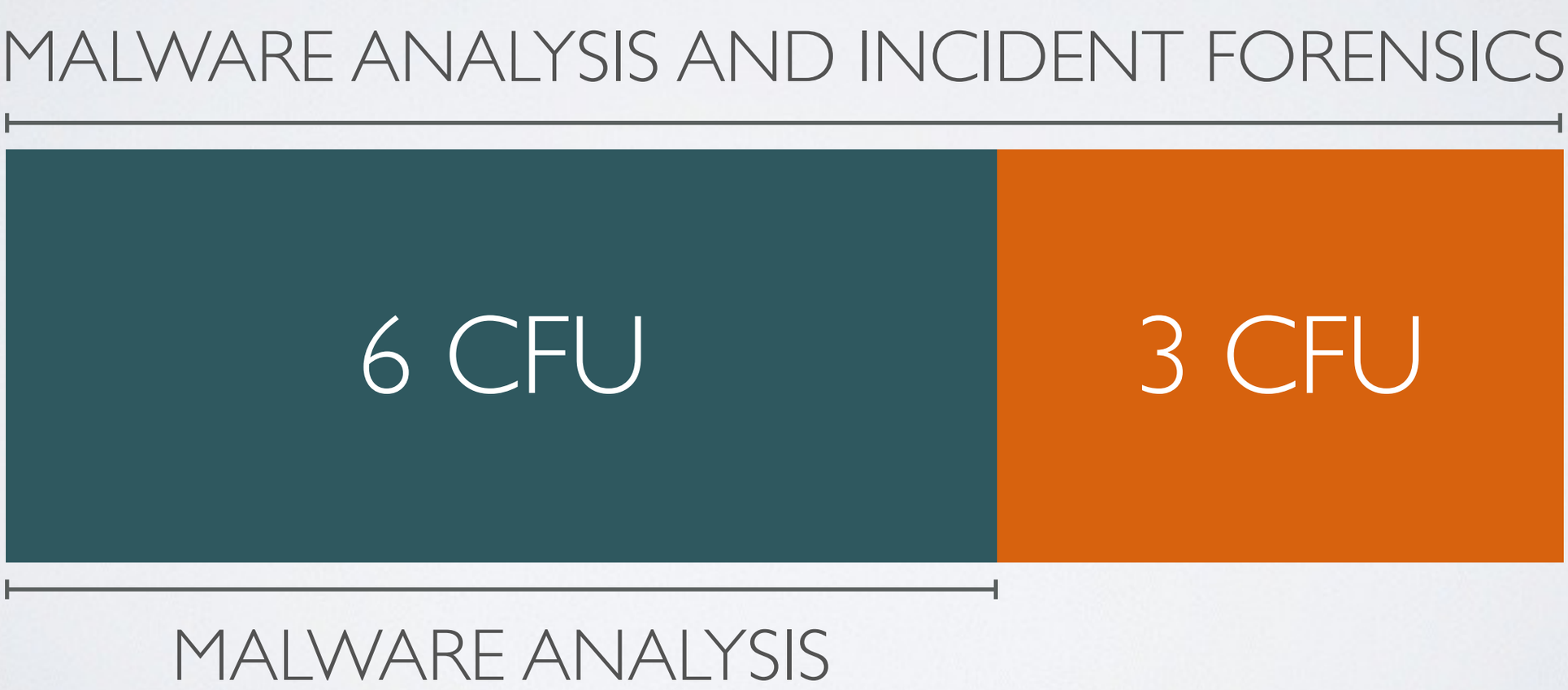
A.Y. 2025/2026

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

GENERAL INFORMATION

- Malware Analysis and Incident Forensics - 9 CFU
- Malware Analysis - 6 CFU
- First semester
  - September 23rd – December 19th



GENERAL INFORMATION

- Class Schedule
  - **Tuesday 14:00-16:00**
    MAIF & MA
    Aula 201, Building D, Viale Regina Elena

  - **Thursday 13:00-16:00**
    MAIF only
    Aula 201, Building D, Viale Regina Elena
    On some days: Aula Alfa in Via Salaria

  - **Friday 14:00-17:00**
    MAIF & MA
    Lab 16, Via Tiburtina 205

GENERAL INFORMATION

Lecturers:

Leonardo Querzoni
querzoni@diag.uniroma1.it
Office hours: online only
(appointments via mail)

6 CFU

3 CFU

Daniele Cono D'Elia
delia@diag.uniroma1.it
Office hours: online only
(appointments via mail)

GENERAL INFORMATION

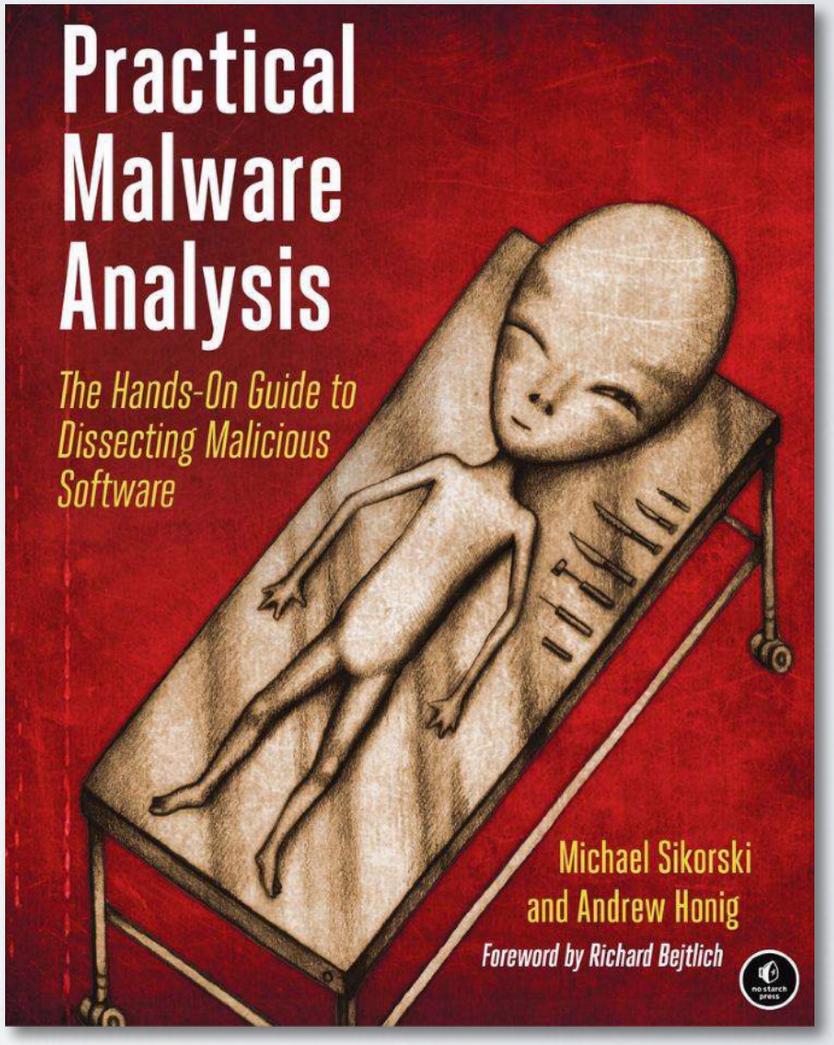
- **https://tinyurl.com/maif25enroll**
  (https://classroom.google.com/c/MjM1MjU0NTczOTVa?cjc=xay2kg64)

- Classroom code:

xay2kg64

GENERAL INFORMATION

- Textbook
  - M. Sikorski and A. Honig; Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press
- Material on Classroom
  - Slides
  - Scientific papers
  - Malware samples, code, etc.
  - Tools
  - VM for malware analysis hands-on



GENERAL INFORMATION

- Examination
  - Practical test (3h)
    - Sample that you will be asked to analyze
    - Write a report
    - Answer questions on the sample
  - Questionnaire (30 mins)
    - Only for MAIF students
    - 10 True/False questions
    - Mandatory (Pass/Fail), does not affect the grade

GENERAL INFORMATION

Expected knowledge after this course:

- Understanding basic characteristics of a cyber attack
- Knowing basic structure of a malware sample
- Performing basic static and dynamic analysis on malware with a mix of automated tools and manual reverse engineering
- Understanding the hurdles posed by anti-analysis techniques
- Understanding the basic concepts of threat intelligence (MAIF only)
- Extracting IoCs from incidents to characterize threats (MAIF only)

We will deal with Windows malware only

- Most approaches we cover have general applicability

DISCLAIMER

Read these parts carefully:

- Some of the techniques you will learn to identify during this course can be used to build malicious software, and most typically are
- **Make responsible use of your knowledge**
  - Developing and spreading malware is a crime
  - Computer and information security comes with ethical guidelines
- **Analyzing malware written by unknown authors can pose you at risk**
  - We will learn about some basic protections and precautions
  - All the samples you will be asked to analyze in this course are harmless

WHAT ARE WE TALKING ABOUT?

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | More | Search

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts | Health | World News TV | More

Technology

Yahoo 'state' hackers stole data from 500 million users

23 September 2016 | Technology | Share

Yahoo says "state-sponsored" hackers stole data on about 500 million users in what could be the largest publicly disclosed cyber-breach in history.

Top Stories

US accuses Russia of Aleppo 'barbarism'

5 hours ago

Swiss approve new surveillance law

6 hours ago

Miami baseball star dies in boat crash

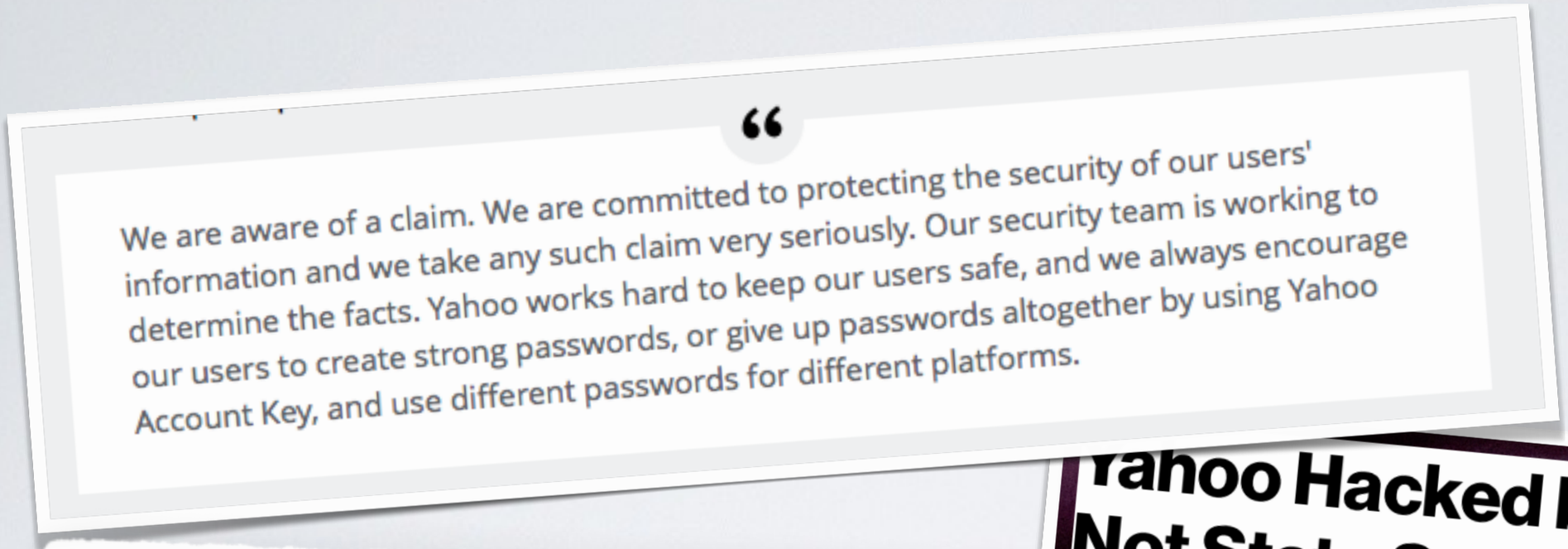
3 hours ago

Features & Analysis

Still missing

The search for Mexican students two

WHAT ARE WE TALKING ABOUT?



We are aware of a claim. We are committed to protecting the security of our users' information and we take any such claim very seriously. Our security team is working to determine the facts. Yahoo works hard to keep our users safe, and we always encourage our users to create strong passwords, or give up passwords altogether by using Yahoo Account Key, and use different passwords for different platforms.

The "Paranoids," the internal name for Yahoo's security team, often clashed with other parts of the business over security costs. And their requests were often overridden because of concerns that the inconvenience of added protection would make people stop using the company's products.

But Yahoo's choices had consequences, resulting in a series of embarrassing security failures over the last four years. Last week, the company disclosed that hackers backed by what it believed was an unnamed foreign government stole the credentials of 500 million users in a breach that went undetected for two years. It was the biggest known intrusion into one company's network, and the episode is now under investigation by both Yahoo and the Federal Bureau of Investigation.

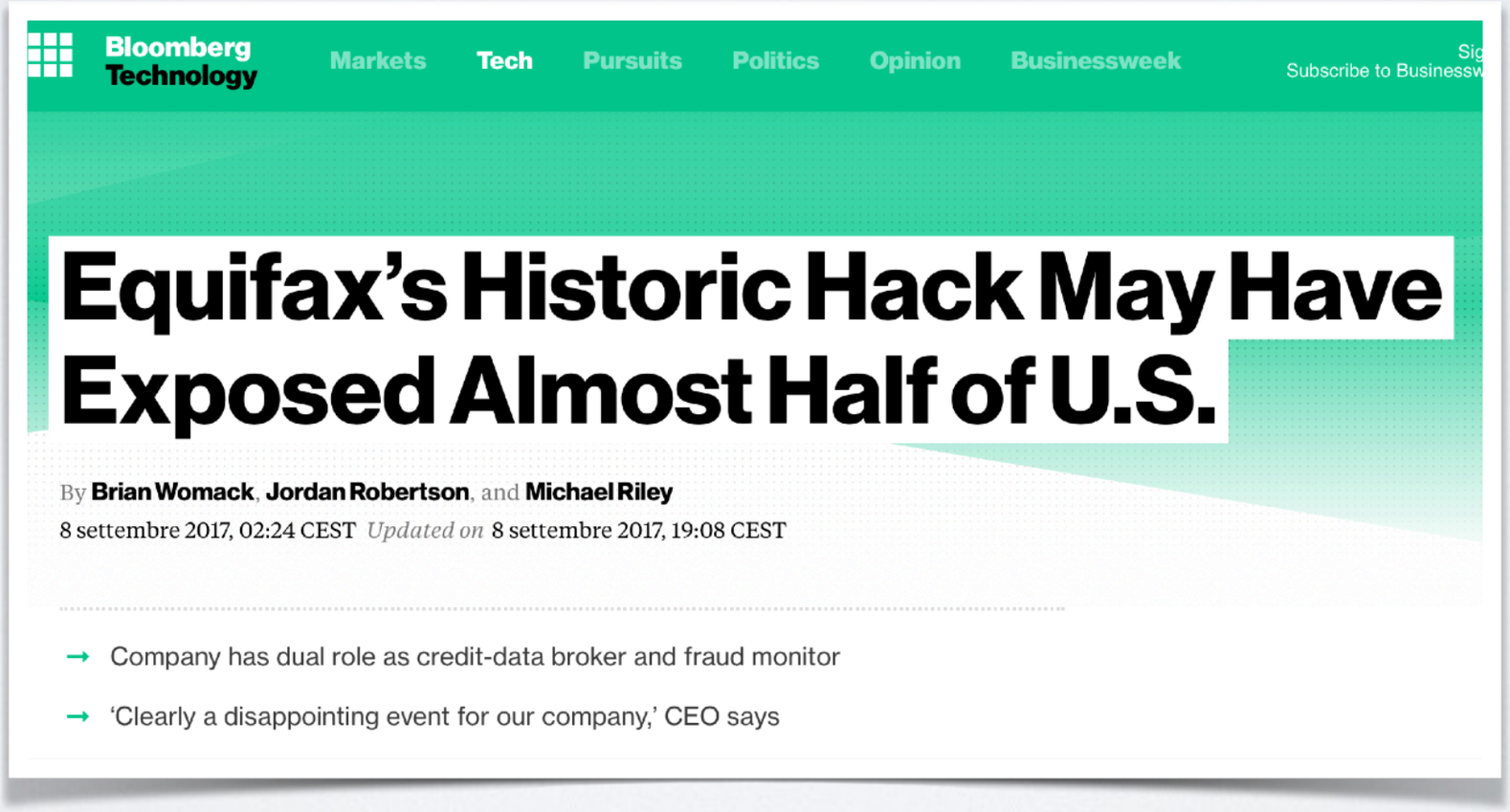
Yahoo Hacked by Criminals, Not State Sponsor, Security Firm Says

by Brian Womack
brianwomack

September 29, 2016 — 12:07 AM CEST

WHAT ARE WE TALKING ABOUT?

- September 2017 - The Equifax data breach exposes extremely sensitive data from >160 million consumers
  - Hackers exploited a known vulnerability in an unpatched server
  - A 2015 internal audit revealed issues on which Equifax didn't act effectively



Bloomberg Technology

Markets Tech Pursuits Politics Opinion Businessweek

Sig
Subscribe to Businessw

Equifax's Historic Hack May Have Exposed Almost Half of U.S.

By **Brian Womack**, **Jordan Robertson**, and **Michael Riley**
8 settembre 2017, 02:24 CEST *Updated on* 8 settembre 2017, 19:08 CEST

→ Company has dual role as credit-data broker and fraud monitor

→ 'Clearly a disappointing event for our company,' CEO says

WHAT ARE WE TALKING ABOUT?

August 2016:

- A hacker group named “Shadow Brokers” sets up an auction for a SW pkg.
- They claim it contains several advanced tools for system penetration
- Source: The Equation Group (allegedly tied to NSA)

The auction goes on for a few weeks with no success

- What was the real purpose of it?
- The SW is then released publicly (14/4/17)
- Contains executable code for several attacks, a few of which were previously unknown (0-day)

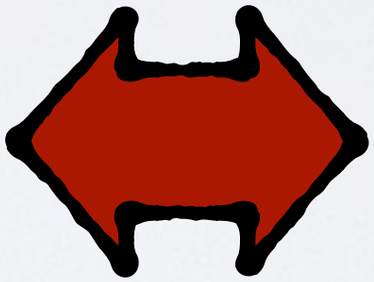
The SW structure makes the claim about the source credible

WHAT ARE WE TALKING ABOUT?

- May 2017 - Wannacry spreads infecting thousands of PCs
  - uses EternalBlue, an exploit leaked from NSA
  - spreads widely, but shows little care in its design

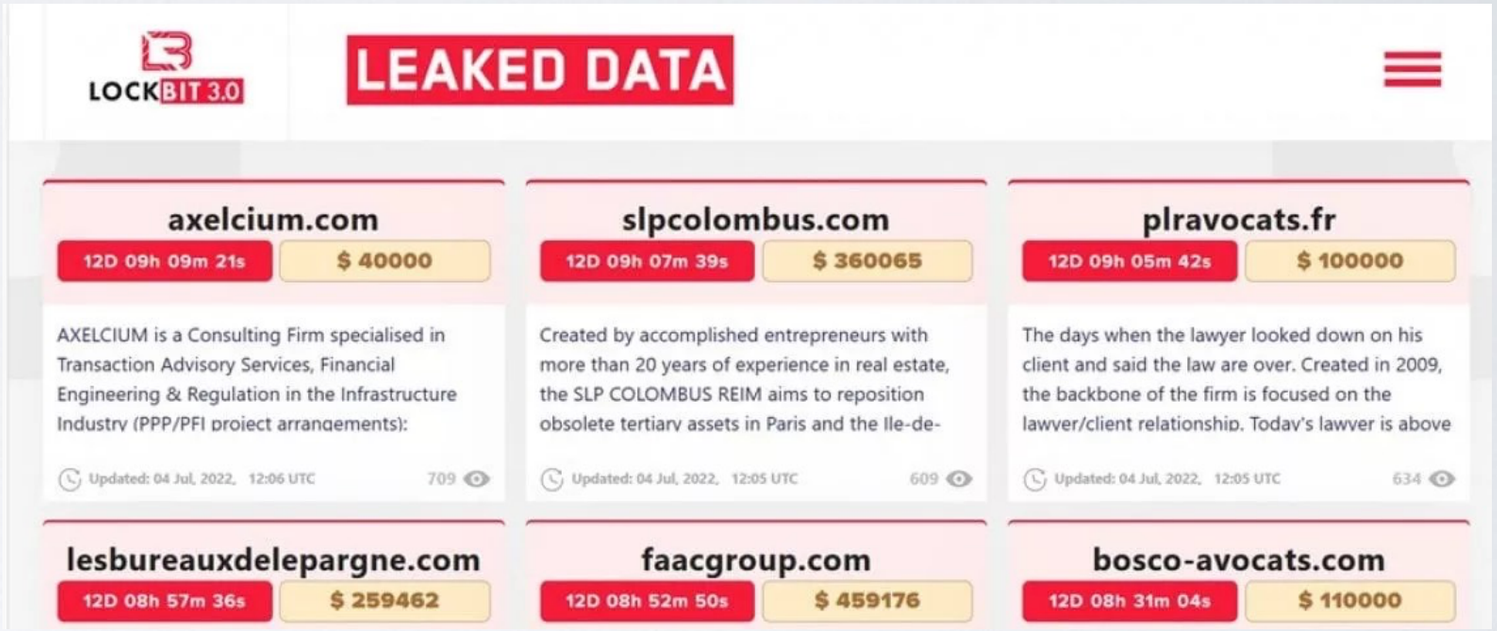
WHAT ARE WE TALKING ABOUT?

- Extremely advanced technologies are within easy reach of any criminal with enough budget

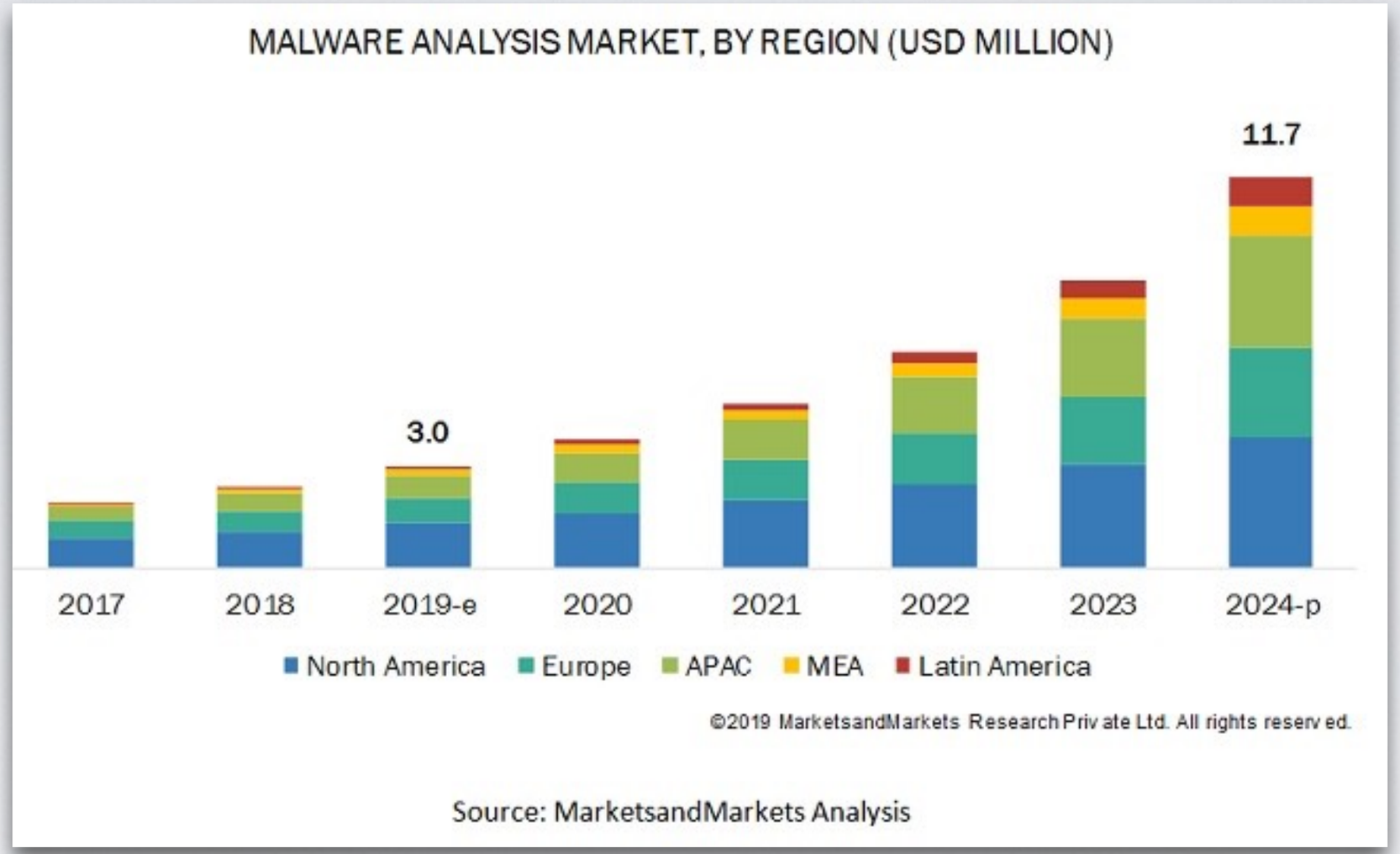


WHAT ARE WE TALKING ABOUT?

- Lockbit
  - Ransomware-as-a-Service since 2019
  - Third iteration of the software platform
  - Triple extortion tactic
    - through encryption
    - threat to publish sensitive data
    - create pressure using tactics like chasing third parties
- Business oriented
  - Bug bounty program
  - Customer care



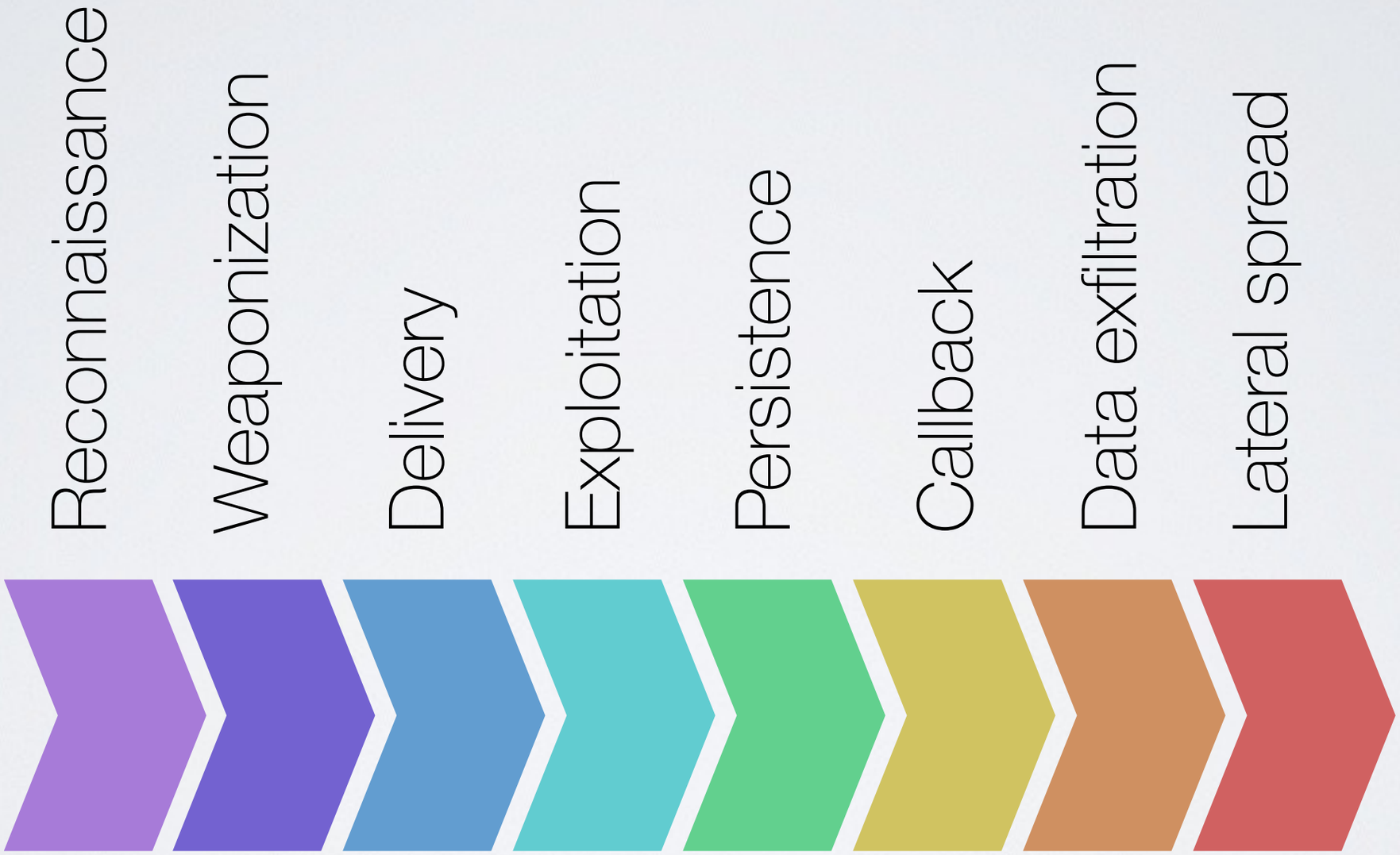
RELEVANT FOR THE JOB MARKET?



https://www.marketsandmarkets.com/Market-Reports/malware-analysis-market-10876513.html

ANATOMY OF AN ATTACK

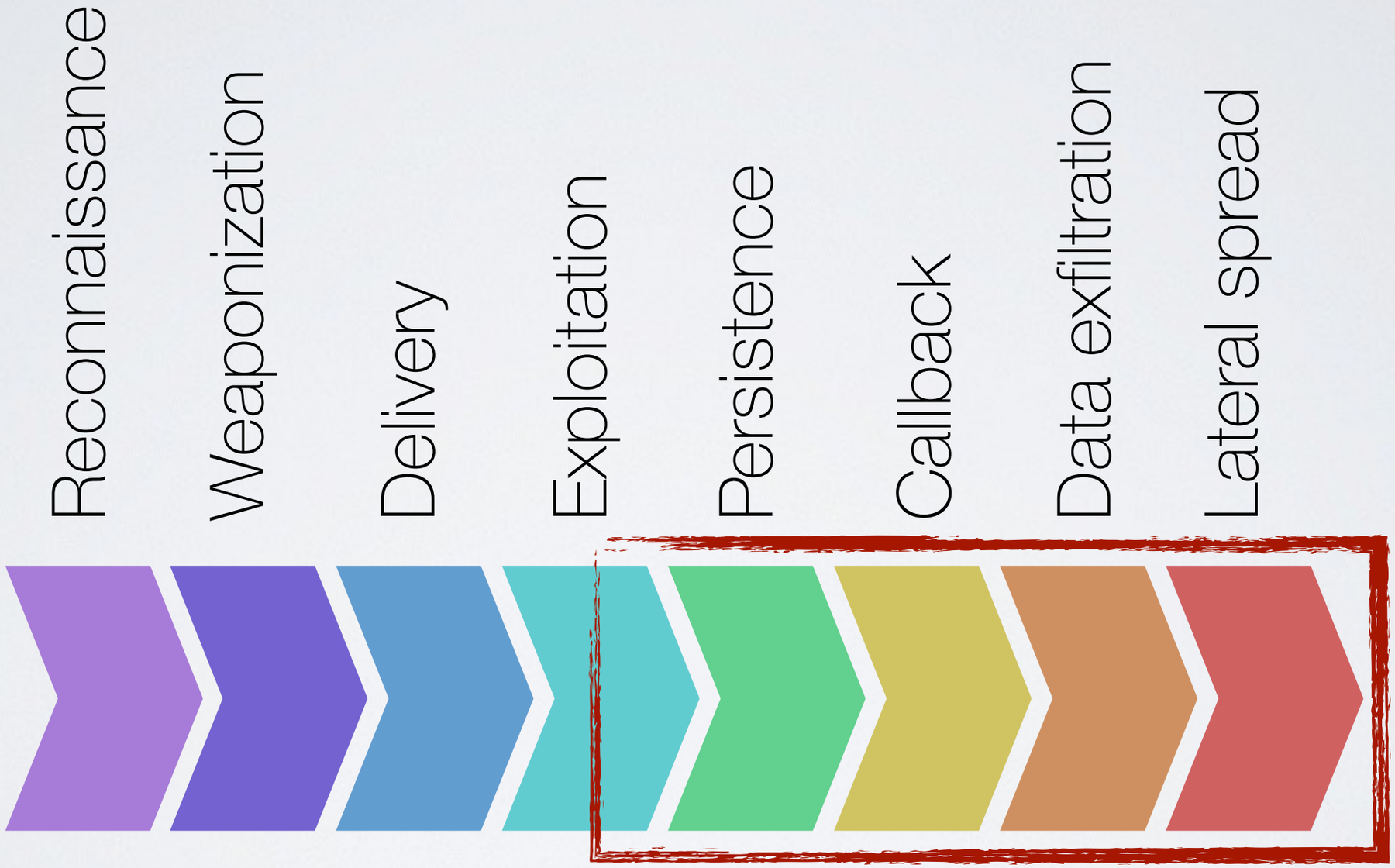
- The intrusion (or cyber) **kill chain**



The process by which perpetrators carry out cyber attacks, as modeled by Lockheed Martin

ANATOMY OF AN ATTACK

- The intrusion (or cyber) **kill chain**



EXPECTED BEHAVIORS

- **Persistence**
  - Malware installs itself in the system
  - It performs actions to guarantee its survivability to
    - reboots
    - inspections
    - etc.
  - It often modifies OS configuration
  - Changes are hidden

EXPECTED BEHAVIORS

- **Uniqueness** (“single-instance”)
  - Malware is often incompatible with itself
  - Multiple concurrent executions are meaningless
    - Sometimes even harmful for malware itself
    - Think about two ransomware instances competing for the same resources and tasks
  - Start-up checks ensure the execution of a single copy

EXPECTED BEHAVIORS

- **Targeting**
  - Malware is sometimes designed to attack specific targets
  - The sample will check if it landed on the correct victim:
    - Region/language information
    - HW/SW characteristics of the machine
    - Presence of specific configuration
    - External devices
    - Presence of known documents
    - ...

EXPECTED BEHAVIORS

- **Obfuscation & evasion**
  - Malware will try to hide its presence and its effects
    - It may scramble its code to hide easily discoverable hints of its malicious nature
    - It may inject code in other processes to conceal its real identity
    - It may employ techniques to hamper the possibility to correctly analyze its behavior

- The typical goal is to stay undercover while acting on the infected machine for as long as possible
  - With exceptions: think about ransomware (why?)

EXPECTED BEHAVIORS

- **Fingerprinting & beaconing**
  - Malware will inspect the infected system and collect information about it
  - Information can be used to notify its presence to a remote server
  - This phase is sometimes referred to as “beaconing”

EXPECTED BEHAVIORS

- **Communication**
  - Malware often interacts with external Command & Control servers to
    - receive instructions and commands
    - update its internal components
    - exfiltrate data
  - Communication may use an impressively heterogeneous set of methodologies
    - Direct links
    - Cloud data storage
    - Social networks
    - Network services (e.g., DNS)
  - Data on channels is often obfuscated