

# Introduction to IT Security for Data Scientists



**SWITCH**

[matthias.seitz@switch.ch](mailto:matthias.seitz@switch.ch)

[daniel.weber@switch.ch](mailto:daniel.weber@switch.ch)

Bern, 17th of June 2020

# Agenda

- 01 - Introduction
- 02 - Current Security Threats
- 03 - Howto protect your Assets
- 04 - Good IT security practices
- 05 - How to react to a Security Incident
- 06 - Selected Topics and wishlist
- 07 - Roundup und Feedback

# Schedule

09:00 Welcome

09:30 Lecture

10:30 Coffee break

11:00 Lecture

12:00 Lunch break

13:30 Lecture

15:00 Coffee break

15:30 Lecture

17:00 End

# About us

- Matthias Seitz
  - BSc Computer Science
  - IT Security Engineer / Product Manager @SWITCH
  - Longtime experience in IT security
- Daniel Weber
  - BSc Computer Science
  - IT System Administrator / Security Engineer @SWITCH
  - Longtime experience in IT security

# About SWITCH

SWITCH is an **integral part of the Swiss academic community**.

Based on our **core competencies**

- Network
- Security
- Identity Management

SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment.

# 01 - Introduction

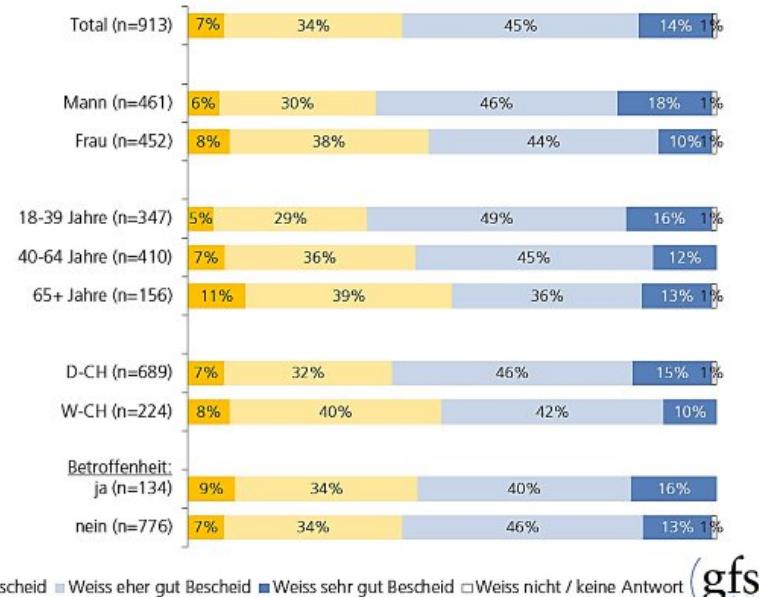
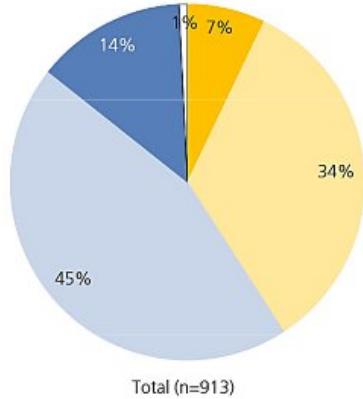
- Short introduction for todays Topics
- Introduce yourself

# A Survey Question form ICT Switzerland

- How good do you think you know, how to protect yourself against attacks from the internet?
- a) You know very little
- b) You rather know little
- c) You know rather good
- d) You know very good

source: <https://ictswitzerland.ch/en/publications/studies/security-on-the-internet/>

# Result from Study



source: <https://ictswitzerland.ch/en/publications/studies/security-on-the-internet/>

# What do you think is Security all about?



# Security is about...

## Threats



## Process



Risk and security management process

## Information Security



# Did you know?

Cybercrime makes more money than top Fortune 500 Companies!

Organization	Annual Revenue
Cybercrime	\$1'500'000'000'000*
Walmart	\$500'343'000'000
Exxon Mobil	\$244'363'000'000
Berkshire Hathaway	\$242'137'000'000
Apple	\$229'234'000'000
UnitedHealth Group	\$201'159'000'000

# More Topics that we will discuss

- Current Security Threats
- How Companies protect themselves
- How you can help
- How you should react to a Security Incident
- Technical Deep Dive (Choose from Topics)

# What do you expect from this Course?



# We wan't to know more about you

- Which field are you working in
- Do you know the Security Process in your company
- Are there already some questions about Security?

# Let's talk about Security

- We encourage you to share your experiences in this Course (Learn from others)
- In Security we are using the [TLP](#) (Traffic Light Protocol)

**RED** - personal for named recipients only

**AMBER** - limited distribution

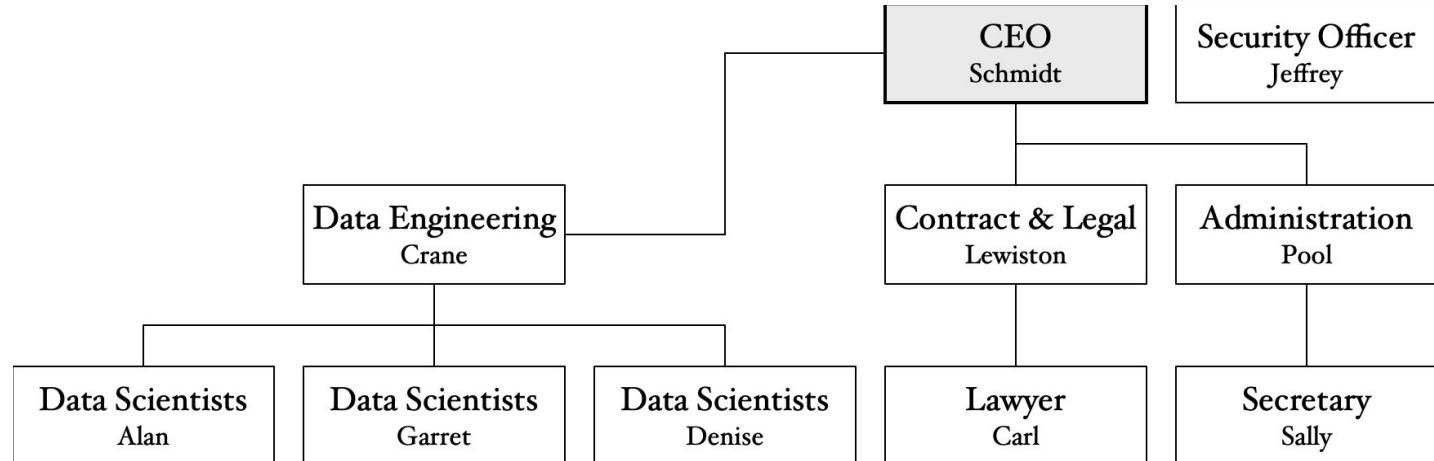
**GREEN** - community wide

**WHITE** - unlimited

- Your experience counts, tell us your Security Story

# The imaginary Startup Company

- Startup with 10 employees
- Data Analytics B2B in a Community Cloud
- Structured in three branches
- Security Officer tries to acquire ISO 27001 Certification



# 02 - Current Security Threats

- Overview
- Phishing
- Malware / Ransomware



# Top 15 Security Threats (Published 2019)

Spam	Ransomware	Web Application Attacks
Malware	Information Leakage	Botnets
	Physical manipulation	Phishing
Denial of Service	Cyber Espionage	Cryptojacking
Data Breaches	Identity Theft	Insider Threat

Question:

What do you think are the biggest Threats?

# ENISA Report

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➡	1. Malware	➡	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➡	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➡	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➡	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➡	10. Physical manipulation/ damage/ theft/loss	➡	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➡ Stable, ↑ Increasing  
 Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

# What we will talk about today...



# About Attackers: From Script Kiddies to APT

- **Internal User Error:** Users making **mistakes** with configurations which may bring down **critical resources** such as **firewalls**, routers and servers causing wide-spread or departmental company outages.
- **Opportunistic:** These attackers are usually **script kiddies** driven by the desire for **notoriety**
- **Insider Threat:** Insider attackers are typically **disgruntled employees** or ex-employees looking for **revenge** or some type of financial gain.
- **Hacktivists:** These attackers have a **political agenda** and create **high-profile attacks**
- **Organized Crime:** Most often, these cybercriminals engage in **mass attacks** driven by **profits**. Typically looking for social security numbers, health records, credit cards, and banking information.
- **Government Sponsored:** Well funded and often build **sophisticated, targeted attacks**. They are typically motivated by **political, economic, technical, and military agendas**.

# Threat Actors and their motivation

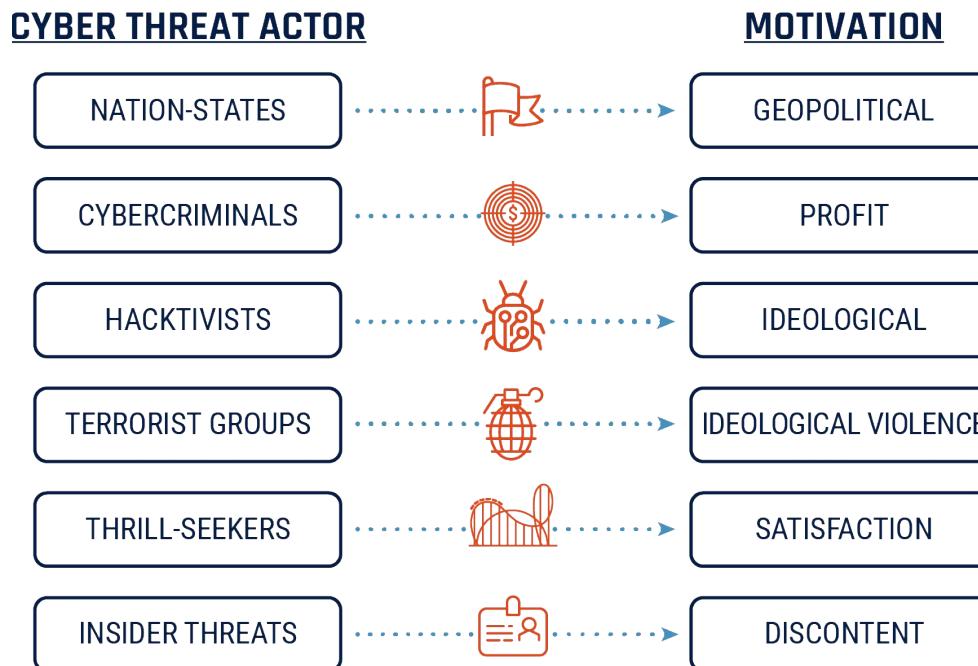


Image Source: <https://cyber.gc.ca/sites/default/files/inline-images/motivations-e.png>

# The Mitre Att&ck Framework or How Attacker works

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	23 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Cloud Service Discovery	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Dynamic Resolution (3)	Data from Information Repositories (2)	Data Manipulation (3)
Phishing (9)	Scheduled Task/Job (5)	Shared Modules	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Execution Guardrails	Domain Trust Discovery	Replication Through Removable Media	Encrypted Channel (2)	Fallback Channels	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Software Deployment Tools	Compromise Client Software Binary	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	File and Directory Discovery	Software Deployment Tools	Data from Local System	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	System Services (2)	Create Account (3)	File and Directory Permissions Modification (2)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	Taint Shared Content	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	User Execution (2)	Create or Modify System Process (4)	Group Policy Modification	Group Policy Modification	Hide Artifacts (4)	OS Credential Dumping (8)	Network Service Scanning	Data from Removable Media	Non-Application Layer Protocol	Non-Standard Port	Firmware Corruption
Valid Accounts (4)	Windows Management Instrumentation	Event Triggered Execution (15)	Hijack Execution Flow (10)	Hijack Execution Flow (10)	Hijack Execution Flow (10)	Steal Application Access Token	Network Share Discovery	Data Staged (2)	Protocol Tunneling	Protocol Tunneling	Inhibit System Recovery
			Impair Defenses (5)	Impair Defenses (5)	Impair Defenses (5)	Network Sniffing	Non-Standard Port	Email Collection (3)	Proxy (4)	Remote Access Software	Network Denial of Service (2)
			Scheduled Task/Job (5)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	>Password Policy Discovery	Protocol Tunneling	Input Capture (4)	Man in the Browser	Transfer Data to Cloud Account	Resource Hijacking
			Implant Container Image	Indirect Command Execution	Indirect Command Execution	Peripheral Device Discovery	Protocol Tunneling	Man-in-the-Middle (1)	Man-in-the-Middle (1)	Traffic Signaling (1)	Service Stop
			Office Application Startup (6)	Masquerading (6)	Masquerading (6)	Permission Groups	Protocol Tunneling	Screen Capture	Screen Capture	Web Service (3)	System Shutdown/Reboot
				Modify Authentication	Modify Authentication						

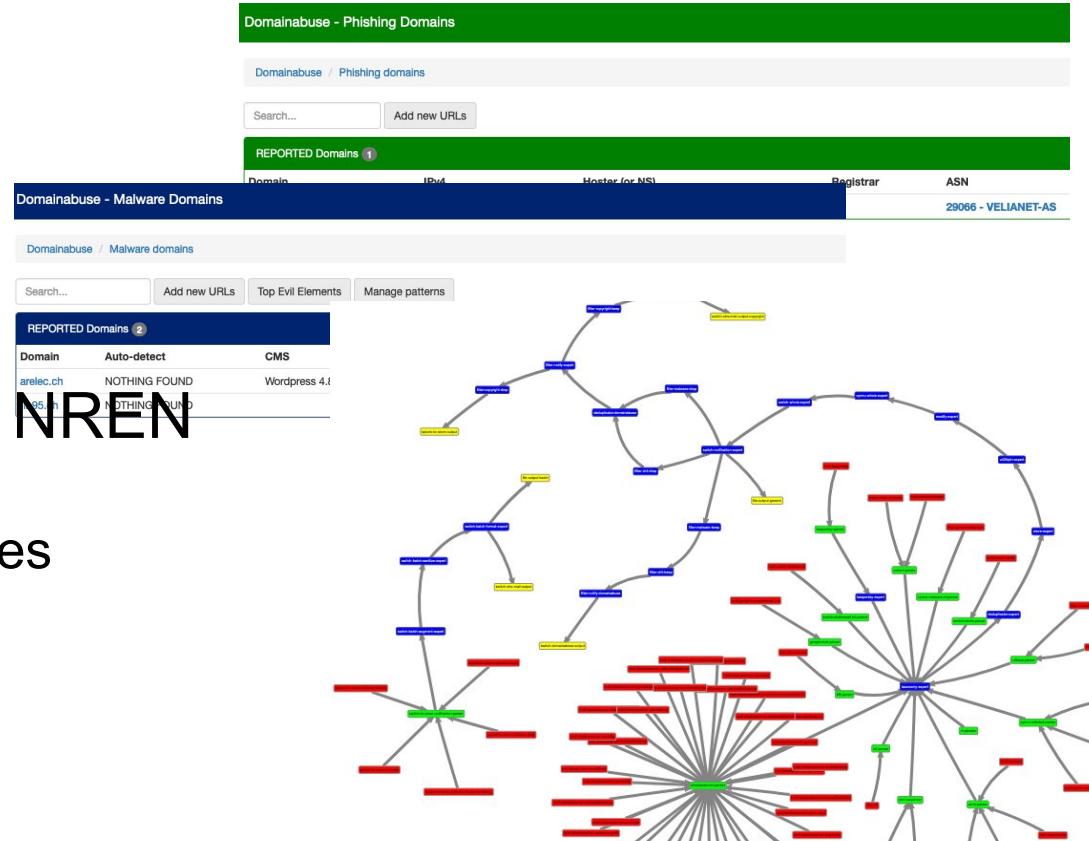
source: <https://attack.mitre.org/>

# Discussion: Top Threats for FuData

- Discuss
  - What could be the motivation from a malicious actors perspective?
  - How do they affect their business?
  - Do you already have ideas how to protect them?

# What does SWITCH see?

- As part of the Registry
  - Phishing sites
  - Fake shops
  - Infected websites
- As part of the CERT and NREN
  - Malware
  - Reports of vulnerable services
  - Reports of open Services
  - DDoS attacks



# Phishing



# Phishing

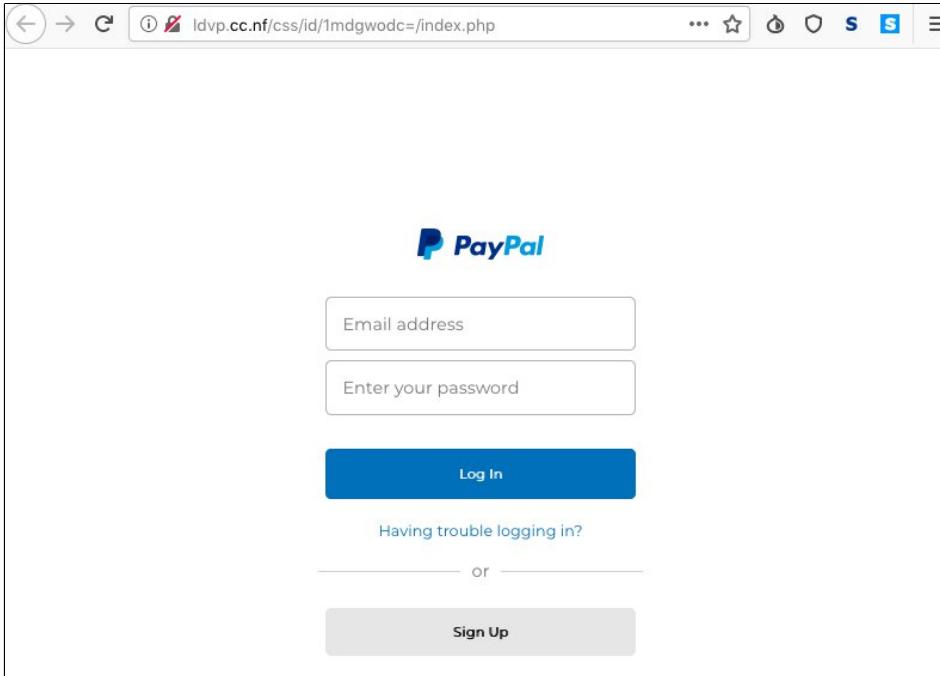
“Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution **to lure individuals into providing sensitive data** such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can **result in identity theft and financial loss.**”

<http://www.phishing.org/what-is-phishing>

“The word "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users. The term was coined in the 1996 timeframe by hackers who were stealing America On-Line accounts by scamming passwords from unsuspecting AOL users.”

[https://docs.apwg.org/word\\_phish.html](https://docs.apwg.org/word_phish.html)

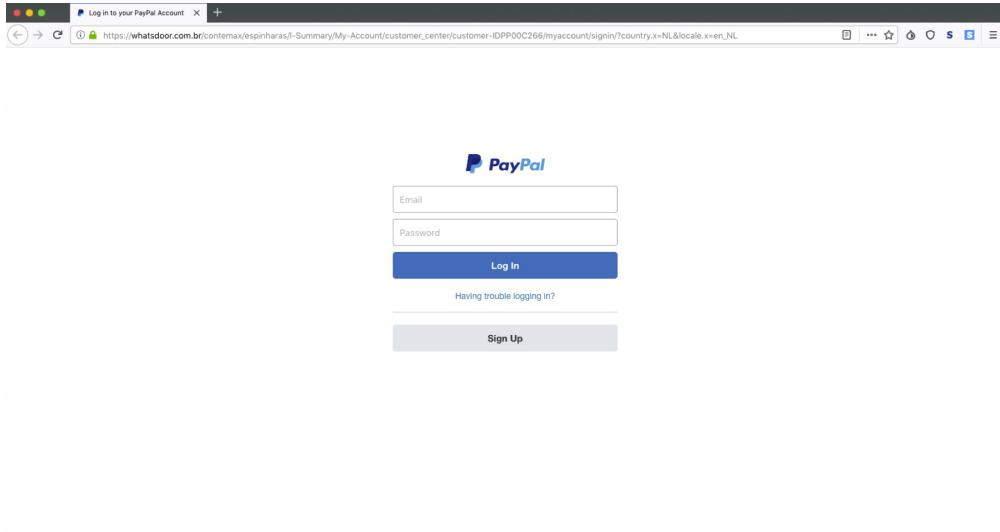
# Phishing



# Phishing Types

- Generic Phishing
- Spear Phishing
- CEO Fraud / Whale Phishing

# Generic Phishing Attack



- Mass sending: Send to thousands of other victims
- Language / cultural border
- The goal is typically to gain credit card info and/or to steal monetary values in the end

# Spear Phishing Attack

- Spear phishing is a targeted attempt to steal credentials from a specific individual
- The individual is typically scouted during target research and identified as a possible asset for infiltration
- Spear phishing attempts use malware, keylogger, or email to get the individual to give away the credentials
- Typically part of a bigger attack (Lateral movement). Credential stealing for an APT.

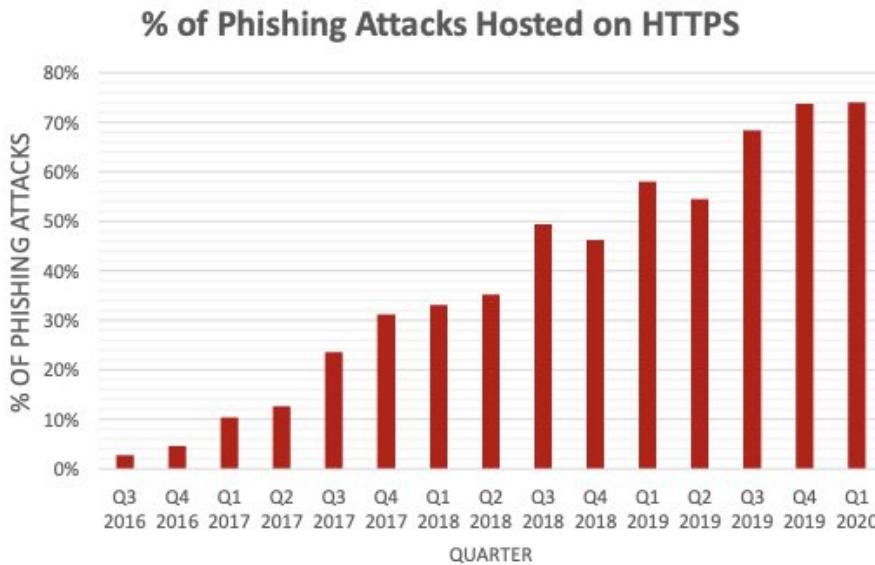
# Whale Phishing

- Phishing attack that is specifically aimed at wealthy, powerful, or prominent individuals
- If such a user becomes the victim of a phishing attack he can be considered a “big phish,” or, alternately, a “whale”
- Whale phishing involves the same tactics used in spear phishing campaigns
- Also known as CEO Fraud, BEC (Business Email Compromise), FPF (Fake President Fraud) oder Bogus Boss Email

# HTTP vs HTTPS

- HTTP stands for Hyper Text Transfer Protocol
- Communication between clients (users) and web servers is done by sending HTTP Requests and receiving HTTP Responses
- **HTTP: No Data Encryption Implemented**
- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the HTTP protocol. In HTTPS, the **communication** protocol is **encrypted** using Transport Layer Security (TLS)

# Does HTTPS help against Phishing?

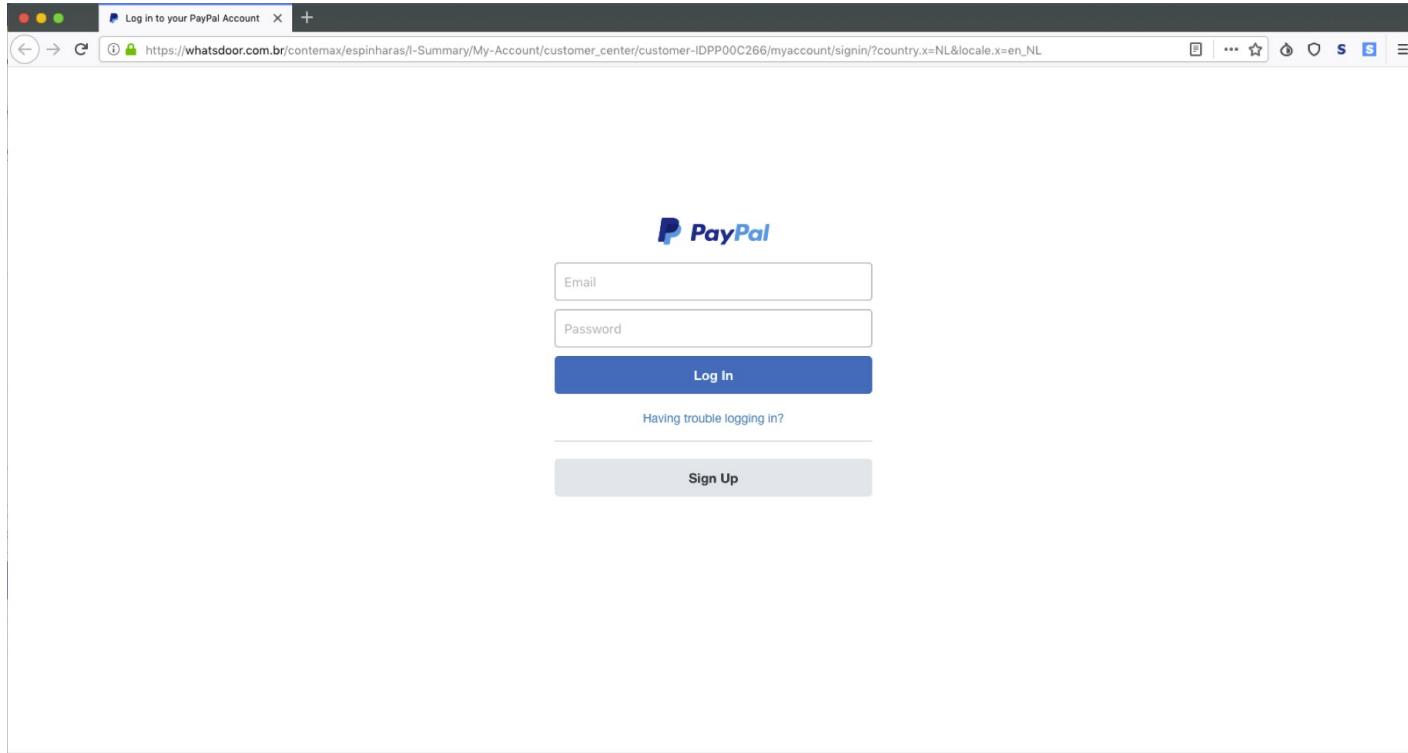


APWG: "In Q1 2020, a new high of 74 percent of sites used for phishing were protected with SSL"

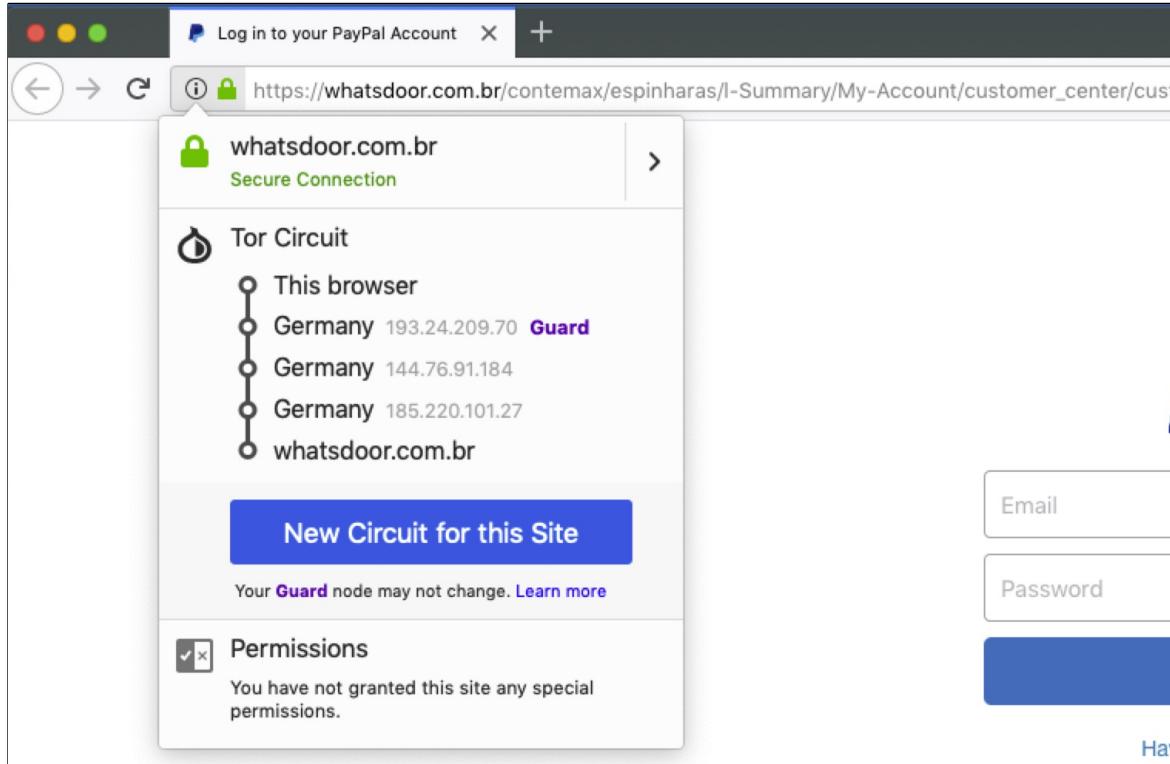
Source:

[https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2020.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf)

# Phishing and HTTPS



# Phishing and HTTPS



# Phishing and HTTPS

● ● ● Page Info - https://whatsdoor.com.br/contemax/espinharas/I-Summary/My-Account/...

General Media Permissions Security

**Website Identity**

Website: **whatsdoor.com.br**  
Owner: **This website does not supply ownership information.**  
Verified by: **cPanel, Inc.**  
Expires on: **6 August 2019**

**View Certificate**

**Privacy & History**

Have I visited this website prior to today? **No**  
Is this website storing information (cookies) on my computer? **No** **View Cookies**  
Have I saved any passwords for this website? **No** **View Saved Passwords**

**Technical Details**

**Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bit keys, TLS 1.2)**  
The page you are viewing was encrypted before being transmitted over the Internet.  
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

?

# Phishing

The screenshot shows the 'Manage Service SSL Certificates' page in cPanel/WHM version 68. The left sidebar lists various management options, and the main content area provides an overview of SSL certificate management for services like SMTP, POP3, IMAP, and Webmail.

**Manage Service SSL Certificates**

Created by Documentation, last modified on Jul 16, 2018

**For cPanel & WHM version 68**

(WHM >> Home >> Service Configuration >> Manage Service SSL Certificates)

**Overview**

- Free cPanel-signed certificate
- Service SSL Certificates
- Reset a Certificate
- Certificate Details
- Apply Certificate to Another Service
- Install a New Certificate
- iOS Mail push notifications
- Additional documentation

**Overview**

This interface allows you to manage certificates for your server's services. For example, you can manage certificates for the following services:

- Exim (SMTP).
- POP3 and IMAP.
- The cPanel services (cPanel & WHM and Webmail).
- Your FTP server.
- iOS Mail Push Notifications (APNs).

SSL certificates allow your web server to identify itself to the computers that access it.

You can use any of the following types of certificates to secure your server's services:

- A free cPanel-signed hostname certificate.
- A certificate that you obtained from a certificate authority (CA).
- A self-signed certificate.

**Warning:**

We recommend that you **do not use** self-signed certificates. They are **not** as secure as certificates from a CA. Any server could claim to be your server with a self-signed certificate because they do not use a third-party verification system. To remedy this, use certificates from a CA, which verifies that users are securely connected to your server.

# Phishing Checks

The screenshot shows the VirusTotal interface for a URL from a Brazilian website. The main summary indicates 11 engines detected the URL as malicious. The URL itself is a 404 page from whatsdoor.com.br. The detection table below lists results from various engines:

Engine	Result	Details
AegisLab WebGuard	Phishing	Avira (no cloud)
BitDefender	Phishing	CLEAN MX
CRDF	Malicious	ESET
Kaspersky	Phishing	Netcraft
OpenPhish	Phishing	Sophos AV
Spamhaus	Phishing	Fortinet

<https://www.virustotal.com>

# Phishing Checks

SUCURI Website Monitoring Website Firewall Website Backups Knowledgebase Support

https://whatsdoor.com.br/contemax/espinharas/l-Su...

**Site Issue** 404 Not Found    **Site is Blacklisted** by Google Safe Browsing and others    Request Cleanup

**Scan info**  
https://whatsdoor.com.br/contemax/espinharas/l-Summary/My-Account/customer\_center/customer-IDP00C266/myaccount/signin/?country.x=Nl&locale.x=en\_NL

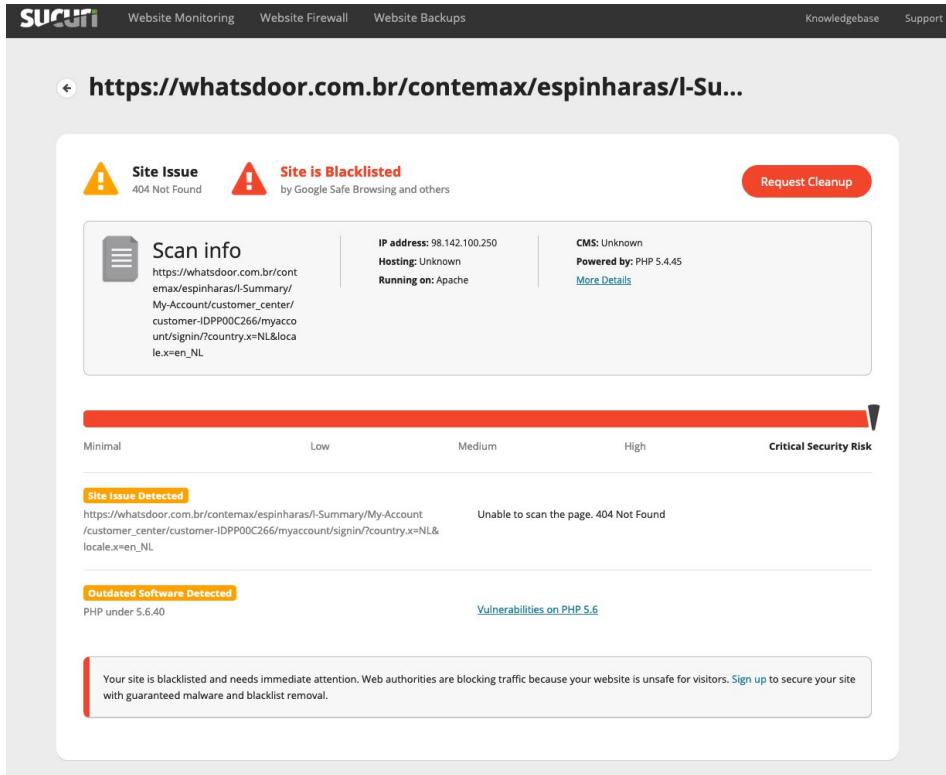
IP address: 98.142.100.250    CMS: Unknown  
Hosting: Unknown    Powered by: PHP 5.4.45  
Running on: Apache    More Details

Minimal Low Medium High Critical Security Risk

**Site Issue Detected**  
https://whatsdoor.com.br/contemax/espinharas/l-Summary/My-Account/customer\_center/customer-IDP00C266/myaccount/signin/?country.x=Nl&locale.x=en\_NL  
Unable to scan the page. 404 Not Found

**Outdated Software Detected**  
PHP under 5.6.40    [Vulnerabilities on PHP 5.6](#)

Your site is blacklisted and needs immediate attention. Web authorities are blocking traffic because your website is unsafe for visitors. [Sign up](#) to secure your site with guaranteed malware and blacklist removal.



<https://sitecheck.sucuri.net/>

# Report Phishing

SWITCH

Antiphishing Form Privacy Statement Search

## Report phishing

You can help us fight phishing by using the simple form below to report e-mails. Your report will be analysed by security experts at SWITCH, and measures will be taken to block dangerous websites as soon as possible. Web browsers will get updates of known phishing pages, thus protecting users.



Please report your phishing mail using the form below:

Sender: Matthias Seitz <matthias.seitz@switch.ch> (Information from your AAI login)

URL: e.g. http://www.dangerous.com/wp-admin/do.php  
Dangerous URL contained in the phishing mail:  
Click here to learn how to extract this URL from your e-mail program.

E-mail: Click here to show a box where you can paste in the full e-mail you received.  
(optional)

Comments: (optional)  
Please tell us if there's something you think we should know.

Targeted organisation: (if known)  
Optional: Choose an organization name from the list below, or leave empty  
In case you know the organisation being targeted by this phishing attack, e.g. your own organisation, you can choose it from the list above. Please only select an organisation if you are sure and if it is available in the list.

By clicking on the "Submit" button below, I agree to send the data entered above to SWITCH, together with my AAI login identity. SWITCH will not share this data with third parties, with the exception of the dangerous URL.

Submit

<https://www.switch.ch/phishing/report-phishing/>

# Report Phishing



DE FR IT EN

[Home](#) | [About](#) | [Contact](#)

## Did you receive a phishing e-mail?

Forward it to [reports@antiphishing.ch](mailto:reports@antiphishing.ch)

**Attention:** This mailbox is being processed by a machine in an automated way. If you have an inquiry and / or wish to receive a feedback from MELANI, please use [reply@melani.admin.ch](mailto:reply@melani.admin.ch) instead or use our [reporting form](#).

## Have you found a phishing site?

Report phishing websites using the following web form:

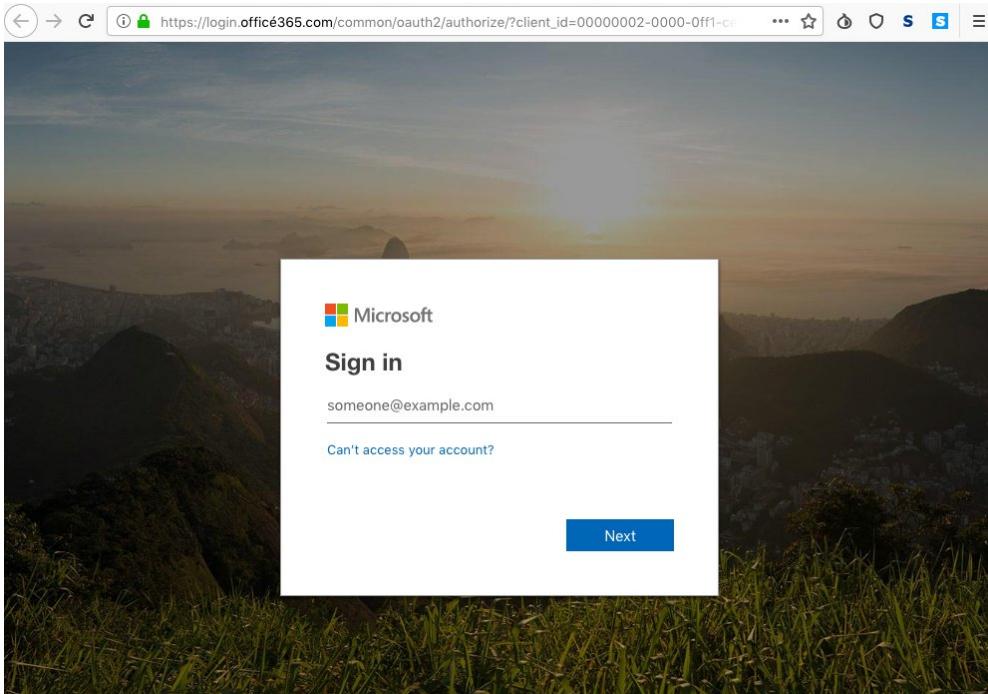
URL...

### About antiphishing.ch

antiphishing.ch is operated by the [Reporting and Analysis Centre for Information Assurance MELANI](#) of the Swiss Federal Administration. The goal is to provide users a simple and easy way to report phishing attempts.

<https://www.antiphishing.ch>

# Advanced Phishing



Page Info - https://login.office365.com/common/oauth2/authorize?client\_id=00000002-0000-0ff1-ce04-000000000000

General Media Permissions Security

#### Website Identity

Website: login.office365.com  
Owner: This website does not supply ownership information.  
Verified by: Let's Encrypt  
Expires on: 29 July 2019

[View Certificate](#)

#### Privacy & History

Have I visited this website prior to today? No  
Is this website storing information (cookies) on my computer? No [View Cookies](#)  
Have I saved any passwords for this website? No [View Saved Passwords](#)

#### Technical Details

**Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bit keys, TLS 1.2)**  
The page you are viewing was encrypted before being transmitted over the Internet.  
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

# Advanced Phishing

- <https://login.xn--offic365-f1a.com>
- Punycode
  - Is a way to **represent International Domain Names (IDNs) with the limited character set (A-Z, 0-9)** supported by the domain name system.
  - For example, "münich" would be encoded as "mnich-kva".
  - An IDN takes the punycode encoding, and adds a "xn--" in front of it.
  - "münich.com" would become "xn--mnich-kva.com".
  - Punycode rendering depends on the browser. Firefox will display it as a look-alike domain

# Phishing

# Phishtank Demo

<https://www.phishtank.com/>

# Malware

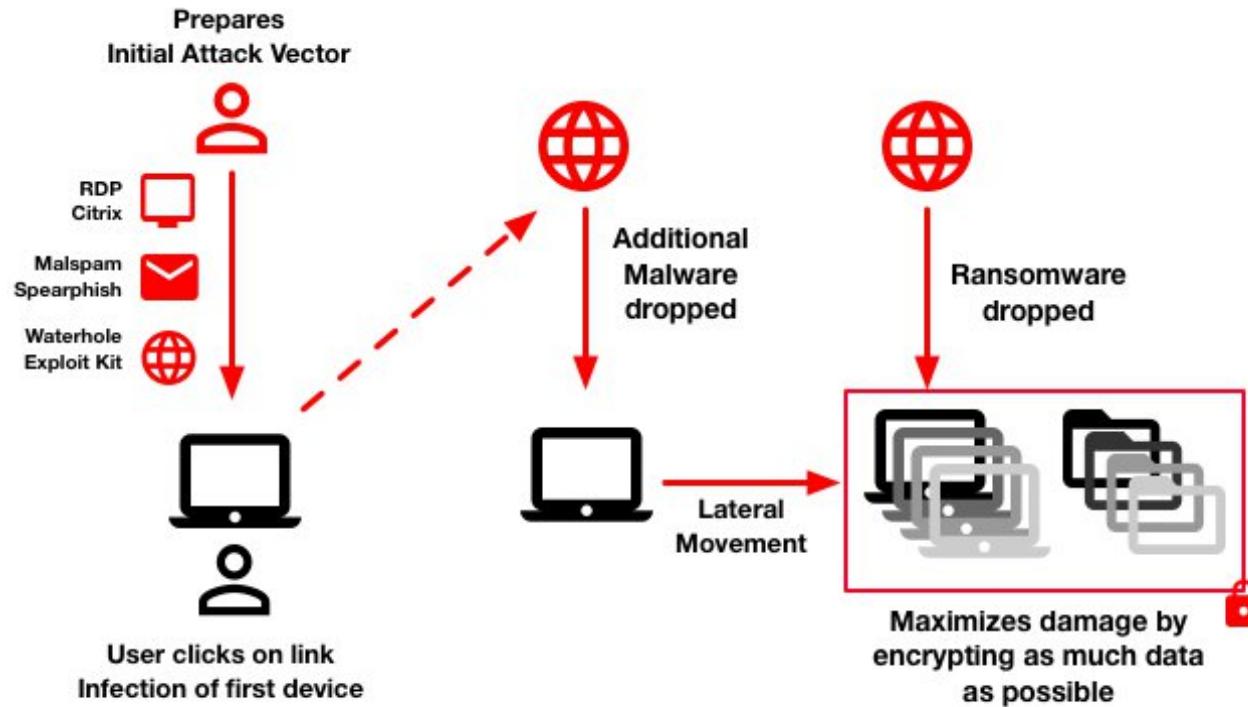
"Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. **Shorthand for malicious software**, malware typically consists of code developed by cyberattackers, designed to **cause extensive damage to data and systems or to gain unauthorized access to a network**.

Malware is typically delivered in the form of a **link** or **file over email** and requires the user to **click on the link** or open the file to **execute the malware**.

Malware has actually been a threat to individuals and organizations since the early 1970s when the Creeper virus first appeared. Since then, the world has been under attack from hundreds of thousands of different malware variants, all with the intent of causing the most disruption and damage as possible."

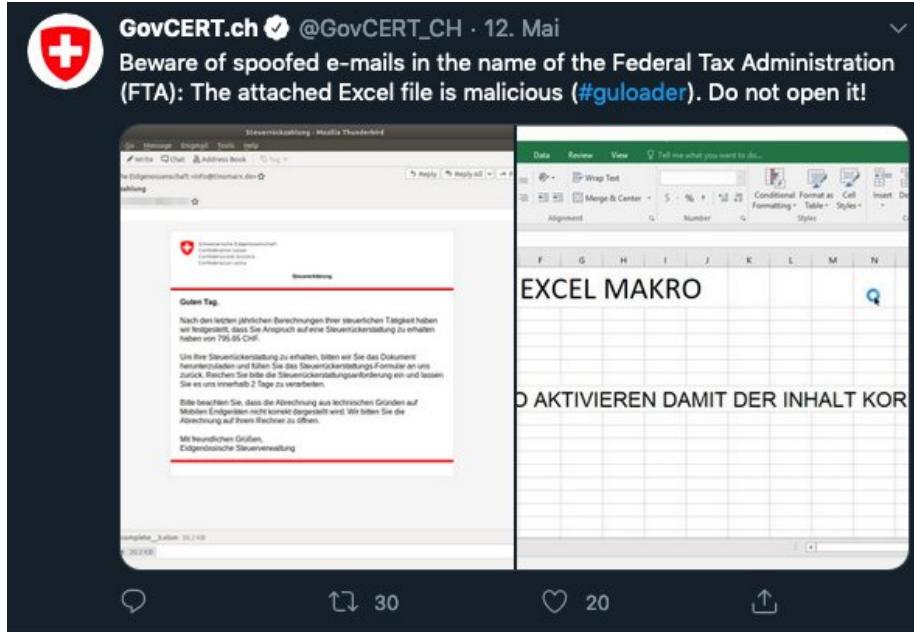
<https://www.forcepoint.com/cyber-edu/malware>

# Malware Attack



cc-by-sa: govcert.ch

# Malware



# Malware

Demo <https://hybrid-analysis.com>

<https://helgrind.switch.ch/joesandbox/index.php/analysis/463786>

# Emotet Infection @Heise

- June 2019
  - Initial infection vector: Email with Emotet malware
  - After execution, the malware spread in the whole network
  - More sophisticated malware / modules were then loaded
    - Domain controller from Active directory also infected?
    - Trickbot
  - Heise decided to full lockdown their network
  - External consultants were hired: Incident response and forensic experts
  - At least 50'000 Euro damage
- 
- <https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html>
  - <https://www.heise.de/security/meldung/Emotet-bei-Heise-Schaeden-von-weit-ueber-50-000-Euro-4444155.html>

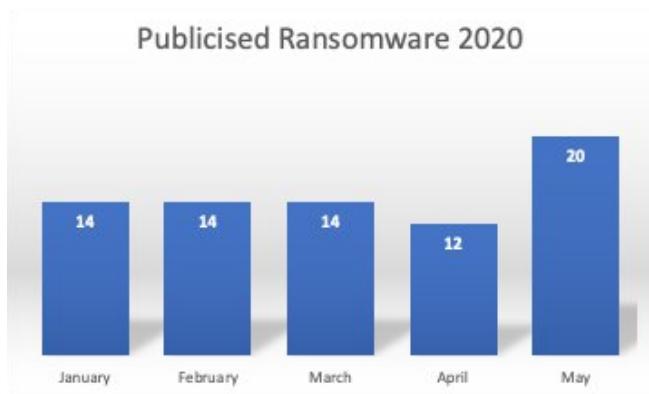
# Conficker Experience

- Found infection by Account Locking (Directory Order)
- Analysis of Security-Logs showed infected Machines
- Antivirus Software on Server was stopped
- Fix from Antivirus Vendor were published and used
- Virus was Hopping between Machines
- It ended up on the Domain Controller it self.

# Ransomware



# Publicised Ransomware Attacks 2020



## Affected well-known Companies:

- Cognizant
- Stadler
- Diebold Nixdorf
- Ruhr University Bochum
- Michigan State University

source:

<https://www.blackfog.com/the-state-of-ransomware-in-2020/>

# Maze Ransomware



The image shows the landing page for Maze Ransomware. At the top center is a large orange circular logo featuring a complex maze pattern. Below the logo, the text "Maze Ransomware" is displayed in a white serif font. The main content area has a dark background. It starts with a question "What's just happened?" followed by a explanatory text: "If you see this page it means you are lucky, because we kindly give you the chance to recover your data. Please upload your ransom note using the form below and start recovering your data. If the ransom note is recognized by our parser, you will be successfully authorized and provided with further instructions." Below this is a file upload input field with the placeholder "Choose File No file chosen". The page is divided into three sections at the bottom: "Guarantees?", "Antivirus corporations?", and "Price?". Each section contains text and a small blue circular icon.

**Guarantees?**

We can recover your files, as our ransomware is carefully designed to keep the integrity of your encrypted data.

Don't be afraid and start recovering!

**Antivirus corporations?**

If you are waiting for a free solution to come, we must disappoint you. Our ransomware uses a strong combination of algorithms. It will require decades to crack.

Start working with us.

**Price?**

We understand that the customer cannot always pay the ransom. We have discounts and sometimes you might recover your files just by working with us.

# Insights of Maze

Time	What happened
2018 Oct	Intrusions via Flash Player and VBScript
2019 Oct	Spam campaign against German IT Service and Italian manufacturer companies (via attached Macro enabled Word Files)
2019 Nov	Threat actors start to leak unpaid Ransom first via bleepingcomputer and afterwards on Russian Forums
2019 Dec	Threat actors distancing from NAC shooting and emphasize they will not target Health Sector (if Maze is used they will provide free encryption)

Source:

<https://www.tripwire.com/state-of-security/featured/maze-ransomware-what-you-need-to-know/>

[https://1f3r982zgpjh2wuihs3suki9-wpengine.netdna-ssl.com/wp-content/uploads/2019/12/Maze\\_Whitepaper.pdf](https://1f3r982zgpjh2wuihs3suki9-wpengine.netdna-ssl.com/wp-content/uploads/2019/12/Maze_Whitepaper.pdf)

# Maze ant their Ransome

Company	Leaked Data	Ransome
Boygues construction	200 GB	10 Mio €
Allied Universal Security	5 GB	2.3 Mio \$ (300 BC)
MDLAB	100 GB	1.4 Mio \$ (100 BC) Encryption 1.4 Mio \$ (100 BC) Data Destruction
Southwire	120 GB	6 Mio \$ (850 BC)

# Clop Ransomware at Maastricht University

Time (2019)	Movement
2019 Oct	First Breach by Phising
2019 Nov	Lateral Movement (System with failed Patches)
23. Dec	Ransomware attacks and Displays Message
24. Dec	Contact Fox-IT for
26. Dec	Police has been notified
30. Dec	University decides to pay 217'000 \$ in Bitcoins

sources:

<https://www.rijksoverheid.nl/documenten/rapporten/2020/02/05/reactie-universiteit-maastricht-op-rapport-fox-it>

<https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks>

# Key Points: Current Security Topics

- Three types of Phishing: Generic, Spear and CEO Fraud
- HTTPS doesn't help against phishing
- Report phishing
- Ransomware is currently the biggest malware threat

# 03 - Howto protect your assets

- CIA triad
- Methods used to ensure Confidentiality, Availability and Integrity
- Authentication and Authorisation
- Factors for Authentication

# Information Security

The term “information security” means **protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction** in order to provide

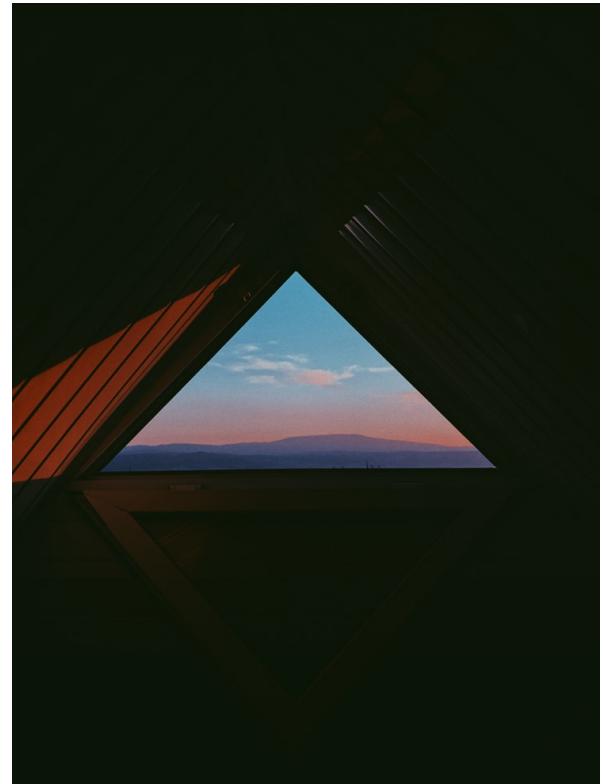
- (A) **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (B) **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (C) **availability**, which means ensuring timely and reliable access to and use of information.

<https://www.law.cornell.edu/uscode/text/44/3542>

# The CIA triad

The “CIA triad.” CIA stands for:

- **Confidentiality** through preventing access by unauthorized users.
- **Integrity** from validating that your data is trustworthy and accurate.
- **Availability** by ensuring data is available when needed.



<https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/>

# CIA triad example



# The CIA triad

**Situation:** General hospital and a specialised hospital. A patient has to be transferred to the specialised hospital. All available information from the patient should be transferred from the General hospital to the specialised hospital.

From the CIA point of view:

- **Confidential:** Nobody except the recipient (Doctor) is able to read it
- **Integrity:** The information is fully transferred and no data has been altered
- **Availability:** The systems to which the Doctors / employees will access the data are available all the time

# Methods used to ensure Confidentiality

- Data encryption and authentication
- Encryption of the data in transit
- Using User IDs, passwords and other methods to access the encrypted data
- Extra measures (extreme form): Air gapped computers, disconnected storage devices hard copy only



# Methods used to ensure Integrity

- Maintaining the **consistency, accuracy, and trustworthiness** of data over its entire life cycle
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people
  - File permissions and user access controls
  - Version Control Systems
- Detect changes
  - Cryptographic checksums

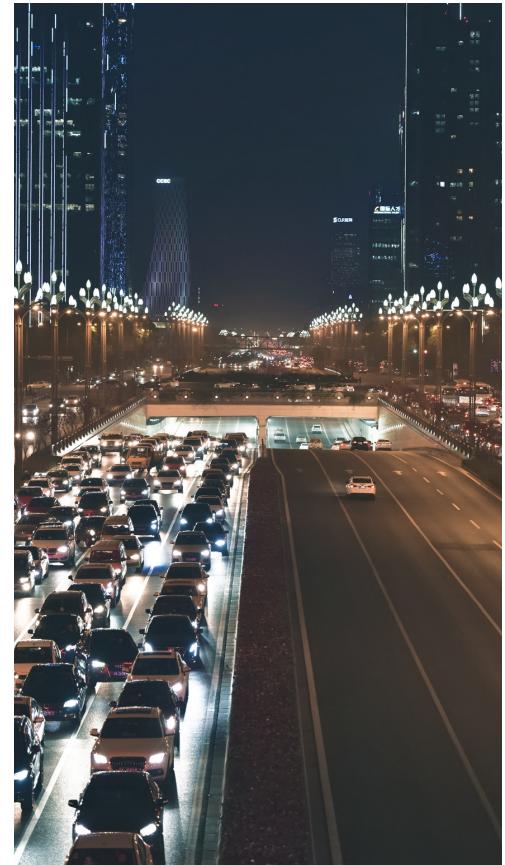
# Methods used to ensure Integrity

- **HMAC: Hash-based message authentication code**
- Is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key
- ~~MD5, SHA-256, SHA-3, ...~~

```
macbook:~ seitz$ echo -n "Hi all" | shasum -a 256  
e6cf54f1c0d4ec54e879ae23f41f87c7361550d7b385d20bd2ba4e9c6064a71a -  
macbook :~ seitz$ echo -n "Hi all" | shasum -a 256  
005a9b72487248c324348c754b7b7a695dd6b98aa0058ff6363f365763d11e8d -
```

# Methods used to ensure Availability

- Redundant hardware
- Fully maintained hardware
- Keep current with all necessary system upgrades and updates
- Ensure to have enough bandwidth to and from the systems
- Remove bottlenecks
- Hot failover
- RAID
- Planed (Disaster recovery plan - DRP) and trained disaster recovery.
- Backups
  - Geographically-isolated location
  - Fireproof, waterproof safe
- Measures against DDoS



# Authentication and Authorisation

- **Authentication (Who you are)**: The process of determining whether someone or something is who or what it declares itself to be.
  - “Are you really person X?”
  - Technical methods: Login Form, HTTP authentication, HTTP digest, X.509 certificate, ...
- **Authorisation (What you can do)**: Decides if you have permission to access a resource
  - Methods: Access controls for URLs, Secure objects and methods, Access control lists (ACLs)

# Authentication and Authorisation



# Factors for Authentication

- Something you **know**
  - Operating system password
  - Credit Card PIN
  - Safe pin
  - Smartphone unlock combination
  - Secret handshakes



# Factors for Authentication

- Something you **have**
  - Physical objects
  - Keys
  - Smartphones
  - Smart Cards
  - USB drives
  - Token devices



# Factors for Authentication

- Something you **are**
  - Fingerprint
  - Palm
  - Iris
  - Retina
  - Blood
  - DNA



# Factors for Authentication

- **(Somewhere you are)**
  - Related to your location
  - IP address



# Factors for Authentication

- **(Something you do)**
  - Gestures
  - Related to something you know



# Multifactor authentication (MFA)

- Combining two or three factors from the previous categories
- More secure because an attacker needs multiple skills to breach an account
- Attacker needs to perform **multiple successful attacks simultaneously**
- Famous example: 2FA
- If available: You should use 2FA

# Multi factor authentication - Examples



# Paper: “Evaluating Login Challenges as a Defense Against Account Takeover”

“In this paper, we study the efficacy of **login challenges at preventing account takeover** .... These secondary authentication ... trigger in response to a suspicious login or account recovery attempt. Using Google as a case study ... preventing over 350,000 real-world hijacking attempts stemming from automated bots, phishers, and targeted attackers. We show that knowledge-based challenges prevent as few as 10% of hijacking attempts rooted in phishing and 73% of automated hijacking attempts. **Device-based challenges provide the best protection, blocking over 94% of hijacking attempts rooted in phishing and 100% of automated hijacking attempts.**”

<https://ai.google/research/pubs/pub48119>

# Google's automatic, proactive hijacking protection

“if we **detect a suspicious sign-in attempt** (say, from a new location or device), we’ll ask for **additional proof** that it’s really you. This proof might be confirming you have access to a trusted phone or answering a question where only you know the correct response.“

“If you’ve signed into your phone or set up a recovery phone number, we can provide a similar level of protection to 2-Step Verification via device-based challenges. We found that an **SMS code sent to a recovery phone number helped block 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks.** On-device prompts, a more secure replacement for SMS, helped prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks.“

<https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>

# Google's automatic, proactive hijacking protection

## Account takeover prevention rates, by challenge type

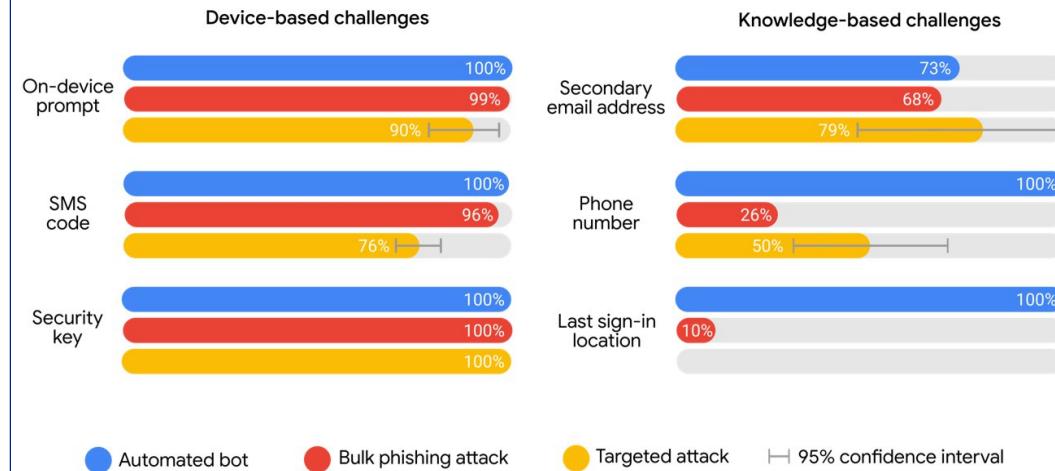


Image Source: <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>

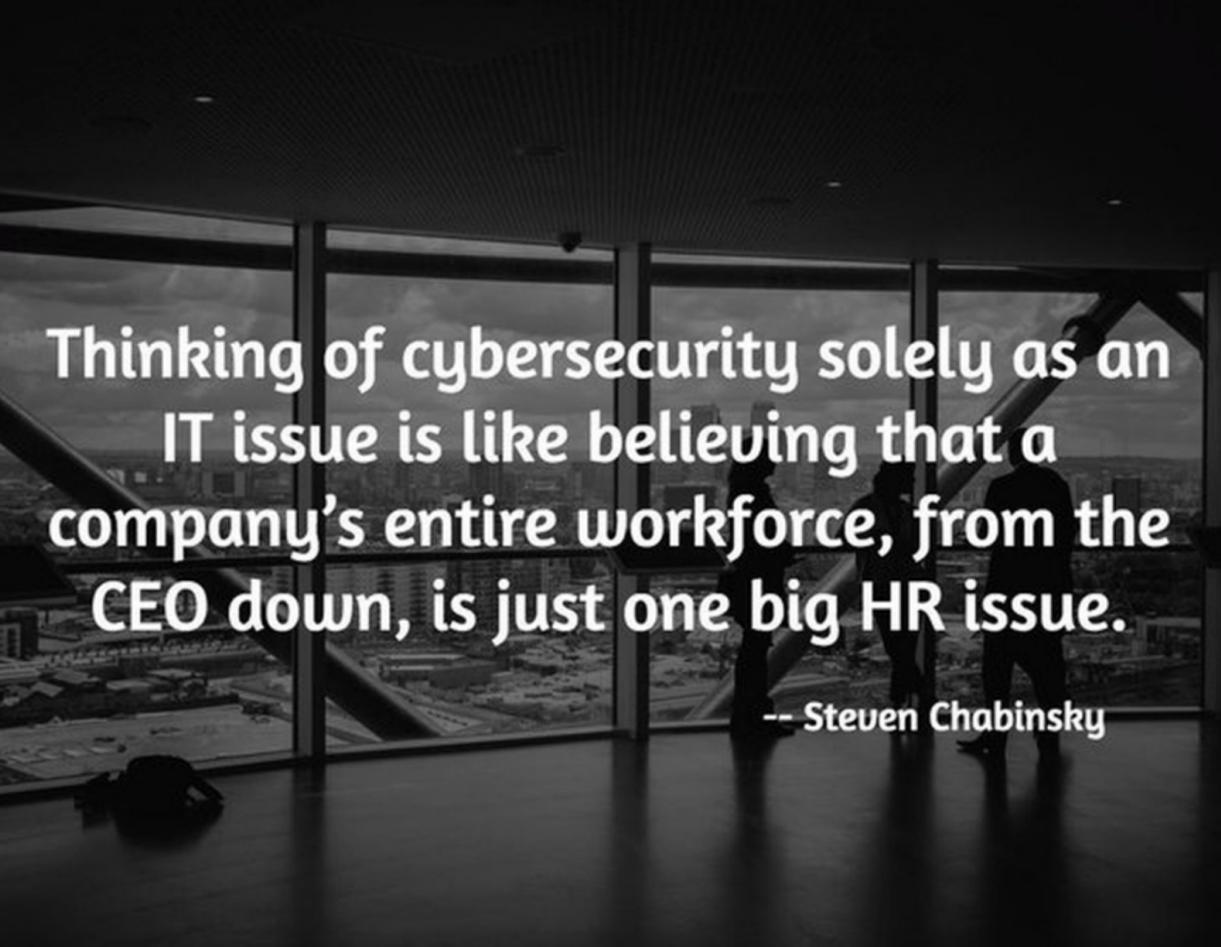
# Key Points: Howto protect your assets

- The CIA Triad
- Use different factors and more than one to protect your assets
- Authentication (Who you are) and Authorisation (What you can do)

# 04 - Good IT security practices

- Awareness
  - Passwords
  - Basic Security
- 
- Our Message to you:

**You are the most important link in the Chain of Security!**



**Thinking of cybersecurity solely as an  
IT issue is like believing that a  
company's entire workforce, from the  
CEO down, is just one big HR issue.**

-- Steven Chabinsky

# The Human Factor

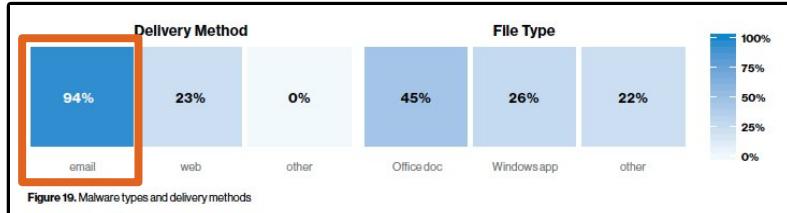
## Die Lage aus Sicht des Channels Der Ransomware Report

datto

Laut MSPs sind Phishing-E-Mails die Hauptursache für erfolgreiche Ransomware-Angriffe. Fehlende Schulungen im Bereich der Cyber-Sicherheit, schwache Passwörter und Nachlässigkeit sind weitere Hauptursachen.



\* Phishing E-Mails are main cause for Ransomware-Attacks

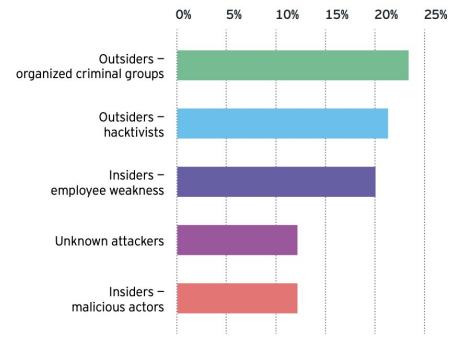


## 2020 Data Breach Investigations Report verizon

Abbildung 3: Welche Taktiken werden genutzt?



Figure 1: Attacks come from multiple sources, including hacktivists  
Threat actors behind confirmed breaches



## EY Global Information Security Survey 2020

# Passwords

## PEOPLE KNOW WHAT'S RIGHT, BUT THEY DO THE OPPOSITE

What people say	What people do
<b>91%</b>  91% say they know using the same or a variation of the same password is a risk ...	<b>66%</b>  ... however, when creating passwords, 66% of respondents always or mostly use the same password or a variation – this is up 8% from our findings in 2018.

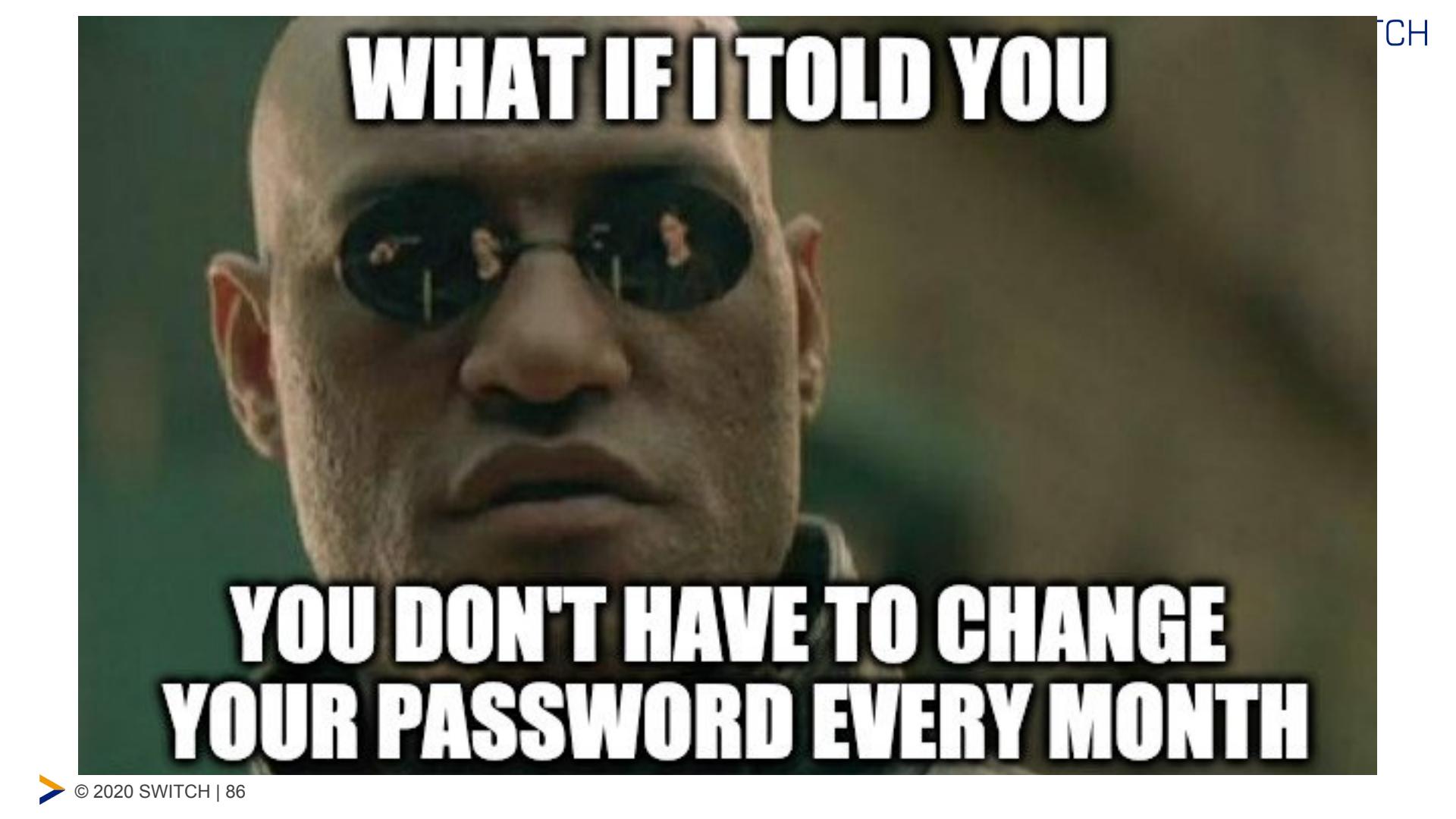
Psychology of Passwords: The Online Behavior That's Putting You at Risk

LastPass ••• |  
by LogMeIn

# Top 10 Passwords CH 2019\*

1. **123456**
2. **123456789**
3. **12345678**
4. **password**
5. **1234567**
6. **abc123**
7. **123123**
8. **123457890**
9. **Switzerland**
10. **111111**

\* Discovered cleartext passwords in leaks



**WHAT IF I TOLD YOU**

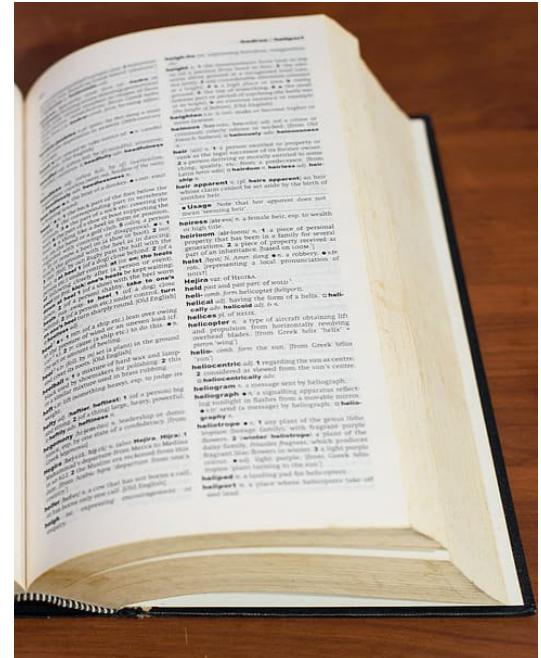
**YOU DON'T HAVE TO CHANGE  
YOUR PASSWORD EVERY MONTH**

# Best Practice with Password (NIST Standard)

- Use longer passwords
- No Passwords Expire (without Reason)
- No Composition Rules (Signs, Numbers, Big Letters)
- Do Check your password against compromised lists
- Use a Password Manager

# How attacker find bad passwords

- Brute Force
- Dictionary Attack
- Rainbow Tables (precalculated Hashes)
- Rule Based Dictionary | Brute Force



source:

<https://securityboulevard.com/2020/05/a-brief-summary-of-nist-password-guidelines/>  
<https://pages.nist.gov/800-63-3/sp800-63b.html>

# Password leaks and checks

- Latest Password Leak Jan. 2019 (Combolist)
- Have i been pwned?
- Hasso-Plattner-Institug

<https://haveibeenpwned.com/>

<https://sec.hpi.de/ilc/search?lang=de>

# Basic Security



# Basic Security

- Inventory
- Patch-Management
- Vulnerability-Management
- Hardening

# Inventory

- Forgotten Machines can be a Risk

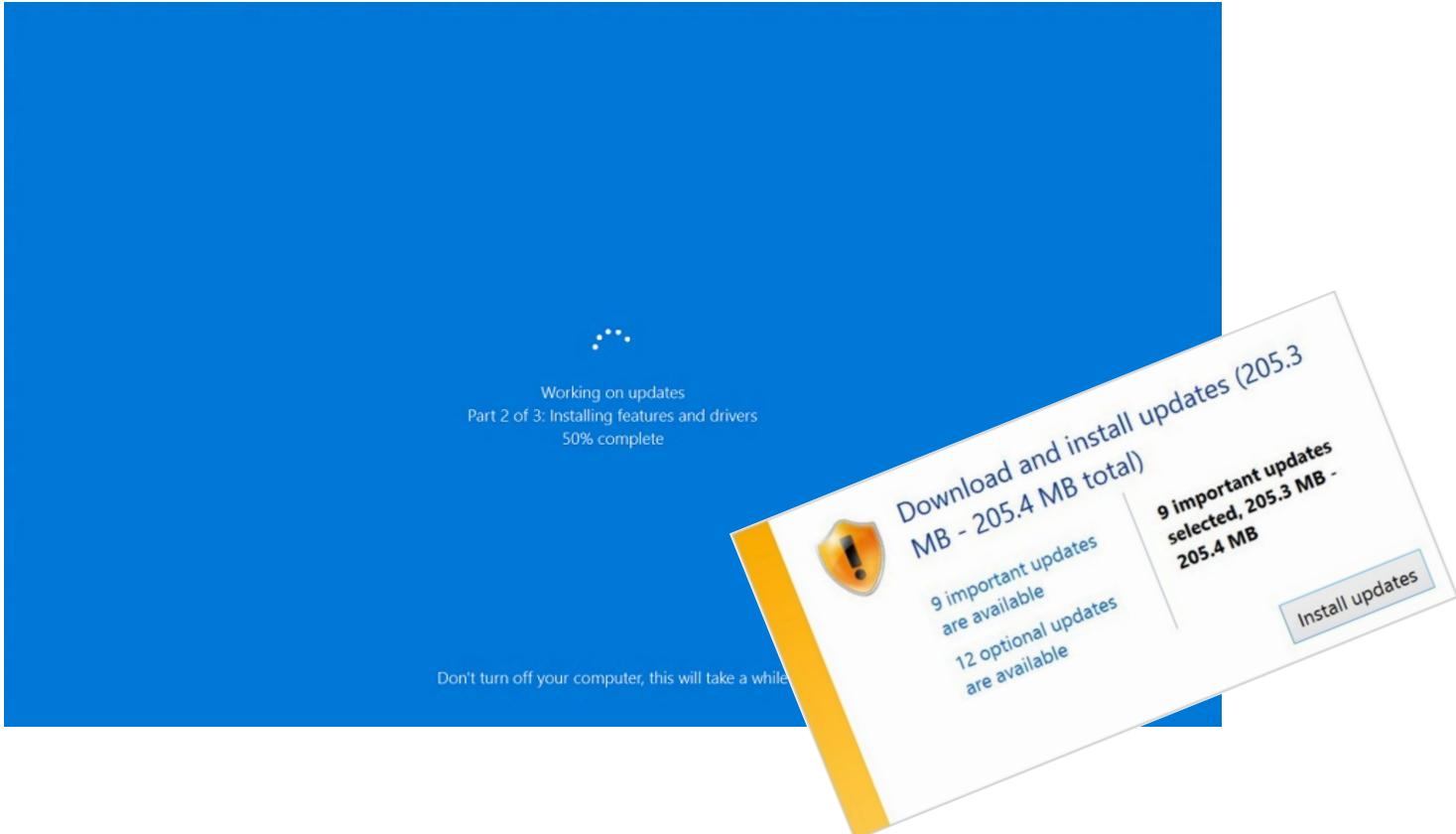
- Inventory:

- Machines
- Services
- Software

- You can also Inventory Risks and Data Collection



# Patch-Management

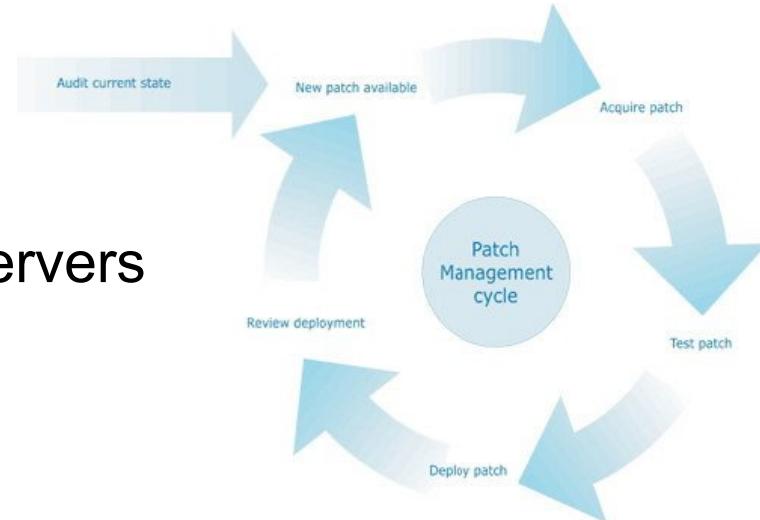


# Patching: Things to remember

- Patch Tuesday (2nd Tuesday)
- With the Patch usually the Vulnerability is Public
- Update as soon as possible
- Test your Updates before rolling out on all Machines
- Keep Test and Prod on the same Patch level
  
- Tipp: Subscribe to your Vendors Security Advisories

# When Patch Management went Wrong

- Citrix VDI
  - Patching Test servers first
  - Some Problems occurred on some Servers
  - Patch was deployed to all Servers
  - All Server had multiple downtimes
- => Didn't realize Problems were due to updates in Test-Week



# Vulnerability-Management



## Security Vulnerabilities Published in 2019

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2019-1010260</a>	284	1	Exec Code	2019-04-02	2019-04-04	9.2	None	Remote	Medium	Not required	Complete	Complete	Complete
Using ktlint to download and execute custom rulesets can result in arbitrary code execution as the served jars can be compromised by a MITM. This attack is exploitable via Man in the Middle of the HTTP connection to the artifact servers. This vulnerability appears to have been fixed in 0.30.0 and later; after commit 5e54702876f6c260d328a2cb58beb67a7ff2261.														
2	<a href="#">CVE-2019-1010258</a>	119	1	Overflow Mem. Corr.	2019-05-15	2019-05-16	4.3	None	Remote	Medium	Not required	None	None	Partial
nanosvg library nanosvg after commit c1f6e209c1b1b46aa9f945d7e619acf42c29726 is affected by: Buffer Overflow. The impact is: Memory corruption leading to at least DoS. More severe impact vectors need more investigation. The component is: it's part of a svg processing library. function nsSVG_parseColorGB in src/nanosvg.h / line 1227. The attack vector is: It depends library usage. If input was passed from the network, then network connectivity is enough. Most likely an attack will require opening a specially crafted .svg file.														
3	<a href="#">CVE-2019-1010257</a>	209	1	+Info	2019-03-27	2019-03-28	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
An Information Disclosure / Data Modification issue exists in article2pdf_getfile.php in the article2pdf Wordpress plugin 0.24, 0.25, 0.26, 0.27. A URL can be constructed which allows overriding the PDF's path leading to any PDF whose path is known and which is readable by the web server can be downloaded. The file will be deleted after download if the web server has permission to do so. For PHP versions before 5.3, any file can be read by null terminating the string left of the file extension.														
4	<a href="#">CVE-2019-1003099</a>	275	1		2019-04-04	2019-05-07	4.0	None	Remote	Low	Single system	None	Partial	None
A missing permission check in Jenkins openid Plugin in the OpenIdSSoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server.														
5	<a href="#">CVE-2019-1003098</a>	352	1	CSRF	2019-04-04	2019-04-22	4.3	None	Remote	Medium	Not required	None	Partial	None
A cross-site request forgery vulnerability in Jenkins openid Plugin in the OpenIdSSoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers to initiate a connection to an attacker-specified server.														

# Vulnerability Management

- There is always the possibility of an open door
- The Human factor: Errors
- The Centralized CVE Database
- Vulnerability Scanner (Nessus)
- Penetration Testing / External Scans
- Zero Day Exploits

# Types of Vulnerabilities

- DoS
- Code Execution
- Overflow
- Memory Corruption
- Sql Injection (OWASP)
- XSS (OWASP)
- Directory Traversal
- Http Response Splitting
- Bypass something
- Gain Information
- Gain Privileges
- CSRF
- File Inclusion

# CVE List by Mitre

## Security Vulnerabilities Published In 2019

2019 : January February March April May CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2019-1010260</a>	284		Exec Code	2019-04-02	2019-04-04	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

Using ktlint to download and execute custom rulesets can result in arbitrary code execution as the served jars can be compromised by a MITM. This attack is exploitable via Man in the Middle of the HTTP connection to the artifact servers. This vulnerability appears to have been fixed in 0.30.0 and later; after commit 5e547b287d6c260d328a2cb658dbe6b7a7ff2261.

2	<a href="#">CVE-2019-1010258</a>	119		Overflow Mem. Corr.	2019-05-15	2019-05-16	4.3	None	Remote	Medium	Not required	None	None	Partial
---	----------------------------------	-----	--	---------------------	------------	------------	-----	------	--------	--------	--------------	------	------	---------

nanosvg library nanosvg after commit c1f6e209c16b18b46aa9f45d7e619acf42c29726 is affected by: Buffer Overflow. The impact is: Memory corruption leading to at least DoS. More severe impact vectors need more investigation. The component is: it's part of a svg processing library. function nsvg\_parseColorRGB in src/nanosvg.h / line 1227. The attack vector is: It depends library usage. If input is passed from the network, then network connectivity is enough. Most likely an attack will require opening a specially crafted .svg file.

3	<a href="#">CVE-2019-1010257</a>	200		+Info	2019-03-27	2019-03-28	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
---	----------------------------------	-----	--	-------	------------	------------	-----	------	--------	-----	--------------	---------	---------	---------

An Information Disclosure / Data Modification issue exists in article2pdf\_getfile.php in the article2pdf Wordpress plugin 0.24, 0.25, 0.26, 0.27. A URL can be constructed which allows overriding the PDF file's path leading to any PDF whose path is known and which is readable to the web server can be downloaded. The file will be deleted after download if the web server has permission to do so. For PHP versions before 5.3, any file can be read by null terminating the string left of the file extension.

4	<a href="#">CVE-2019-1003099</a>	275			2019-04-04	2019-05-07	4.0	None	Remote	Low	Single system	None	Partial	None
---	----------------------------------	-----	--	--	------------	------------	-----	------	--------	-----	---------------	------	---------	------

A missing permission check in Jenkins openid Plugin in the OpenIdSsoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server.

5	<a href="#">CVE-2019-1003098</a>	352		CSRF	2019-04-04	2019-04-22	4.3	None	Remote	Medium	Not required	None	Partial	None
---	----------------------------------	-----	--	------	------------	------------	-----	------	--------	--------	--------------	------	---------	------

A cross-site request forgery vulnerability in Jenkins openid Plugin in the OpenIdSsoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers to initiate a connection to an attacker-specified server.

# Hands-On: CVE in Detail

- CVE-ID (Unique)
- Vulnerability Types
- Score
- Access (Remote, Local)
- Complexity

## Task:

Search CVS Score > 7.5 for a Software of your choice  
Present it afterwards in 30 seconds

# Software and Resource list

- Hadoop
- Elasticsearch
- Apache Spark
- MongoDB
- Redit
- Visual Studio Code
- Notepad++
- Microsoft Excel/Word/...
- Windows 10
- Cisco IOS

## Resources:

- <https://cve.mitre.org>
- <https://www.cvedetails.com>
- <https://nvd.nist.gov/vuln/>

# Vulnerability Scanner

- Vulnerability Scanner: Nessus
- also as Open Source: OpenVAS  
(Note: it has limited capabilities)

[Demo](#)

# Hardening

"Hardening is usually the process of securing a system by reducing its surface of vulnerability."

"Reducing available ways of attack typically includes **changing default passwords**, the **removal of unnecessary software**, unnecessary usernames or logins, and the **disabling or removal of unnecessary services**."

source: [https://en.wikipedia.org/wiki/Hardening\\_\(computing\)](https://en.wikipedia.org/wiki/Hardening_(computing))

# Default Pages

## Testing 123..

This page is used to test the proper operation of the [Apache HTTP server](#) after it has been installed. If you can read this page, your server is working properly. This server is powered by [CentOS](#).

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name 'webmaster' and the appropriate person.

For example, if you experienced problems while visiting [www.example.com](http://www.example.com), you should send e-mail to 'webmaster@example.com'.

Are you the Administrator?

You should add your website content to the directory `/var/www/html/`.

To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

Promoting Apache and CentOS



If a Hacker see these Pages, what do you think they know about your server?

# Example: CVE-2020-1938

"In Feb 2020, 54k systems were confirmed vulnerable on tcp/8009 to CVE-2020-1938 aka Ghostcat" (source: Security Mailing List)

CVE-ID	
<b>CVE-2020-1938</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	<p>When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.</p>

- There are still 25593 machines vulnerable!
- We received a list of 68 machines in Switzerland.

# Hardening: Things to remember

- Most Software not Hardened by default
  - Security vs. User-Friendly
  - Check Guides from Vendor
  - For some Configuration deep knowledge is required
- 
- Tipp: Change default passwords immediately, even for a test deployment

# Basic Security Roundup

- Know what you have (inventory)
- Stay updated - Subscribe to Security advisories
- Change standard passwords immediately
- Harden your systems (according to recommendations)
- Run an external Vulnerability scans

There is no perfect security  
try to find a balance between effort and reward  
the basic rules gives you quick rewards

# OWASP



# OWASP

## OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

<https://www.owasp.org>

# About OWASP

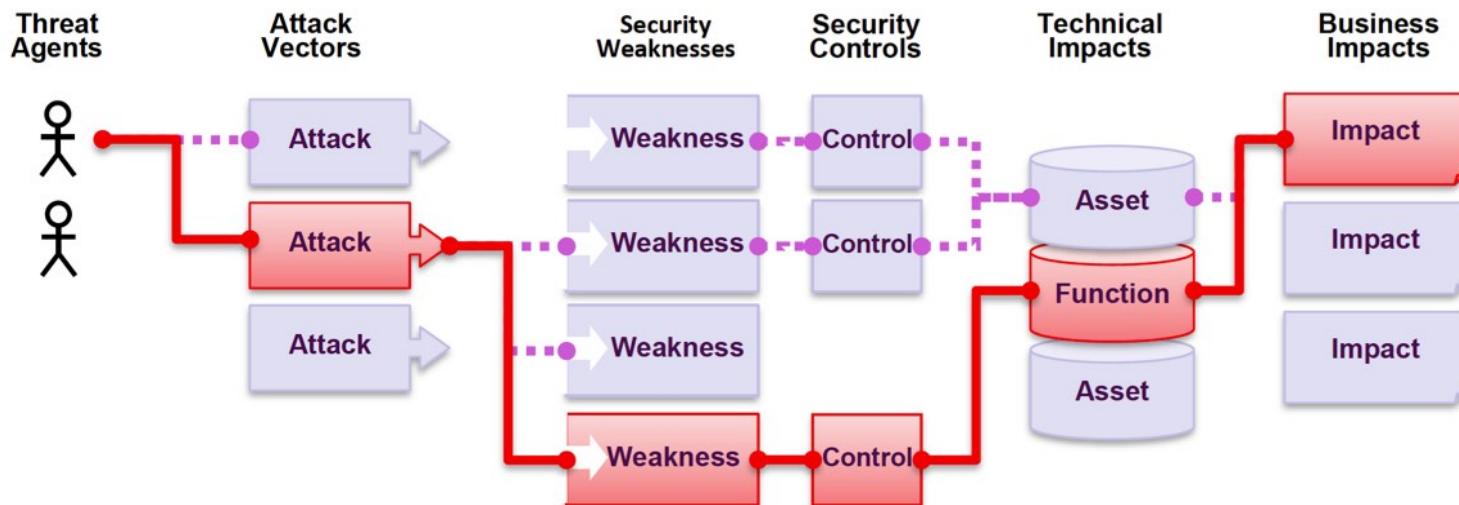
- The **Open Web Application Security Project** (OWASP) is an **open community** dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.
- At OWASP, you'll find free and open:
  - Application security tools and standards.
  - Complete books on application security testing, secure code development, and secure code review.
  - Presentations and videos
  - Cheat sheets on many common topics.

Learn more at: <https://www.owasp.org>

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↳	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	↳	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↳	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	↳	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

# What Are Application Security Risks?

- **Attackers** can potentially use **many different paths** through your **application** to do harm to your business or organization. Each of these paths represents a **risk** that may, or may not, be serious enough to warrant attention.



# What's My Risk?

- The OWASP Top 10 focuses on identifying the **most serious web application security risks** for a broad array of organizations. For each of these risks, we provide generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
Application Specific	Easy: 3	Widespread: 3	Easy: 3	Severe: 3	Business Specific
	Average: 2	Common: 2	Average: 2	Moderate: 2	
	Difficult: 1	Uncommon: 1	Difficult: 1	Minor: 1	

# OWASP Top 3

## Top 3

- A1:2017 Injection
- A2:2017 Broken Authentication
- A3:2017 Sensitive Data Exposure



# A1:2017 Injection

- **Problem:** User-supplied data is not validated, filtered, or sanitized by the application (Interpreter)
- Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries.
- **Impact:** Injection can result in **data loss, corruption, or disclosure to unauthorized parties**, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact **depends on the needs of the application and data**.

# A1:2017 Injection - Example Attack Scenarios

**Scenario #1:** An application uses untrusted data in the construction of the following **vulnerable** SQL call:

```
String query = "SELECT * FROM accounts WHERE  
custID='' + request.getParameter("id") + """;
```

**Scenario #2:** Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts  
WHERE custID='' + request.getParameter("id") + "");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: '**' or '1'='1**'. For example:

**<http://example.com/app/accountView?id=' or '1='1>**

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify or delete data, or even invoke stored procedures.

# A1:2017 Injection - Prevention

- The preferred option is to use a **safe API**, which avoids the use of the interpreter entirely or provides a **parameterized interface**
- **Use positive or "whitelist" server side input validation.** This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- Use **LIMIT and other SQL controls** within queries to prevent mass disclosure of records in case of SQL injection.
- For any residual dynamic queries, **escape special characters** using the specific escape syntax for that interpreter.
- For old software / applications: Use a **Web Application Firewall** to filter out the malicious queries

# A2:2017 Broken Authentication

- **Problem:** Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools.
- Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks
- **Impact:** Attackers have to gain access to only a few accounts, or just one admin account to compromise the system. Depending on the domain of the application, this may **allow money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.**

# A2:2017 Broken Authentication – Example Attack Scenarios

- **Scenario #1:** Credential stuffing , the use of **lists of known passwords** , is a common attack. If an application does not implement **automated threat or credential stuffing protections**, the application can be used as a **password oracle** to determine if the credentials are valid.
- **Scenario #2:** Most authentication attacks occur due to the continued use of **passwords as a sole factor**. Once considered best practices, password rotation and complexity requirements are viewed as encouraging users to use, and reuse, weak passwords. Organizations are recommended to stop these practices per NIST 800 63 and **use multi factor authentication**.
- **Scenario #3:** Application **session timeouts aren't set properly**. A user uses a public computer to access an application. Instead of selecting “**logout**” the user simply closes the browser tab and walks away. An attacker uses the same browser an hour later, and the user is still authenticated.

# A2:2017 Broken Authentication – Prevention

- Implement **multi factor authentication** to prevent attacks.
- Do not ship or deploy with **any default credentials**, particularly for admin users.
- Implement **weak password checks**, e.g. against a list of the top 10000 worst passwords
- Align password length, complexity and **rotation policies** with NIST 800 63 B's
- Ensure **registration, credential recovery**, and API pathways are **hardened** against account enumeration attacks by using the same messages for all outcomes.
- **Limit** or increasingly delay **failed login attempts**.
- Use a server side, secure, **built in session manager** that generates a new random session ID with high entropy after login.
- **Session IDs should not be in the URL**, be securely stored and invalidated after logout, idle, and absolute timeouts

# A3:2017 Sensitive Data Exposure

- **Problem:** Rather than directly attacking crypto, **attackers steal keys, execute man in the middle attacks, or steal clear text data off the server**, while in **transit**, or from the user's client, e.g. browser. A manual attack is generally required. Previously **retrieved password databases** could **be brute forced** by Graphics Processing Units (GPUs).
- The most common flaw is simply **not encrypting sensitive data**. When crypto is employed, **weak key generation and management**, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques.
- **Impact:** Failure frequently **compromises all data that should have been protected**. Typically, this information includes **sensitive personal information (PII)** data such as health records, credentials , personal data, and credit cards, which often require protection as defined by **laws** or regulations such as the **EU GDPR** or local **privacy laws**.

# A3:2017 Sensitive Data Exposure – Example Attack Scenarios

- Scenario #1: An application encrypts **credit card numbers** in a database using **automatic database encryption**. However, this data is automatically decrypted when **retrieved**, allowing an **SQL injection flaw** to retrieve credit card numbers in clear text.
- Scenario #2: A site doesn't use or enforce **TLS** for all pages or supports **weak encryption**. An attacker **monitors network traffic** (e.g. at an insecure wireless network), **downgrades** connections from **HTTPS to HTTP**, intercepts requests, and steals the user's session cookie. The attacker then **replays** this cookie and hijacks the user's (authenticated) session, accessing or modifying the **user's private data**. Instead of the above they could alter all transported data, e.g. the recipient of a money transfer.
- Scenario #3: The password **database** uses **unsalted** or **simple hashes** to store everyone's passwords. A file upload flaw allows an attacker to **retrieve the password database**. All the unsalted hashes can be exposed with a **rainbow table** of pre **calculated hashes**. Hashes generated by simple or fast hash functions may be cracked by GPUs, even if they were salted.

# A3:2017 Sensitive Data Exposure – Prevention

- **Classify** data processed, stored, or transmitted by an application.
- **Apply controls** as per the **classification**.
- **Don't store sensitive data unnecessarily**. Discard it as soon as possible. Data that is not retained cannot be stolen.
- **Make sure to encrypt all sensitive data at rest**.
- Ensure up to date and **strong standard algorithms**
- **Encrypt all data in transit** with **secure protocols**
- **Disable caching** for **responses** that contain **sensitive data**.
- Store passwords using strong adaptive and **salted hashing functions**
- **Verify independently** the effectiveness of configuration and settings.

# Further hands on info and exercises

A screenshot of the Hacking-Lab website homepage. The header features a large 'H' logo and the text 'HACKING-LAB®'. It includes a user count (135672), a post count (187), and links for 'Login page' and 'Sign up'. A navigation bar on the left lists 'Home', 'About', 'Membership', 'Security Events', 'Reference Projects', 'How it Works', 'Global Scoring', 'Mobile Services', 'Download', 'Jobs', and 'Login / Sign up'. Below the navigation bar are several cards: 'Membership' (Become a Hacking-Lab member!), 'HACKvent 2018' (Closed), 'Hacking-Lab Services' (Jazz up your class or training!), 'CSCG 2019' (Cyber Security Challenge Germany, Closed), 'ACSC 2019' (Austria Cyber Security Challenge, Running), and 'Hacky Easter 2019' (Closed).

The Hacking-Lab website homepage displays various challenges and services. Key features include:

- Membership:** Encourages users to become members.
- HACKvent 2018:** A completed challenge.
- Hacking-Lab Services:** Offers services for educational institutions.
- CSCG 2019:** A completed challenge from the Cyber Security Challenge Germany.
- ACSC 2019:** An ongoing challenge from the Austria Cyber Security Challenge.
- Hacky Easter 2019:** A completed challenge.

## What is Hacking-Lab?

Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents. ... Hacking-Labs' goal is to raise awareness towards increased education and ethics in information security through a series of cyber competitions that encompass forensics, cryptography, reverse-engineering, ethical hacking and defense. One key initiative for Hacking-Lab is to foster an environment that creates cyber protection through education.

<https://www.hacking-lab.com/about/>

# Key Points: Good IT security practices

- Security is also a Human factor
- Use a Password Manager
- Keep your Systems up to date
- Use Security Guides (from Vendor and Guides like OWASP)
- Your Company should have Processes in place to ensure the above points

# 05 - How to react to a Security Incident



# How to react to a Security Incident

- Contact the right person within your organisation
  - CISO
  - Security Officer, SOC, CERT
  - IT department
  - CEO, Marketing / Communication
- Get external support if necessary
  - Incident Response Specialists, Forensic Experts
- Report the Security Incident
  - NREN organisations: SWITCH-CERT (<https://www.switch.ch/security/contact/>)
  - Melani (<https://www.govcert.admin.ch/report/>)
- Press charges (against unknown)
  - <https://www.kkpks.ch/de/organisation/polizeikorps>

# How to React to a Security Incident

## Report an incident to MELANI

If you want to report an IT security incident to MELANI, please use the following contact form:

- [MELANI Reporting Form](#)

## Point of contact for CERTs and CSIRTs

As GovCERT.ch is the technical team of MELANI, the following email address can be considered as point of contact for FIRST members and other CERTs/CSIRTs. Please also direct any inquiries or reports regarding critical IT infrastructure in Switzerland to this email address. If you wish to communicate through a secure channel, please use our PGP key (download: [0x61624749](#)) or SMIME certificate (download: [govcert.crt](#)).

Report an incident: incidents[at]govcert{dot}ch

## Report a phishing site or phishing email

If you want to report a phishing site or phishing email, you can report them to antiphishing.ch:

- [antiphishing.ch](#)

## Report a crime

If you wish to report a crime, please direct your request to the Cybercrime Coordinate Unit (CYCO), using the following contact form:

- [CYCO Complaints Form](#)

### Point of Contact

- [Report an Incident to MELANI](#)
- [Report a crime to CYCO](#)
- [Report phishing](#)
- [GovCERT.ch PGP-Key](#)
- [GovCERT.ch SMIME](#)

### Reporting addresses

Report an incident:  
Incidents[at]govcert{dot}ch

General inquiries:  
outreach[at]govcert{dot}ch

# How to React to a Security Incident

The screenshot shows a website for the Konferenz der kantonalen Polizeikommandanten (KKPKS). The header features the KKPKS logo and the text "KONFERENZ DER KANTONALEN POLIZEIKOMMANDANTEN". Below the header, there are language links "DE | FR". The main navigation menu on the left includes "Members Login", "Startseite", "Aktuell", "Organisation" (with sub-links "Wer wir sind", "Leitbild", "Mitglieder", "Präsident", "Vorstand", "Generalsekretariat", "Konkordate"), "Polizeikorps" (with sub-links "Partner & Links", "Kontakt", "Impressum", "Datenschutz"), and "Datenschutz". The breadcrumb navigation on the right indicates the current page is "Home > Organisation > Polizeikorps". A search bar is located in the top right corner. The main content area displays three entries for different cantonal police corps, each with a shield logo and name: "Kantonspolizei Aargau", "Kantonspolizei Appenzell Innerrhoden", and "Kantonspolizei Appenzell Ausserrhoden". In the background of the content area, there is a photograph of several police officers standing near a white police car.

<https://www.kkpks.ch/de/organisation/polizeikorps>

# 06 - Selected Topics and wishlist

- APT – Advanced Persistent Threat
- SSL / TLS Certificates
- Cryptology
- Asymmetric Ciphers (RSA/ECDSA)

# APT – Advanced Persistent Threat

- Long-term operations designed to infiltrate and/or exfiltrate valuable data without being discovered
- Very few, but targeted victim (group)
- Example Stuxnet
  - In development since at least 2005
  - Stuxnet targets SCADA systems
  - Responsible for causing substantial damage to
  - Worm is believed to be a jointly built American / Israeli cyberweapon

# APT – Advanced Persistent Threat

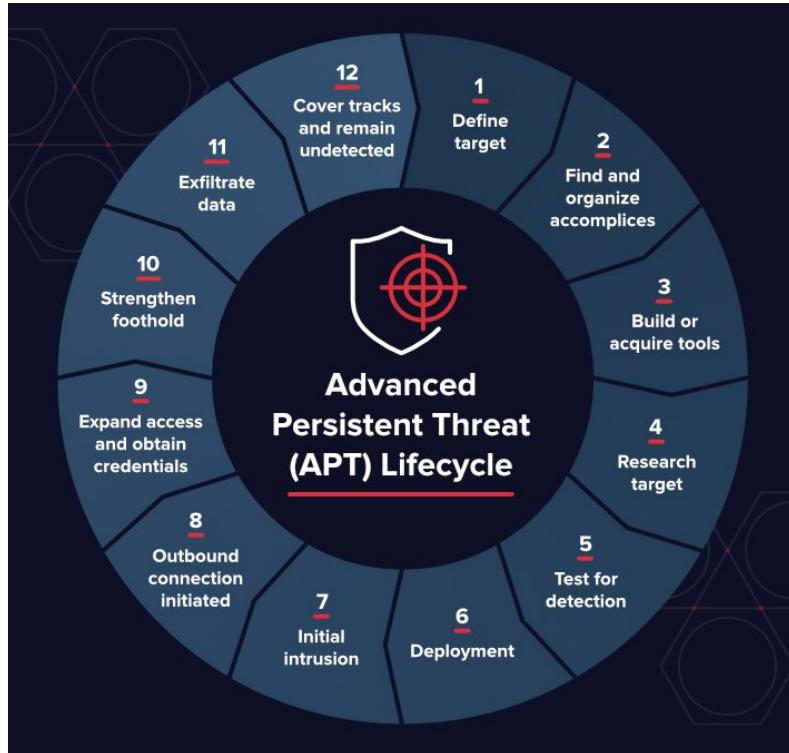


Image Source:

<https://www.varonis.com/blog/advanced-persistent-threat/>

# APT – Advanced Persistent Threat

- Different Names per APT group, depends on the IT security vendor. There is no standard
- As an example, from FireEye:

APT Groups: APT40 | APT39 | APT38 | APT37 | APT34 | APT33 |  
APT32 | APT30 | APT29 | APT28 | APT19 | APT18 | APT17 | APT16 |  
APT12 | APT10 | APT5 | APT3 | APT1

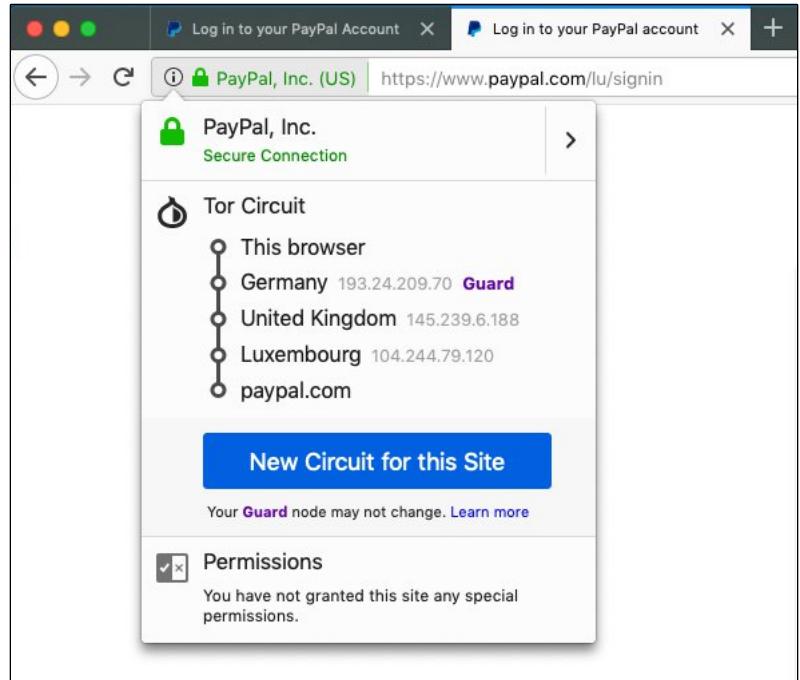
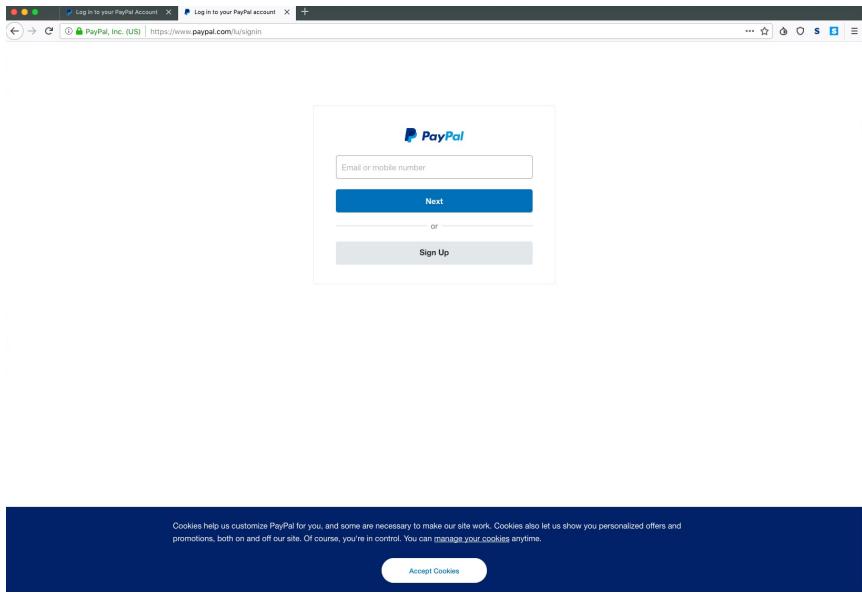
<https://www.fireeye.com/current-threats/apt-groups.html>

# APT – Advanced Persistent Threat

## APT40

- **Suspected attribution:** China
- **Target sectors:** APT40 is a Chinese cyber espionage group that typically targets countries strategically important to the Belt and Road Initiative ...
- **Overview:** FireEye Intelligence believes that APT40's operations are a cyber counterpart to China's efforts to modernize its naval capabilities; ...
- **Associated malware:** APT40 has been observed using at least 51 different code families. Of these, 37 are non-public. At least seven of these non-public tools (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDGETONE) are shared with other suspected China-nexus operators.
- **Attack vectors:** APT40 typically poses as a prominent individual who is probably of interest to a target to send **spear-phishing emails** ...

# SSL / TLS Certificates



# SSL / TLS Certificates

Page Info - https://www.paypal.com/lu/signin

General Media Permissions Security

**Website Identity**

Website: www.paypal.com  
Owner: PayPal, Inc.  
Verified by: DigiCert Inc  
Expires on: 18 August 2020

**Privacy & History**

Have I visited this website prior to today? No  
Is this website storing information (cookies) on my computer? No  
View Cookies  
Have I saved any passwords for this website? No  
View Saved Passwords

**Technical Details**

**Connection Encrypted (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, 128 bit keys, TLS 1.2)**  
The page you are viewing was encrypted before being transmitted over the Internet.  
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

?

Certificate Viewer: "www.paypal.com"

General Details

This certificate has been verified for the following uses:

SSL Client Certificate  
SSL Server Certificate

**Issued To**

Common Name (CN) www.paypal.com  
Organization (O) PayPal, Inc.  
Organizational Unit (OU) CDN Support  
Serial Number 01:5B:DA:66:5F:C4:4B:75:17:B6:88:2C:1E:AB:D4:DC

**Issued By**

Common Name (CN) DigiCert SHA2 Extended Validation Server CA  
Organization (O) DigiCert Inc  
Organizational Unit (OU) www.digicert.com

**Period of Validity**

Begins On 14 August 2018  
Expires On 18 August 2020

**Fingerprints**

SHA-256 Fingerprint 57:BD:41:24:4C:39:74:6F:04:E9:35:46:55:63:90:47:  
31:C0:A2:5E:42:28:CF:23:C1:D7:B1:A6:5D:CF:AB:01  
SHA1 Fingerprint E8:20:7A:27:8C:8E:D4:D9:7F:44:32:89:E7:6B:13:DD:CE:58:50:F6

Close

# Certificates

**Certificate Manager**

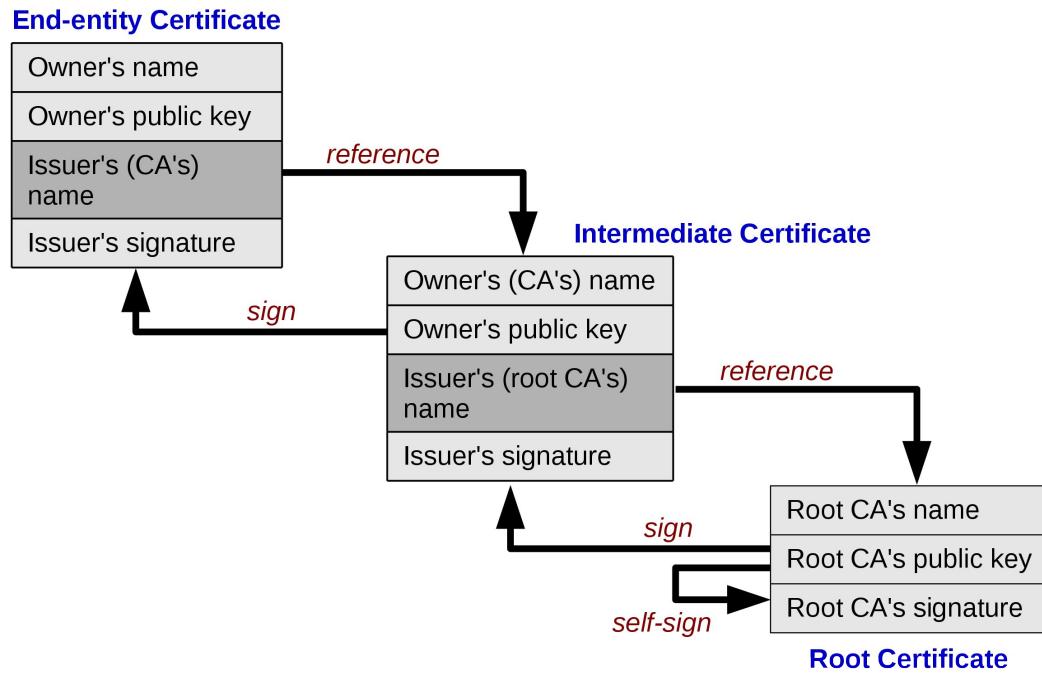
Your Certificates    People    Servers    Authorities

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
DigiCert Assured ID Root CA	Builtin Object Token
DigiCert Trusted Root G4	Builtin Object Token
DigiCert Global Root CA	Builtin Object Token
DigiCert Assured ID Root G3	Builtin Object Token
DigiCert High Assurance EV Root CA	Builtin Object Token
DigiCert Global Root G2	Builtin Object Token
DigiCert Assured ID Root G2	Builtin Object Token

**View...    Edit Trust...    Import...    Export...    Delete or Distrust...    OK**

# Chain of Trust and Root CA's



# SSL/TLS Certificate Classes

- Class 1
  - Considered to be **low assurance**
  - Confirms that the Subscriber **controls the asserted email address**
  - **No verification checks** of the Subscriber's **identity** are performed
  - This kind of certificate enables SSL encryption but makes it impossible for users to know the identity
  - This level of validation is referred to as **Domain Validation (DV)**
  - Free

# SSL/TLS Certificate Classes

- Class 2

- Considered to be **medium assurance**
- Provide a greater level of assurance over Class 1 Certificates
- **Basic verification steps** to confirm the identity of the Subscriber
- The certification authority guarantees the existence of the organization, that it owns the associated FQDN
- One of the organization's manager has authorized the certificate deliverance
- Referred to as **Organization Validation (OV)**
- \$

# SSL/TLS Certificate Classes

- Class 3

- Certificates provide a **high level of assurance**
- Issued only after rigorous validation of the identity
- Those are client certificates that are delivered after an audit that checks the organization and the certificate's owner
- This level of validation is referred to as **Extended Validation (EV)**
- \$\$\$

# Buy SSL/TLS Certificates

The chart compares three SSL/TLS certificate types:

- Business SSL:** Certificate with an increased level of assurance. Price: 8.- CHF/month (Term of 1 year). Rating: ★★☆. Suitable for: Service providers, Software and web service providers. Buy button.
- Business EV SSL:** Certificate with **highest** level of assurance. Price: 0.- CHF/month (Term of 2 years: First year free, then CHF 12.-/month). Rating: ★★★. Special Offer! Buy button.
- Business Wildcard SSL:** Certificate for your domain and all subdomains. Price: 30.- CHF/month (Term of 1 year). Rating: ★★★. Suitable for: SMEs and online shops, Online registrations, Large companies, Media platforms. Buy button.

- As an Example – There are plenty of providers
- <https://www.hostpoint.ch/en/ssl/ssl-certificate.html>

# Certificates

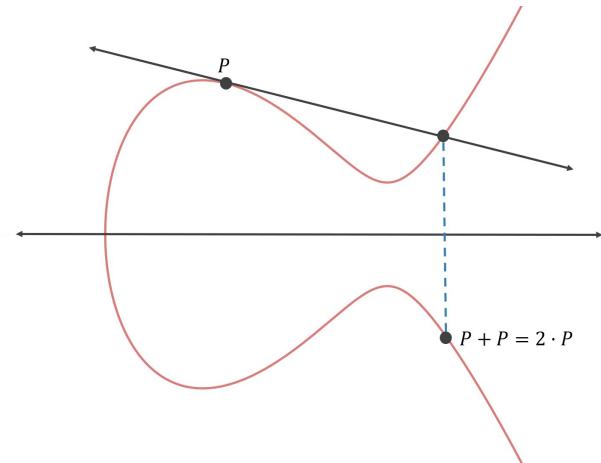
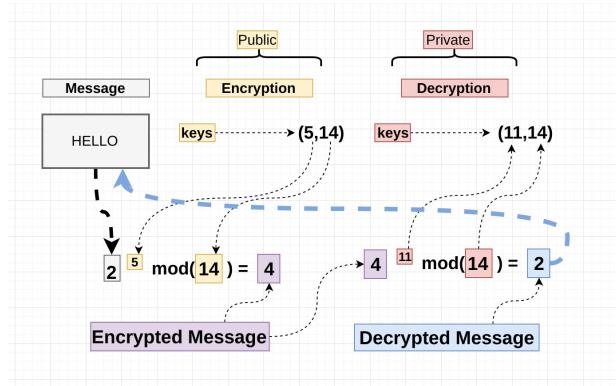
**Demo 1: Show certificates in browser**

**Demo 2: SSL Labs**

<https://www.ssllabs.com/ssltest/>

# Asymmetric Ciphers (RSA)

- RSA (Rivest/Shamir/Adelaid)
  - Secured by Factorization Problem
  - Exchange Exponent (Secret two Primes)
  - Big Key Size
- ECDSA
  - Secured by extreme amount of Points ( $2^{256}$ )
  - Exchange Curve Point  $X=x \cdot P$  (Secret  $x$ )
  - Relative small Key Size



# Future of Cryptology

- Quantum Computer will bypass Prime Factorization Problem
- D-Wave currently can factorizing a 17 bit Number  
(Far away from 2048 Bit)
- New Quantum Cryptography brings new possibilities

What does that mean?

- Even if actually your secrets are kept, in near future, all your encrypted Data can be decrypted!
- Bigger companies already prepare for this Date

# Source of current Information

- NIST (National Institute of Standards and Technology US)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)

# Passwords and offline Hacking

- Passwords should be stored as Hashes
- Here Example of Linux Password:

test:\$6\$n/L4kZYI\$tKLzmKZSU85laE6IIUjpUP[...]:18058:0:99999:7...

SHA512 SALT Hashed Password LastSet MinMax PW Age Day PW Remind

- Salt adds complexity to Crack

# Demo: Password cracking

- HashCat



# Entropy (information theory)

- Information entropy is measured in bits
- Strength of a password is measured with Entropy bits (Log2)
- Example:
  - Password policy: Length of the password must be 8 characters and has to contain a special character and is case-sensitive
  - Possibilities per character: 29 (uncapitalised) + 29 (capitalised) + 11 special characters (!" \$%&/()=?)  
= 69 possibilities per character

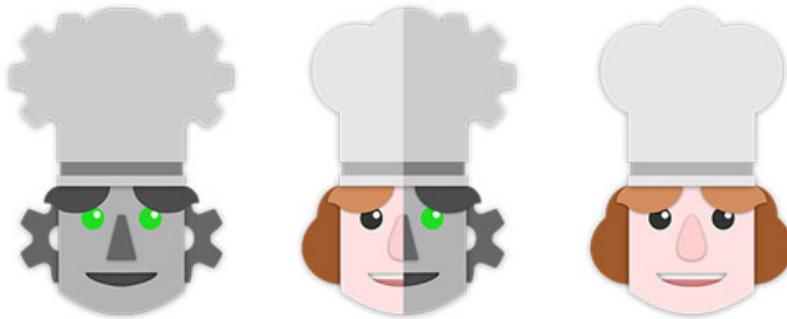
$\text{Log2}(69) = 6,1$  Bit entropy per character

**Password strength =  $8 * 6.1 = 48.9$  bits**

# Entropy (information theory)

- Calculate the password strength of the following two passwords
  - 10 characters, a-z and A-Z are allowed
  - 7 characters, a-z, A-Z and 0-9 are allowed

# Demo: Entropy with CyberChef



# CyberChef

# Cryptology

# Cryptology Where used in daily life?



## Task:

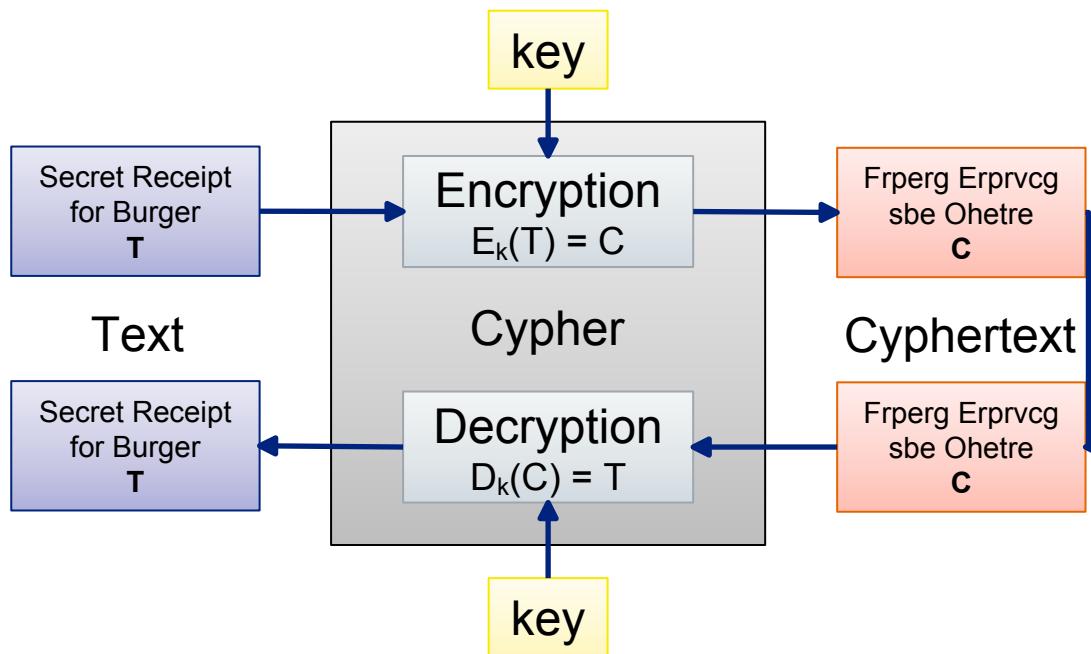
Take a Website and look at the Certificate.  
What Ciphers are they using? Try to find out...

# Cryptology Definition

Cryptology	
Cryptography	Cryptoanalysis
The art and science of <b>creating</b> ciphers	The art and science of <b>breaking</b> ciphers

# What is a Cipher?

- Algorithm to encrypt (or decrypt) a Message



# Cryptographic Algorithms

Algorithms		
Symmetric	Asymmetric	Hash
One Cipher and Key to Encrypt and Decrypt Data	Cipher with a Public and Private Key to Encrypt and Decrypt Data	Checksum of Data to prove consistency

# Basic Encryption

- Text

“We are here at UniBe learning about Security”

- Encrypted

“Jr ner urer ng HavOr yrneavat nobhg Frphevg!”

## Question / Task:

Any Idea what Cipher is used?

# ROT13 and Cryptoanalysis

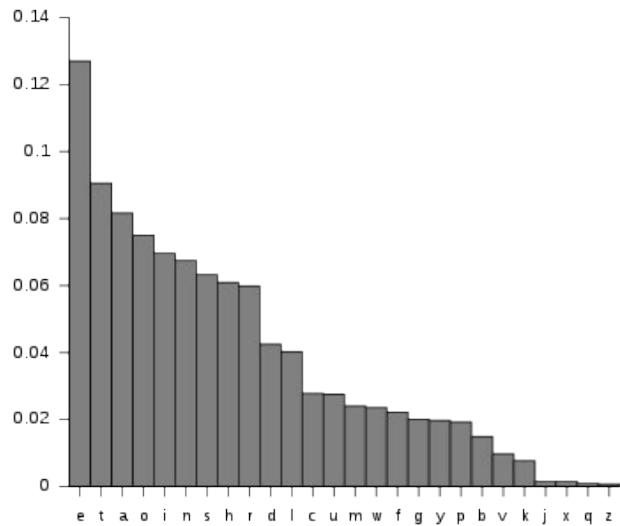
- Overlaying the Text, easy to find similarities  
“We are here at UniBe learning about Security”  
“Jr ner urer ng HavOr yrneavat nobhg Frphevg!”
- ROT13 Cipher (rotate by 13)
- Encryption and Decryption with same algorithm (and option)

# Distribution in the Text

- e: 7
- l: 7
- a: 4
- r: 4
- t: 3

**Task:**

Do you have an idea to make it more complex?



# Vigenere

Weareh|ereatU|niBele|arning|aboutS|ecurit|y  
 SWITCH|SWITCH|SWITCH|SWITCH|SWITCH|SWITCH|S

Oaikgo wnmtvB feJxnl snvbpn sxwnvZ wyckka q

## Task:

Do you have an idea to make it more complex?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Z	A	B	C	D	E	F	G	H	
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	

# XOR on Binary Level (switch bit if Key is 1)

T:

01010011010101101001001010100100001101001000

K:

0101010001011001010100100100100100111101001110

C:

00000110000111000011011000111010000110000000110

# Excercise: Encrypt and Hack

- Group up in Teams of two Members
- Write a Text and Use a Cesar Cipher
- Give it to your Neighbor group
- Try to Hack the Text

# 07 - Roundup und Feedback

Please fill out the feedback form from the University of Bern

[https://docs.google.com/forms/d/e/1FAIpQLSeK4JKDH415IJjPlq5EfULMZ07EnbGILmcg9L5UgWg4D\\_fkSw/viewform](https://docs.google.com/forms/d/e/1FAIpQLSeK4JKDH415IJjPlq5EfULMZ07EnbGILmcg9L5UgWg4D_fkSw/viewform)

# SWITCH

Working for a better digital world



# References

- [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_2017\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project)
- <https://www.entrustdatacard.com/knowledgebase/what-are-the-ssl-tls-certificate-assurance-levels>
- [https://en.wikipedia.org/wiki/Root\\_certificate#/media/File:Chain\\_of\\_trust.svg](https://en.wikipedia.org/wiki/Root_certificate#/media/File:Chain_of_trust.svg)
- <https://www.dynadot.com/community/help/question/what-is-punycode>
- <https://en.wikipedia.org/wiki/Stuxnet>
- <https://www.varonis.com/blog/advanced-persistent-threat/>
- <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
- <https://www.trendmicro.com/vinfo/us/security/definition/whale-phishing>
- <https://www.tbs-certificates.co.uk/FAQ/en/204.html>
- <https://www.cherwell.com/library/blog/what-is-an-information-management-security-system/>
- <https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one>
- <https://whatis.techtarget.com/definition/information-security-management-system-ISMS>
- <https://www.fortinet.com/blog/industry-trends/threat-intelligence-understanding-your-threat-actors-101-part-1-of-3.html>
- <https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors>