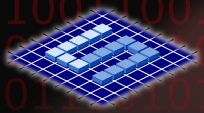
CYBER ATTACKS



SimuLearn

THE EXTENDED STORIES OF THE CASES IN THE CARD GAME

This e-book is still work in progress. I will gradually extend the contents of the book. You will get a notification once a new version is available.
Version: September 1st 2026

CYBER ATTACKS

THE EXTENDED STORIES

Assembled and edited by Koen Vastmans

MMXXV - MMXXVI

INTRODUCTION

This e-book is meant as accompaniment of the Cyber Attacks card game. The cards of the game have a limited size: they are all size A6, with a front and back.

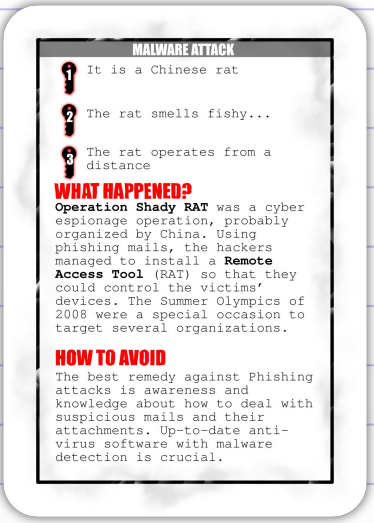
The **front of each card** contains:

- the title of the case
- an image
- a short, rather cryptic description

The **back of each card** contains

- 3 keys to decipher the case
- what actually happened
- how to avoid this

Front of a card



Back of a card

The limited space of the cards means that I needed to be very selective with the information shared on the cards. But quite often I really had to cut in background information of the cases, just to fit the information on the card, even with a slightly reduced font size. And that's a pity, because sometimes you need a bit more information. That's why I created this e-book: to give you more information than what I could fit on the front and back of an A6 size card and also provide some extra pointers, links to online articles covering the case, to give you different angles to the story.

The book follows the exact same structure as the cards:

- Chapters divide the cases according to their category (as mentioned in the grey box at the top of the card back)
- Cases are explained with:
  - Their title
  - The image
  - The brief description that was meant to trigger the game
  - What really happened. This is a more extensive description than the ones on the cards. This also contains the explanation of the hints.
  - How to avoid this kind of security incident
  - A link to further reading about the case

The cards of the game, and thus also the chapters of this book, are divided according to the following categories:

- Weak authentication
- Patch management
- Internet of Things
- Malware attack
- Ransomware attack
- Supply chain attack

No more guessing...

- Data scraping
- Impersonation attack
- Zero day vulnerability

Enjoy the full stories!

CHAPTER 1: WEAK AUTHENTICATION

A lot of the cyber attacks and cybersecurity incidents boil down to weak authentication, or authentication not adapted to the needs. Because of this inappropriate authentication mechanism, people with bad intentions can easily access the systems that are not adequately protected.

This chapter gives an overview of a number of cases that fall into this category and expose the harm that was done. This can be a database server that still uses user-ID and password, an insecure file transfer, passwords stored in the clear…

These are the cases of this chapter:

- Big consultancy, no big security?
- Playground closed
- No NDA for DNA?
- The US Government got sunburned
- The unintended interview
- Open vault

BIG CONSULTANCY, NO BIG SECURITY?

In September 2017 the e-mail infrastructure of a big consultancy company got hacked, breaching the confidentiality of numerous customers and 244.000 staff members.

WHAT HAPPENED?

Deloitte's mail infrastructure, hosted on Azure Cloud got hacked. The database had no 2-factor authentication. They became suspicious about the breach in April 2017, but it probably started already in September 2016. Among the affected customers are several U.S. Government Departments.

HOW TO AVOID

User-ID and password are too weak as authentication mechanism, especially if you are dealing with confidential information, even more so on public cloud infrastructure.

FURTHER READING

<tbc>

PLAYGROUND CLOSED

In April 2011 the network service of a game console manufacturer had an "external intrusion". The personal data of 77 million users were compromised. The service was unavailable during 23 days.

WHAT HAPPENED?

Sony Playstation network went down for 3 weeks due to PS3 hack. Hackers gained access via SQL injection and could steal personal and credit card information. The passwords of users were only stored hashed, not encrypted. Sony had to close their entire entertainment service, not only the game

store, but also video on demand. The total financial loss was $171 million, reputational damage not included.

HOW TO AVOID

Encrypt passwords or better, store them in a vault. Regularly Check your code for OWASP Top 10 vulnerabilities.

FURTHER READING

<tbc>

NO NDA FOR DNA?

DNA information is considered as strictly confidential information, that one can only collect and disclose under very strict conditions. But in 2023 the DNA data of over 7 million people worldwide got leaked.

WHAT HAPPENED?

In October 2023, 23andMe, a company providing direct-to-consumer genetic tests, got hacked. Personal genetic data of 7

million customers were stolen. A sample was leaked to several

hackers fora. The company blamed the customers for not changing their password...

HOW TO AVOID?

Medical information should be treated as highly confidential. Access via user-ID and password only is a bad choice. Data should be encrypted and access should be strictly limited to specific users.

FURTHER READING

<tbc>

THE US GOVERNMENT GOT SUNBURNED

On December 13th 2020 a cyberattack was reported against several U.S. Government institutions. The attack had already begun in March 2020. This was the worst cyber espionage incident of the US.

WHAT HAPPENED?

In 2020 several US Government departments were victim of the SolarWinds breach. Russians exploited a vulnerability in SolarWinds Orion. Via an unprotected FTP server they could build and distribute a Trojan Horse to the users of Orion (supplychain attack). The vulnerability in

the FTP server was already reported in 2019 but never fixed.

HOW TO AVOID

An insecure file transfer mechanism should be avoided at all cost, especially for distributing (security)updates.

FURTHER READING

<tbc>

$WHOAMI

My name is Koen Vastmans. I am originally a software developer. In 2011 I made the switch from development to coaching and training.

I began (co-)creating my first serious game in 2018. By the end of 2019 I started SimuLearn, a one-man company dedicated to developing and selling serious games, mainly, but not exclusively, focused on Agile and DevOps.

Over the course of the years I created 10 games and/or card decks, several in co-creation with others, and not only focused on Agile or DevOps. This e-book and the card game it accompanies, are the proof of that.

If you want to know more about my other games, feel free to check out my website:

https://www.simu-learn.net

SimuLearn

Learn through simulations and gamification

TABLE OF CONTENTS