# IT-Security (ITS) B1

# DIKU, E2024

# Today’s agenda

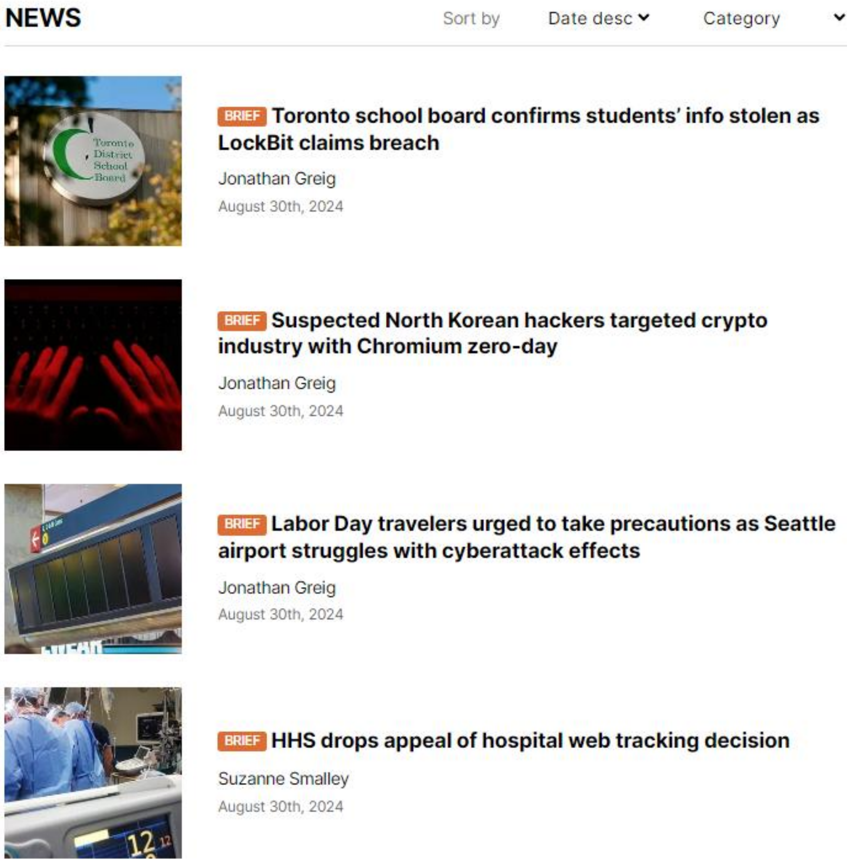
Part 1.

Course overview & Security defined

Part 2.

Who hacks?

# Security news



NEWS

Sort by Date desc Category

BRIEF **Toronto school board confirms students' info stolen as LockBit claims breach**

Jonathan Greig

August 30th, 2024

BRIEF **Suspected North Korean hackers targeted crypto industry with Chromium zero-day**

Jonathan Greig

August 30th, 2024

BRIEF **Labor Day travelers urged to take precautions as Seattle airport struggles with cyberattack effects**

Jonathan Greig

August 30th, 2024

BRIEF **HHS drops appeal of hospital web tracking decision**

Suzanne Smalley

August 30th, 2024

# Lectures

Lectures

Mondays at 10-12 in Aud 02 HCØ, Universitetsparken 5
Fridays at 10-12 in AUD 01 AKB, Universitetsparken 13

Instructors

James Avery (course organiser)
Troels Langkjær
Carsten Jørgensen

# Lecture plan

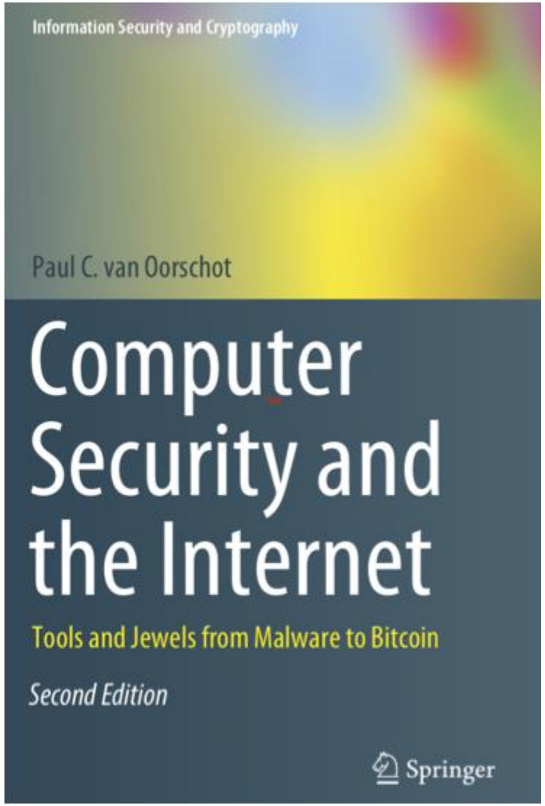
| Week | Date | Topic |
| ---- | ---- | ----- |
| 36 | 02 Sep | Security concepts and principles |
| | 06 Sep | Cryptographic building blocks |
| 37 | 09 Sep | Key establishment and certificate management |
| | 13 Sep | User authentication, IAM |
| 38 | 16 Sep | Operating systems security, web, browser and mail security |
| | 20 Sep | IT security management and risk assessment |
| 39 | 23 Sep | Software security - exploits and privilege escalation |
| | 27 Sep | Malicious software |
| 40 | 30 Oct | Firewalls and tunnels, security architecture |
| | 04 Oct | Cloud and IoT security |
| 41 | 07 Oct | Intrusion detection and network attacks |
| | 11 Oct | Forensics |
| 42 | | Fall Vacation - No lectures |
| 43 | 21 Oct | Privacy and GDPR |
| | 25 Oct | Privacy engineering |
| 44 | 28 Oct | Final guest lecture and Exam Q/A |

# Course book

Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, Second Edition by Paul C. van Oorschot. Springer, 2021

+ a few online resources

Note: Lectures focus on the big picture and are not 1:1 with the reading material


Information Security and Cryptography
Paul C. van Oorschot
Computer Security and the Internet
Tools and Jewels from Malware to Bitcoin
Second Edition
Springer

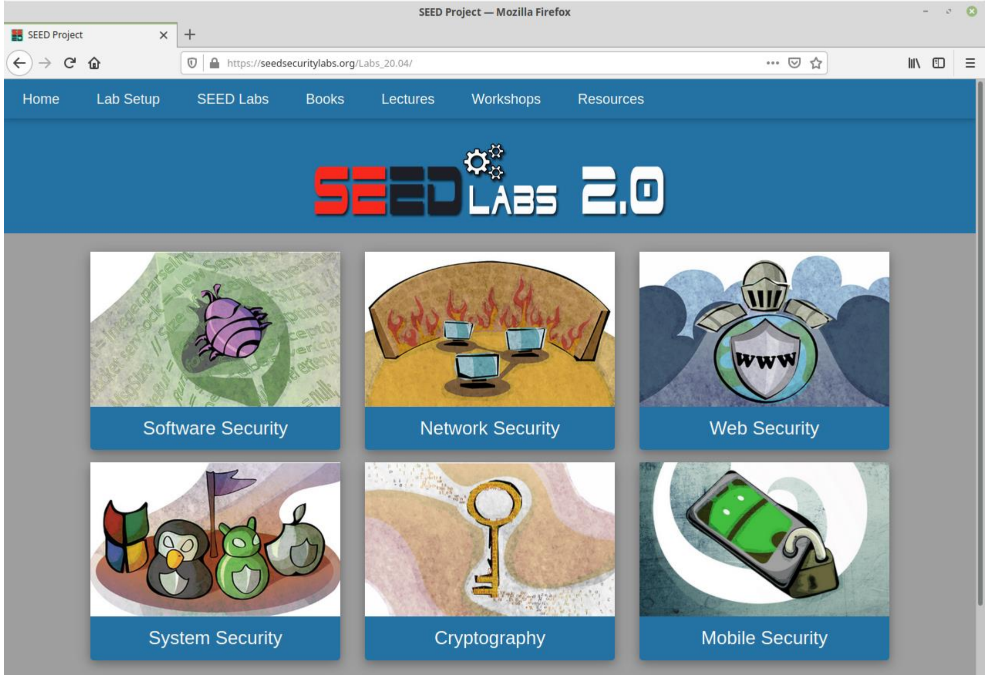
# Assignments

There are 6 weekly assignments during the course.

| Week | Date | Topic |
| ---- | ---- | ----- |
| 36 | 08 Sep | No handin first week |
| 37 | 15 Sep | Assignment 1 handin |
| 38 | 22 Sep | Assignment 2 handin |
| 39 | 29 Sep | Assignment 3 handin |
| 40 | 06 Oct | Assignment 4 handin |
| 41 | 13 Oct | Assignment 5 handin |
| 42 | 20 | Possible re-handin of one assignment (1-4) |
| 43 | 27 Oct | Assignment 6 handin |

Pass/fail; groups of up to 3; expect at least 66 % correct to pass; re-handin of only one.

# SEED Labs


SEED Project — Mozilla Firefox
SEED Project
https://seedsecuritylabs.org/Labs_20.04/
Home
Lab Setup
SEED Labs
Books
Lectures
Workshops
Resources
SEED LABS 2.0
Software Security
Network Security
Web Security
System Security
Cryptography
Mobile Security

# Exercise classes

Exercise classes

- Tuesdays 13-17 in Auditorium Syd, Nørre Alle 51 & Karnapsalen, Nørre Alle 53

TAs

- Lucas Haahr Yri
- Anders Friis Persson
- Johan Sørensen Topp

# Exam

08 Nov 2024

4-hour written exam

All aids allowed except Internet

(Oral re-exam)

# Course site

https://github.com/diku-its/e2024

# What you will learn

This course is *not*

- Not a course in how to hack
- Not the latest and greatest in hacks
- Not every aspect of IT-security

We focus on

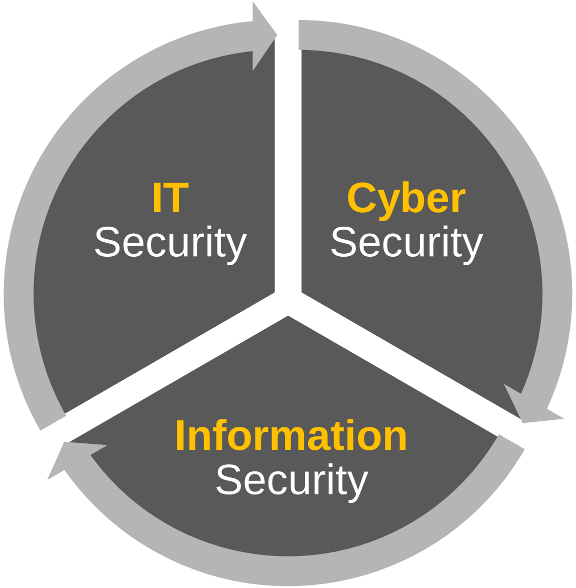
- Introduction to the field
- Breadth of topics, some depth
- Getting hands-on (assignments)

# Ethics and legal disclaimer

# Fame, or infamous

# So, what is IT-Security?

# Also known as (security, for short)



# IT-security is many things

Firewalls

Cryptography

Vulnerabilities

Exploits

Malware

Reverse engineering

Passwords

Patching

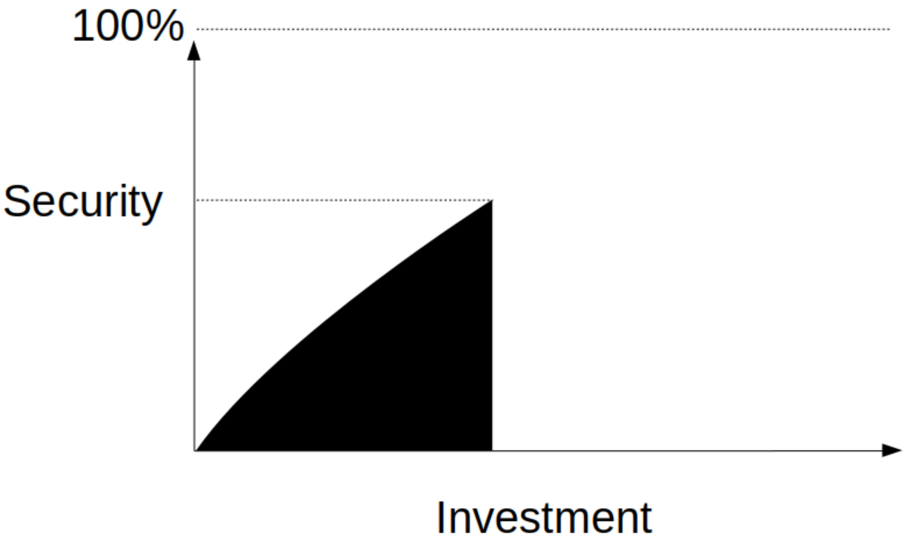
Threat models

Intrusion detection

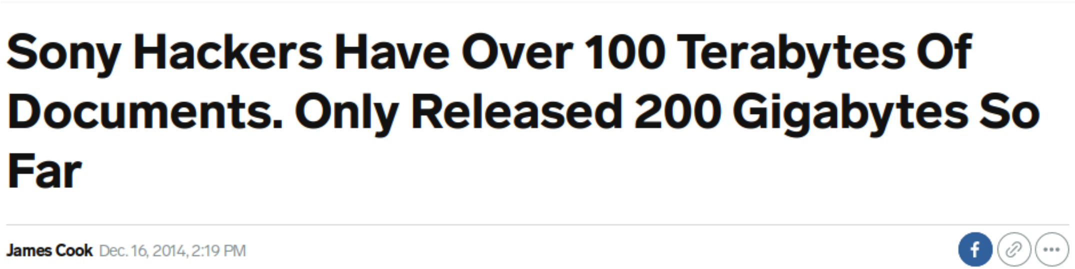
Security management

And much more

# 100% security is an illusion



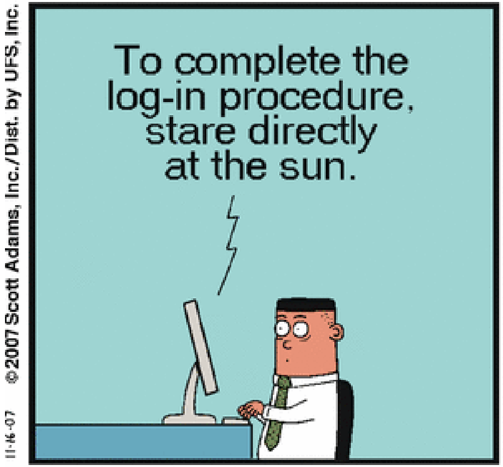
# Even big-budget firms get hacked

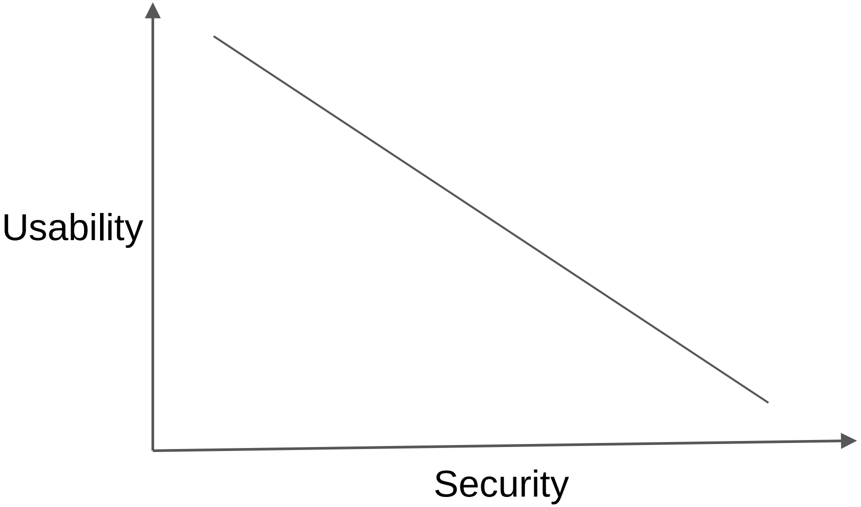


Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far

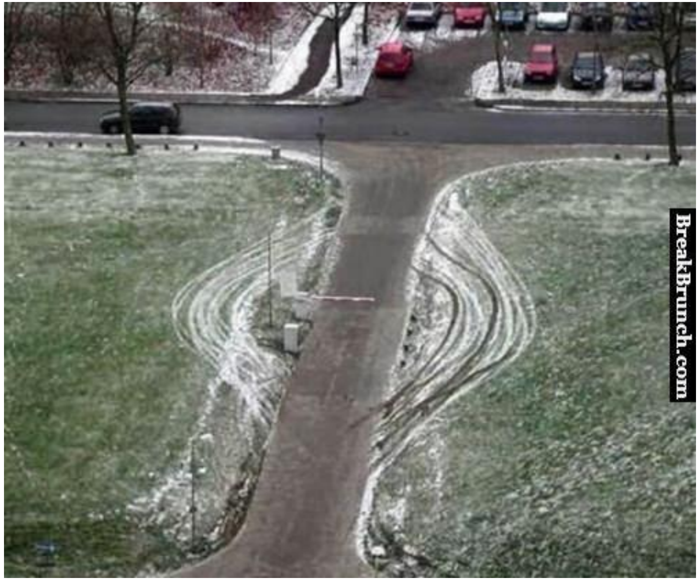
James Cook Dec. 16, 2014, 2:19 PM

# Usability – the dual of security?

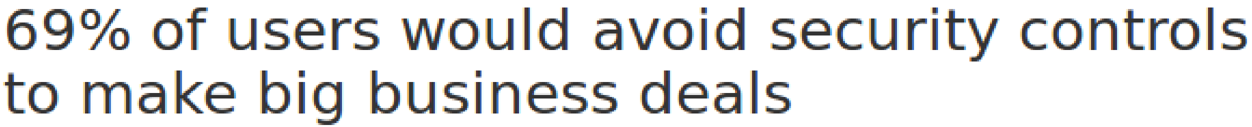

To complete the log-in procedure, stare directly at the sun.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-16-07



# If we make security too easy to bypass



# Who wins – security or business?



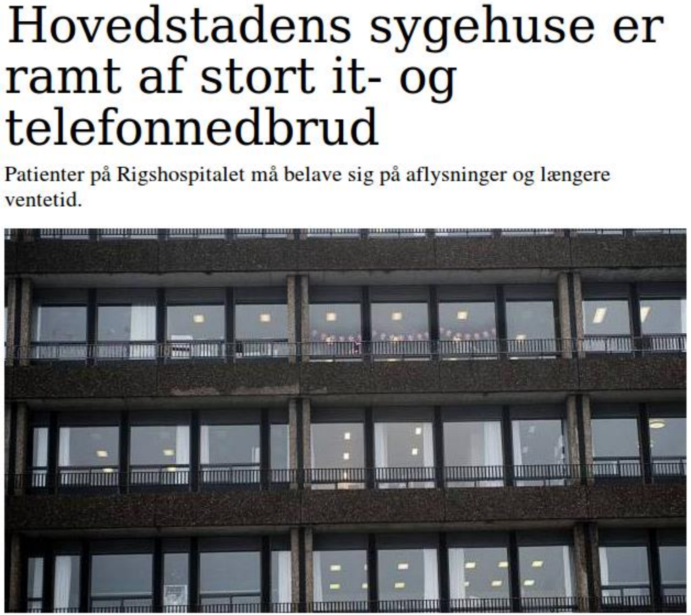
> 69% of users would avoid security controls to make big business deals

# BUT security *is* important

**Security News This Week: How Shipping Giant Maersk Dealt With a Malware Meltdown**

# What does IT-security mean to *you*?

# Is this security?



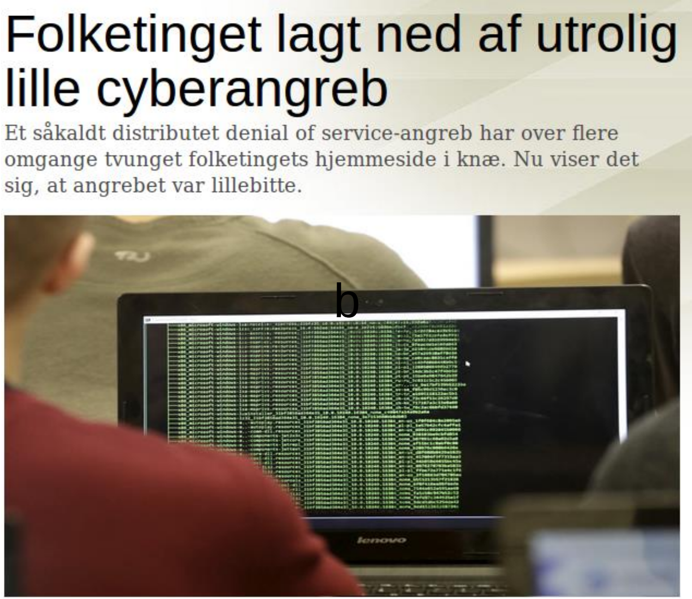
## Hovedstadens sygehuse er ramt af stort it- og telefonnedbrud

Patienter på Rigshospitalet må belave sig på aflysninger og længere ventetid.

# Is this security?

Massive Flooding Damages Several NYC Data Centers

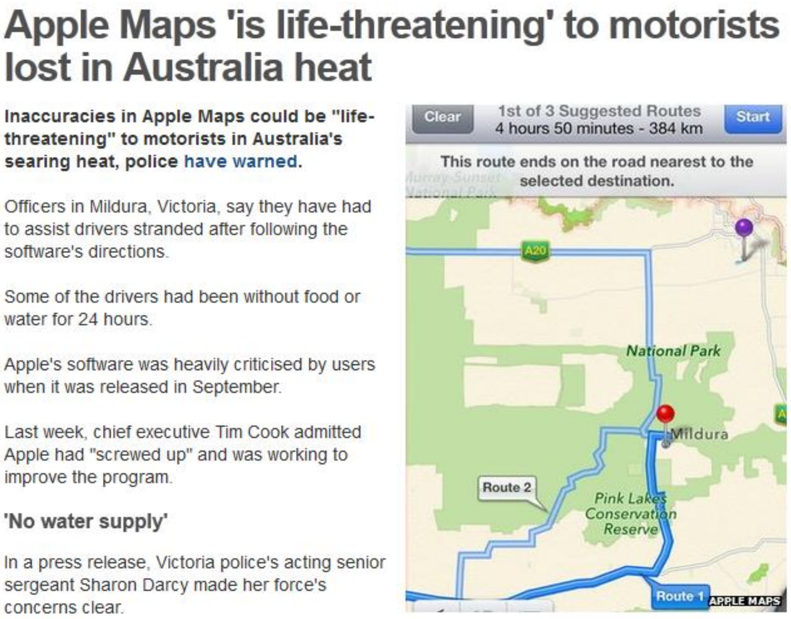
# Is this security?



Folketinget lagt ned af utrolig lille cyberangreb

Et såkaldt distributet denial of service-angreb har over flere omgange tvunget folketingets hjemmeside i knæ. Nu viser det sig, at angrebet var lillebitte.

# Is this security?



## Apple Maps 'is life-threatening' to motorists lost in Australia heat

**Inaccuracies in Apple Maps could be "life-threatening" to motorists in Australia's searing heat, police have warned.**

Officers in Mildura, Victoria, say they have had to assist drivers stranded after following the software's directions.

Some of the drivers had been without food or water for 24 hours.

Apple's software was heavily criticised by users when it was released in September.

Last week, chief executive Tim Cook admitted Apple had "screwed up" and was working to improve the program.

### 'No water supply'

In a press release, Victoria police's acting senior sergeant Sharon Darcy made her force's concerns clear.

1st of 3 Suggested Routes
4 hours 50 minutes - 384 km

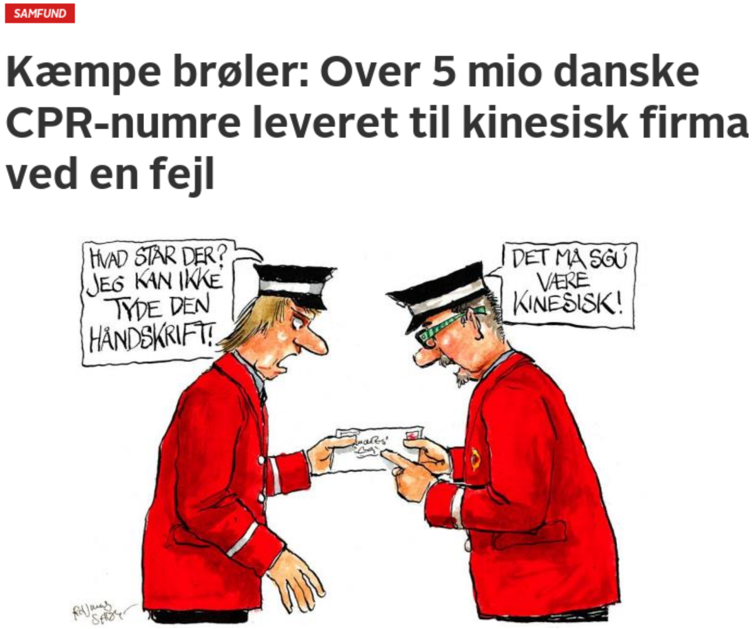
This route ends on the road nearest to the selected destination.

# Is this security?

**Texas students hijack superyacht with GPS-spoofing luggage**

Don't panic, yet

# Is this security?



SAMFUND

Kæmpe brøler: Over 5 mio danske CPR-numre leveret til kinesisk firma ved en fejl

HVAD STÅR DER? JEG KAN IKKE TYDE DEN HÅNDSKRIFT!
DET MÅ SGÚ VÆRE KINESISK!

# Is this security?

Sony Breach Exposed Employee Healthcare Data, Salaries

# Security defined

So, computers fail for many reasons

**Reliability** deals with accidental fails

**Usability** deals with problems arising from operating mistakes made by users

**Security** deals with intentional failures made by malicious parties

Security is about computing in the presence of an adversary

# A flat tire analogy

# Key questions in security

What is important to me?

- My web site, my research data, my production, my pictures, my ...

Who / what threatens this?

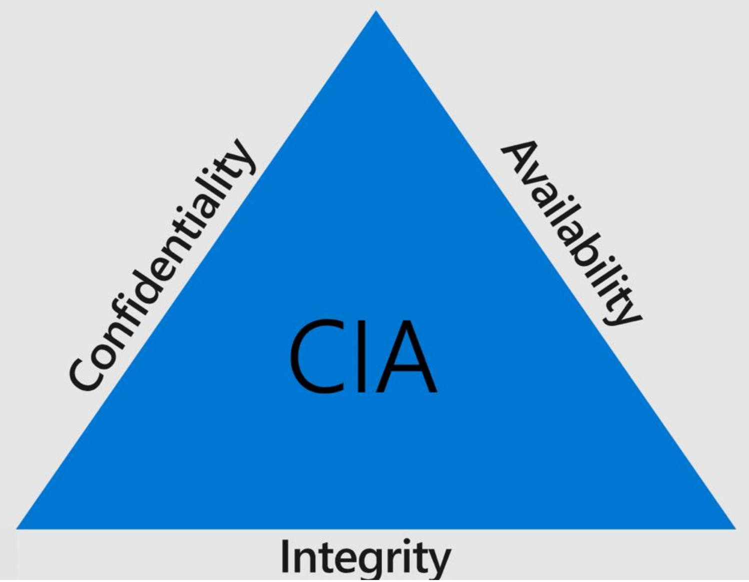
- And what are their motivations and capabilities?

Am I secure enough?

- How do you know?

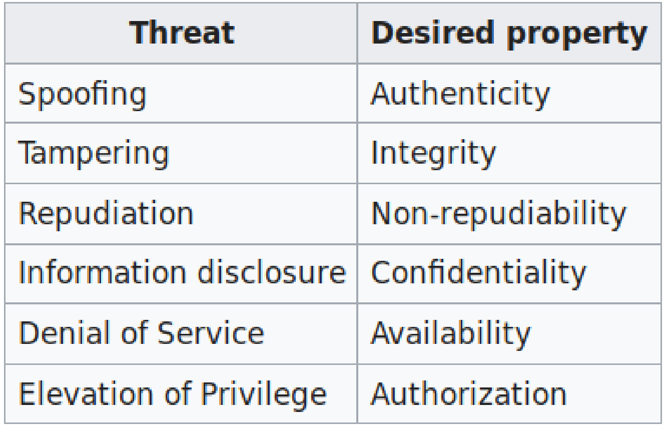
Plan, do, check, act. Repeat.

# Security goals – or CIA



# Security goals and their threats

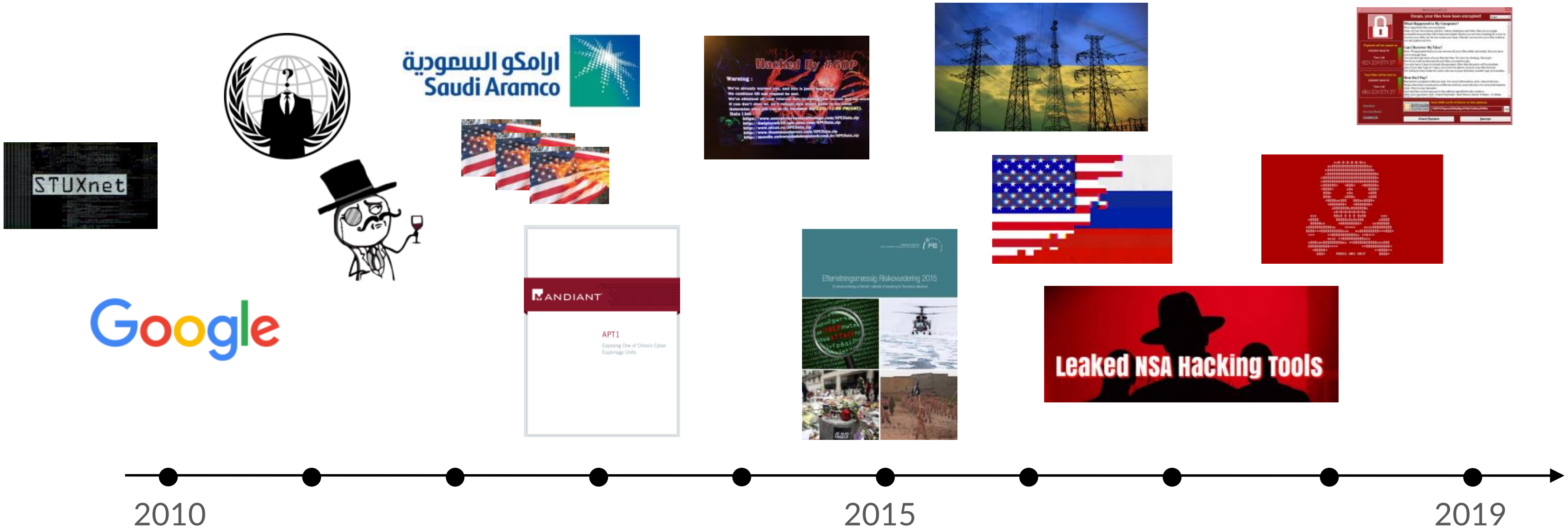
The STRIDE threat model helps to answer, "what can go wrong in this system we're working on?"



| Threat | Desired property |
|---|---|
| Spoofing | Authenticity |
| Tampering | Integrity |
| Repudiation | Non-repudiability |
| Information disclosure | Confidentiality |
| Denial of Service | Availability |
| Elevation of Privilege | Authorization |

# Who hacks?

# Hacks, or notable events, of the decade

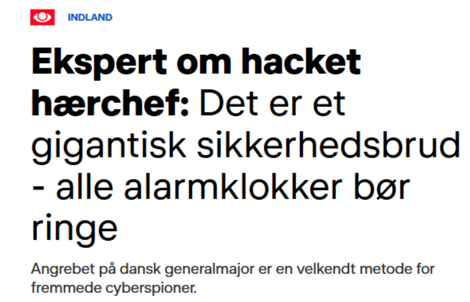


# 2020-2024

# CFCS: the ‘cyber threat’ is very high

**Cybertruslen 2023** →

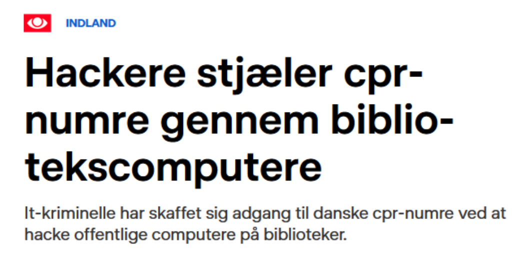
Cybertruslen mod Danmark 2023



INDLAND

**Ekspert om hacket hærchef:** Det er et gigantisk sikkerhedsbrud - alle alarmklokker bør ringe

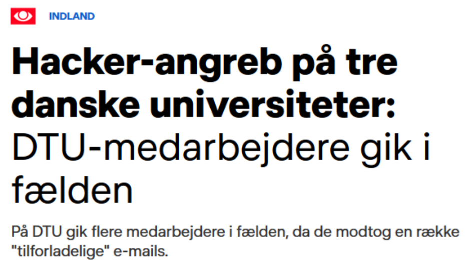
Angrebet på dansk generalmajor er en velkendt metode for fremmede cyberspioner.



INDLAND

**Hackere stjæler cpr-numre gennem biblio-tekscomputere**

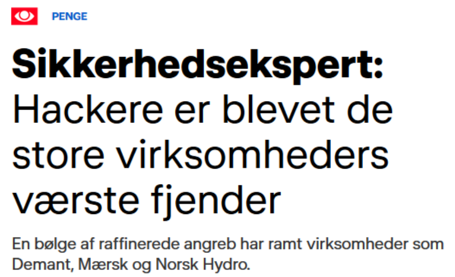
It-kriminelle har skaffet sig adgang til danske cpr-numre ved at hacke offentlige computere på biblioteker.



INDLAND

**Hacker-angreb på tre danske universiteter:** DTU-medarbejdere gik i fælden

På DTU gik flere medarbejdere i fælden, da de modtog en række "tilforladelige" e-mails.



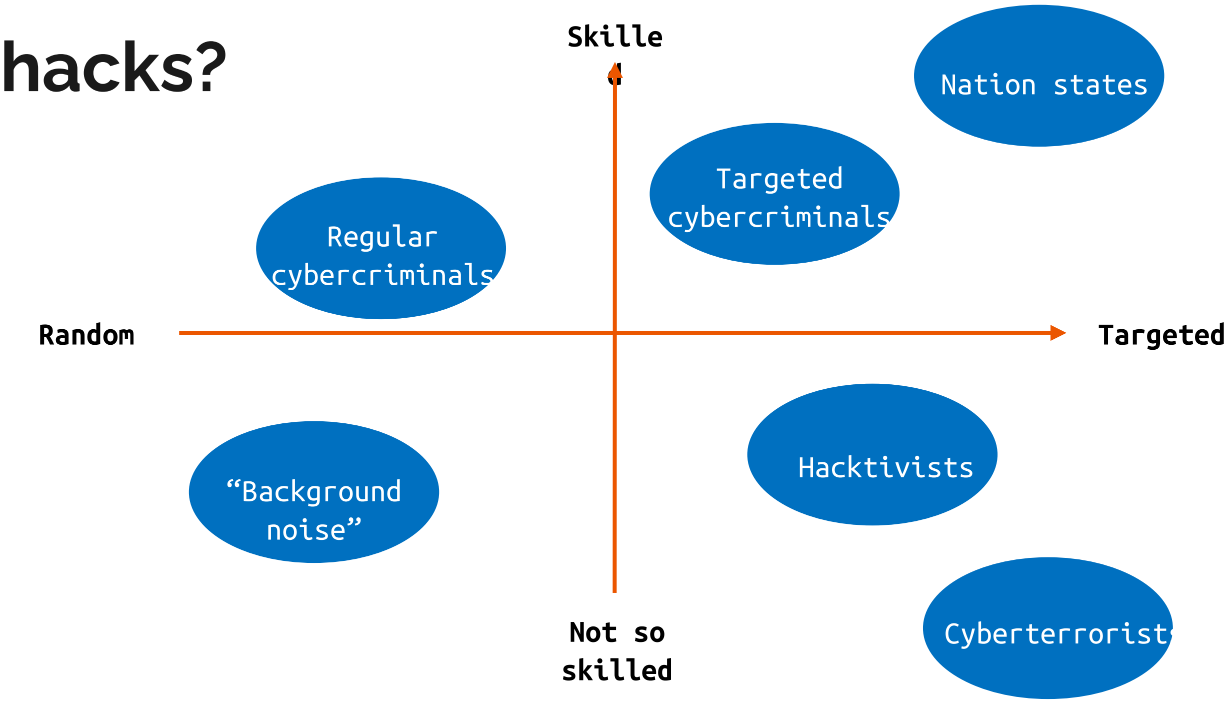
PENGE

**Sikkerhedsekspert:** Hackere er blevet de store virksomheders værste fjender

En bølge af raffinerede angreb har ramt virksomheder som Demant, Mærsk og Norsk Hydro.

https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger

# Who hacks?



Skille
Nation states
Targeted cybercriminals
Regular cybercriminals
Random
Targeted
Hacktivists
“Background noise”
Cyberterrorist
Not so skilled

# Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

Espionage

Cyber crime

# Cyber war?

“Actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”

- Richard A. Clarke, tidl. White House Special Advisor

# Estonia, 2007

# Iran, 2009/10

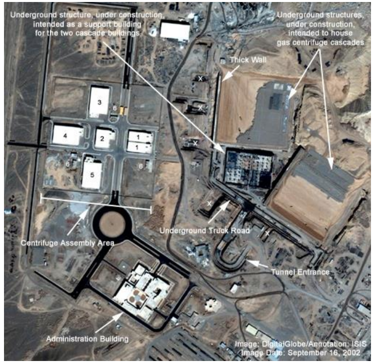
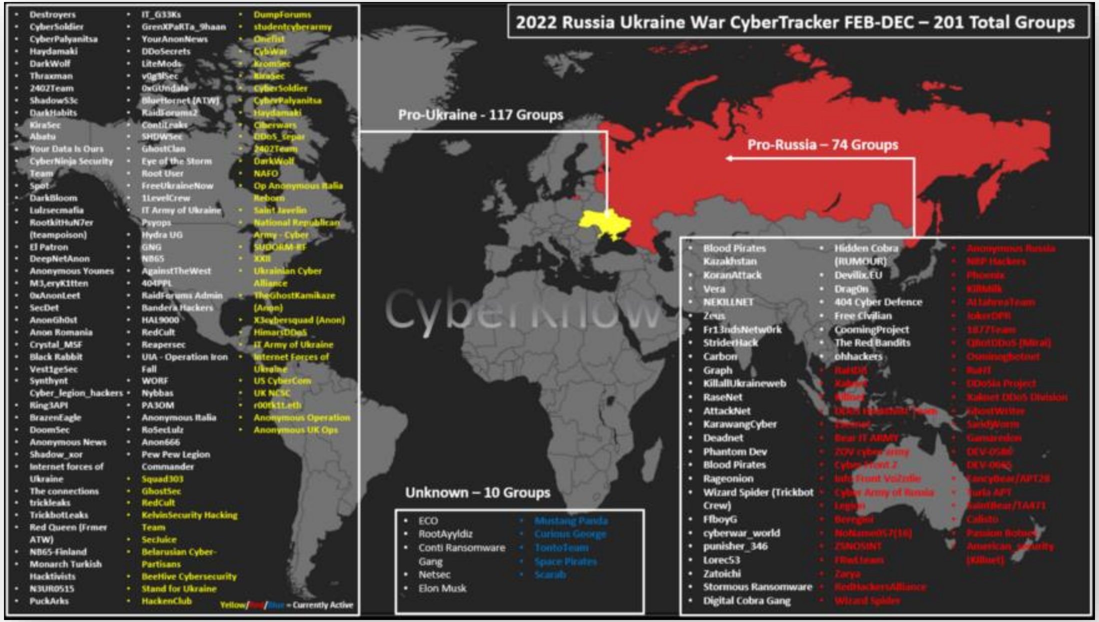

Underground structure, under construction, intended as a support building for the two cascade buildings
Underground structures, under construction, intended to house gas centrifuge cascades
Thick Wall
3
6
4
2
1
1
6
5
6
X
X
X
X
X
Underground Truck Road
Centrifuge Assembly Area
Tunnel Entrance
Administration Building

Image: DigitalGlobe/Annotation: ISIS
Image Date: September 16, 2002

# Palestine, 2019

# Ukraine, 2022+



2022 Russia Ukraine War CyberTracker FEB-DEC – 201 Total Groups

Pro-Ukraine - 117 Groups

- Destroyers
- CyberSoldier
- CyberPalyanitsa
- Haydamaki
- DarkWolf
- Thraxman
- 2402Team
- ShadowS3c
- DarkHabits
- KiraSec
- Abatu
- Your Data Is Ours
- CyberNinja Security Team
- Spot
- DarkBloom
- Lulzsecmafia
- RootkitHuN7er (teampoison)
- El Patron
- DeepNetAnon
- Anonymous Younes
- M3,eryK1tten
- 0xAnonLeet
- SecDet
- AnonGh0st
- Anon Romania
- Crystal_MSF
- Black Rabbit
- Vest1geSec
- Synthynt
- Cyber_legion_hackers
- Ring3API
- BrazenEagle
- DoomSec
- Anonymous News
- Shadow_xor
- Internet forces of Ukraine
- The connections
- trickleaks
- TrickbotLeaks
- Red Queen (Frmer ATW)
- NB65-Finland
- Monarch Turkish Hacktivists
- N3UR0515
- PuckArks
- IT_G33Ks
- GrenXPaRTa_9haan
- YourAnonNews
- DDoSecrets
- LiteMods
- v0g3lSec
- 0xGUndala
- BlueHornet (ATW)
- RaidForums2
- ContiLeaks
- SHDWSec
- GhostClan
- Eye of the Storm
- Root User
- FreeUkraineNow
- 1LevelCrew
- IT Army of Ukraine
- Psyops
- Hydra UG
- GNG
- NB65
- AgainstTheWest
- 404PPL
- RaidForums Admin
- Bandera Hackers
- HAL9000
- RedCult
- Reapersec
- UIA - Operation Iron Fall
- WORF
- Nybbas
- PA3OM
- Anonymous Italia
- RoSecLulz
- Anon666
- Pew Pew Legion Commander
- Squad303
- GhostSec
- RedCult
- KelvinSecurity Hacking Team
- SecJuice
- Belarusian Cyber-Partisans
- BeeHive Cybersecurity
- Stand for Ukraine
- HackenClub
- DumpForums
- studentcyberarmy
- Onefist
- CybWar
- KromSec
- KiraSec
- CyberSoldier
- CyberPalyanitsa
- Haydamaki
- Ciberwars
- DDoS_Separ
- 2402Team
- DarkWolf
- NAFO
- Op Anonymous Italia Reborn
- Saint Javelin
- National Republican Army - Cyber
- SUDORM-RF
- XXII
- Ukrainian Cyber Alliance
- TheGhostKamikaze (Anon)
- X3cybersquad (Anon)
- HimarsDDoS
- IT Army of Ukraine
- Internet Forces of Ukraine
- US CyberCom
- UK NCSC
- r00tk1t.eth
- Anonymous Operation
- Anonymous UK Ops

Yellow/Red/Blue = Currently Active

Pro-Russia – 74 Groups

- Blood Pirates Kazakhstan
- KoranAttack
- Vera
- NEKILLNET
- Zeus
- Fr13ndsNetw0rk
- StriderHack
- Carbon
- Graph
- KillallUkraineweb
- RaseNet
- AttackNet
- KarawangCyber
- Deadnet
- Phantom Dev
- Blood Pirates
- Rageonion
- Wizard Spider (Trickbot Crew)
- FfboyG
- cyberwar_world
- punisher_346
- Lorec53
- Zatoichi
- Stormous Ransomware
- Digital Cobra Gang
- Hidden Cobra (RUMOUR)
- Devilix.EU
- Drag0n
- 404 Cyber Defence
- Free Civilian
- CoomingProject
- The Red Bandits
- ohhackers
- RaHDit
- Xaknet
- Killnet
- DDoS Hacktivist Team
- [illegible]
- Bear IT ARMY
- Z0V cyber army
- Cyber Front Z
- Info Front VoZnDe
- Cyber Army of Russia
- Legion
- Beregini
- NoName057(16)
- ZSNOSINT
- FRwLteam
- Zarya
- RedHackersAlliance
- Wizard Spider
- Anonymous Russia
- NBP Hackers
- Phoenix
- KillMilk
- Al TahreaTeam
- JokerDPR
- 1877Team
- QbotDDoS (Mirai)
- Dumnogbotnet
- Ru44
- DDoSia Project
- Xaknet DDoS Division
- GhostWriter
- SandWorm
- Gamaredon
- DEV-0586
- DEV-0665
- FancyBear/APT28
- Turla APT
- SaintBear/TA471
- Callisto
- Passion Botnet
- American_security (Killnet)

Unknown – 10 Groups

- ECO
- RootAyyldiz
- Conti Ransomware Gang
- Netsec
- Elon Musk
- Mustang Panda
- Curious George
- TontoTeam
- Space Pirates
- Scarab

# Who hacks? Or, threats in cyber space

Cyber war

**Cyber terror**

Hacktivists

Espionage

Cyber crime

# Cyber terror

UN: any act “intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act.”

e

# Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

**Hacktivists**

Espionage

Cyber crime

# Hacktivists

# Hacktivists false flag operations

Guccifer 2.0 – the attack on Hillary Clinton’s campaign in 2016

Guardians of Peace – the attack on Sony in 2014

Cutting Sword of Justice – the attack on Saudi Aramco in 2012

# Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

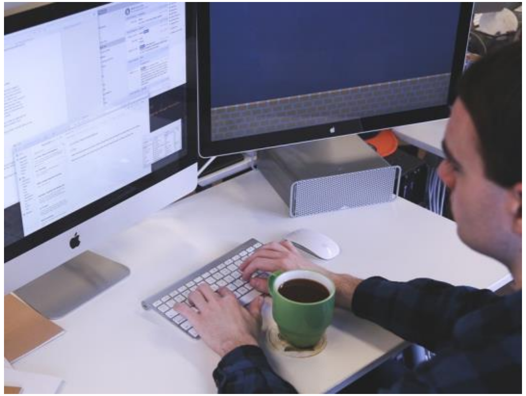
**Espionage**

Cyber crime

# Espionage

Classic

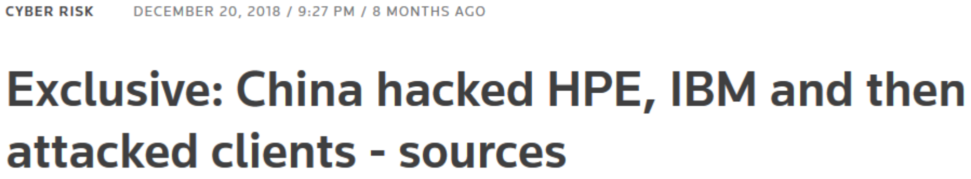
Modern



# Espionage

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
GCHQ
FE
СЛУЖБА
وزارت اطلاعات
جمهوری اسلامی ایران

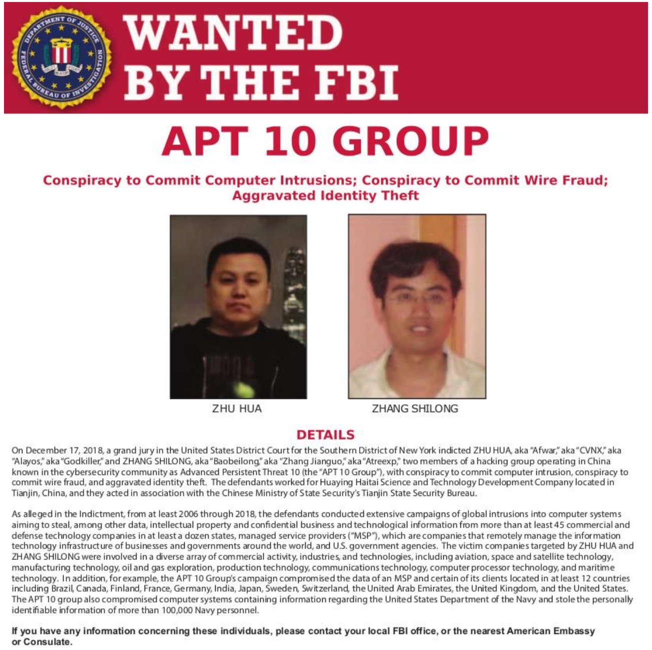
# APT10 / STONE PANDA / POTASSIUM / RED APOLLO



CYBER RISK DECEMBER 20, 2018 / 9:27 PM / 8 MONTHS AGO

## Exclusive: China hacked HPE, IBM and then attacked clients - sources

# FBI’s most wanted - APT10



WANTED BY THE FBI

## APT 10 GROUP

**Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft**

ZHU HUA

ZHANG SHILONG

### DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka “Afwar,” aka “CVNX,” aka “Alayos,” aka “Godkiller,” and ZHANG SHILONG, aka “Baobeilong,” aka “Zhang Jianguo,” aka “Atreexp,” two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the “APT 10 Group”), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security’s Tianjin State Security Bureau.

As alleged in the Indictment, from at least 2006 through 2018, the defendants conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least 45 commercial and defense technology companies in at least a dozen states, managed service providers (“MSP”), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The victim companies targeted by ZHU HUA and ZHANG SHILONG were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology, and maritime technology. In addition, for example, the APT 10 Group’s campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.

**If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.**

# Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

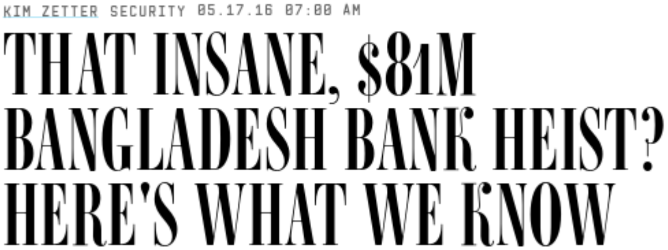
Hacktivists

Espionage

**Cyber crime**

# Cyber crime

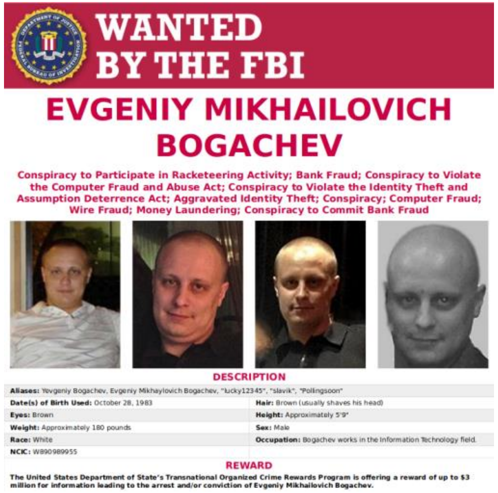
Very targeted



KIM ZETTER SECURITY 05.17.16 07:00 AM

THAT INSANE, $81M BANGLADESH BANK HEIST? HERE'S WHAT WE KNOW

Not so targeted



WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

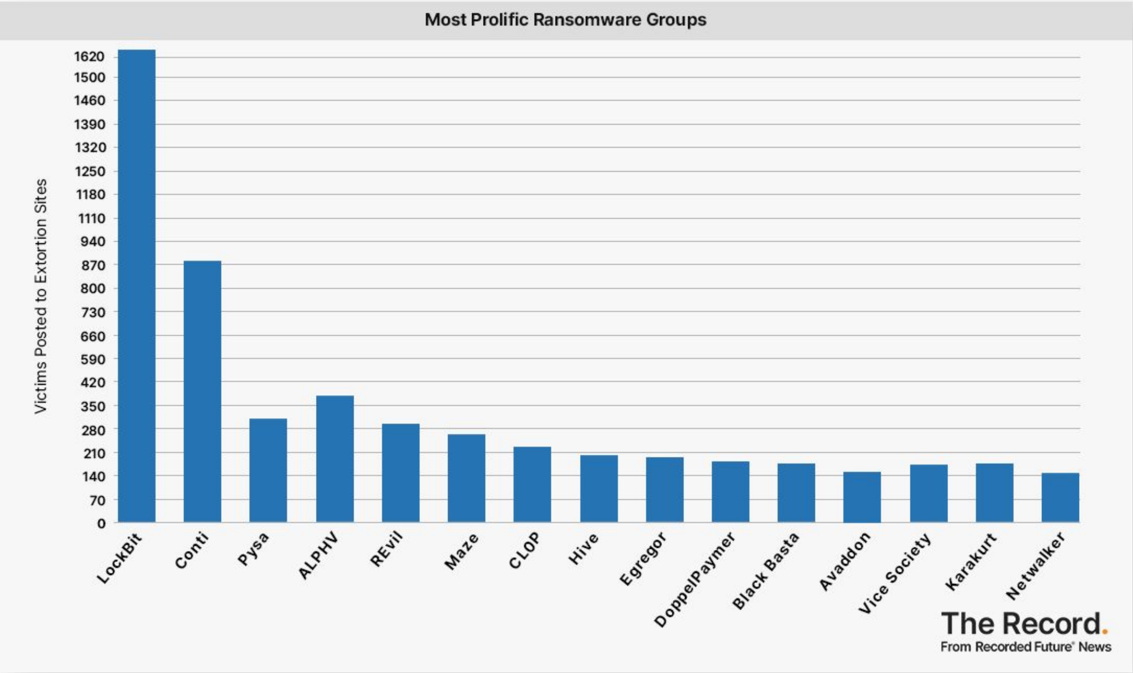
DESCRIPTION

| | |
|---|---|
| **Aliases:** Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon" | |
| **Date(s) of Birth Used:** October 28, 1983 | **Hair:** Brown (usually shaves his head) |
| **Eyes:** Brown | **Height:** Approximately 5'9" |
| **Weight:** Approximately 180 pounds | **Sex:** Male |
| **Race:** White | **Occupation:** Bogachev works in the Information Technology field. |
| **NCIC:** W890989955 | |

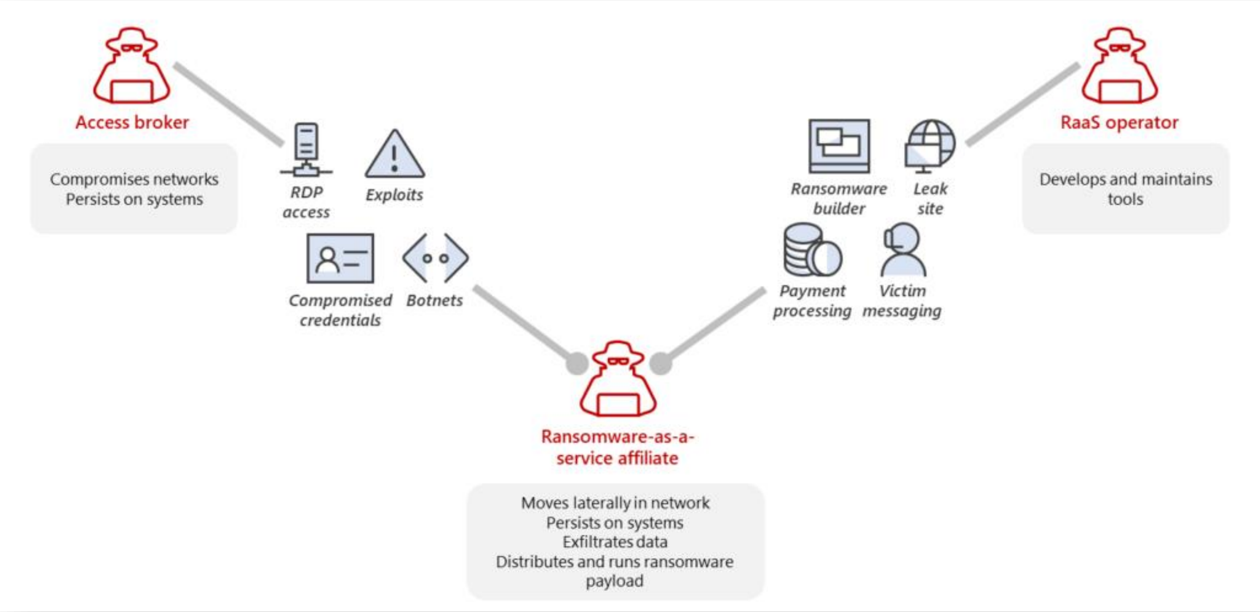
REWARD

**The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.**

# Ransomware


Most Prolific Ransomware Groups
Victims Posted to Extortion Sites
1620
1500
1460
1390
1320
1250
1180
1110
940
870
800
730
660
590
420
350
280
210
140
70
0
LockBit
Conti
Pysa
ALPHV
REvil
Maze
CLOP
Hive
Egregor
DoppelPaymer
Black Basta
Avaddon
Vice Society
Karakurt
Netwalker
The Record.
From Recorded Future® News

# Ransomware


Access broker
Compromises networks
Persists on systems
RDP access
Exploits
Compromised credentials
Botnets
Ransomware builder
Leak site
Payment processing
Victim messaging
RaaS operator
Develops and maintains tools
Ransomware-as-a-service affiliate
Moves laterally in network
Persists on systems
Exfiltrates data
Distributes and runs ransomware payload

# Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

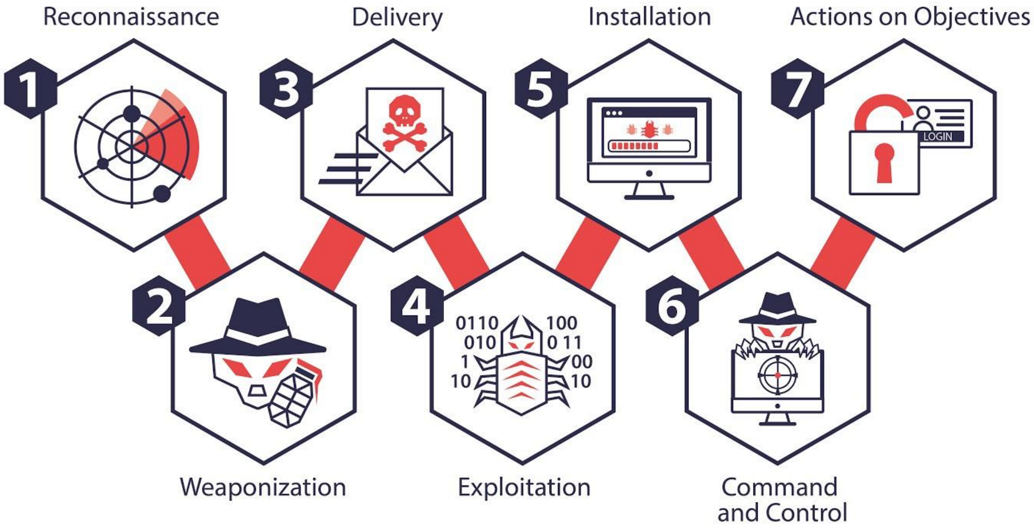
Hacktivists

Espionage

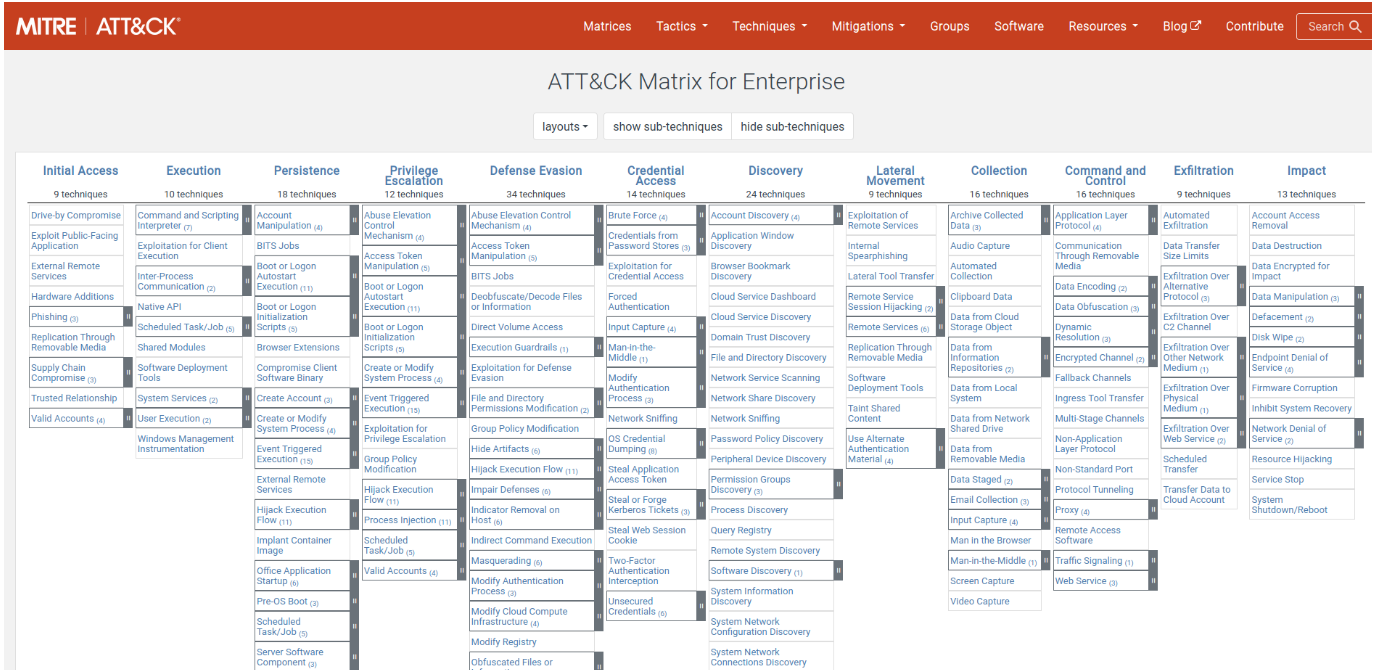
Cyber crime

# How hackers hack

# The Cyber Kill Chain



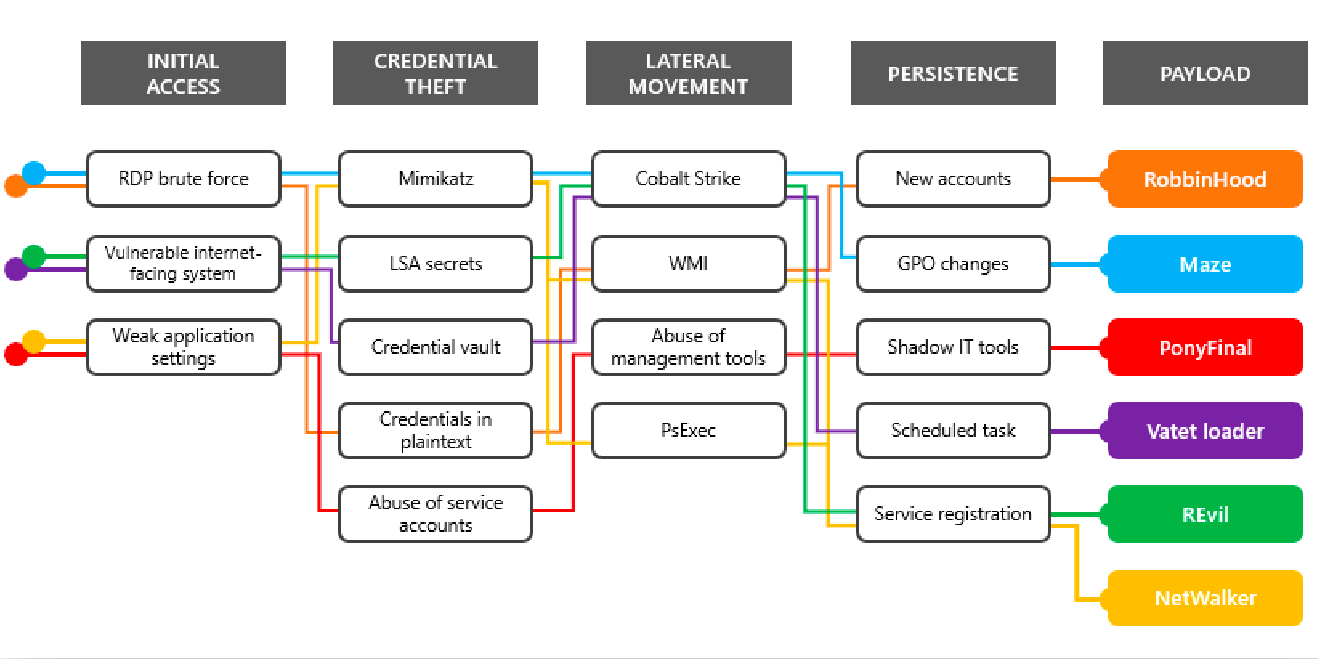
# MITRE ATT&CK



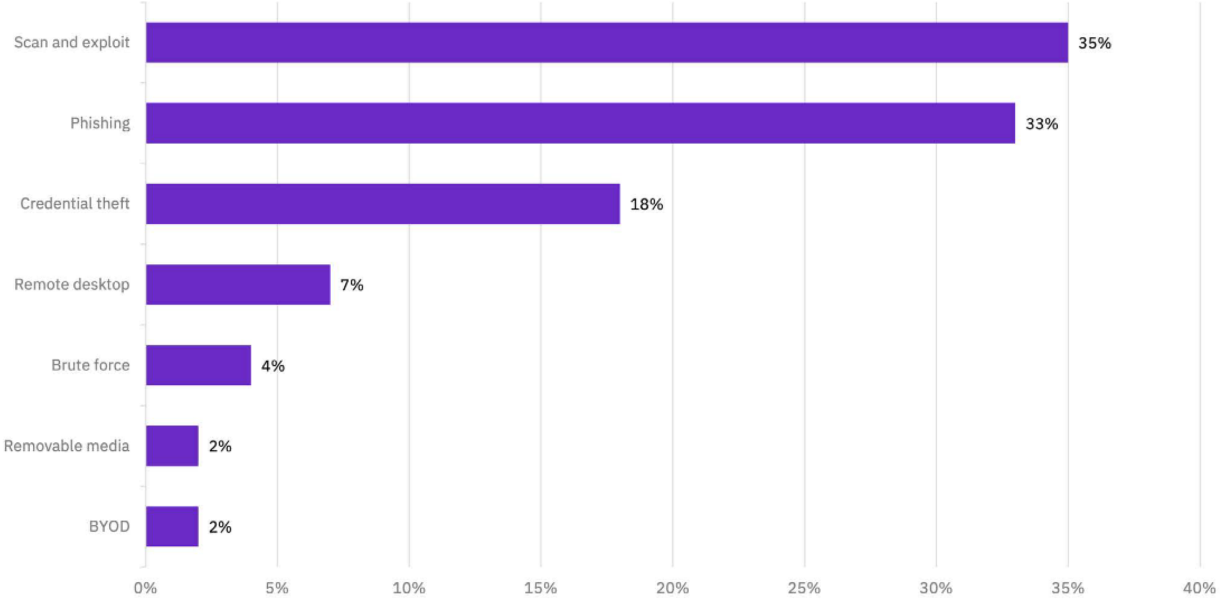
## ATT&CK Matrix for Enterprise

| Initial Access<br>9 techniques | Execution<br>10 techniques | Persistence<br>18 techniques | Privilege Escalation<br>12 techniques | Defense Evasion<br>34 techniques | Credential Access<br>14 techniques | Discovery<br>24 techniques | Lateral Movement<br>9 techniques | Collection<br>16 techniques | Command and Control<br>16 techniques | Exfiltration<br>9 techniques | Impact<br>13 techniques |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | Command and Scripting Interpreter (7) | Account Manipulation (4) | 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 | Data Encoding (2) | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact |
| Hardware Additions | Native API | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Deobfuscate/Decode Files or Information | Forced Authentication | Cloud Service Dashboard | Remote Service Session Hijacking (2) | Clipboard Data | Data Obfuscation (3) | Exfiltration Over C2 Channel | Data Manipulation (3) |
| Phishing (3) | Scheduled Task/Job (5) | Browser Extensions | Create or Modify System Process (4) | Direct Volume Access | Input Capture (4) | Cloud Service Discovery | Remote Services (6) | Data from Cloud Storage Object | Dynamic Resolution (3) | Exfiltration Over Other Network Medium (1) | Defacement (2) |
| Replication Through Removable Media | Shared Modules | Compromise Client Software Binary | Event Triggered Execution (15) | Execution Guardrails (1) | Man-in-the-Middle (1) | Domain Trust Discovery | Replication Through Removable Media | Data from Information Repositories (2) | Encrypted Channel (2) | Exfiltration Over Physical Medium (1) | Disk Wipe (2) |
| Supply Chain Compromise (3) | Software Deployment Tools | Create Account (3) | Exploitation for Privilege Escalation | Exploitation for Defense Evasion | Modify Authentication Process (3) | File and Directory Discovery | Software Deployment Tools | Data from Local System | Fallback Channels | Exfiltration Over Web Service (2) | Endpoint Denial of Service (4) |
| Trusted Relationship | System Services (2) | Create or Modify System Process (4) | Group Policy Modification | File and Directory Permissions Modification (2) | Network Sniffing | Network Service Scanning | Taint Shared Content | Data from Network Shared Drive | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Valid Accounts (4) | User Execution (2) | Event Triggered Execution (15) | Hijack Execution Flow (11) | Group Policy Modification | OS Credential Dumping (8) | Network Share Discovery | Use Alternate Authentication Material (4) | Data from Removable Media | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| | Windows Management Instrumentation | External Remote Services | Process Injection (11) | Hide Artifacts (6) | Steal Application Access Token | Network Sniffing | | Data Staged (2) | Non-Application Layer Protocol | | Network Denial of Service (2) |
| | | Hijack Execution Flow (11) | Scheduled Task/Job (5) | Hijack Execution Flow (11) | Steal or Forge Kerberos Tickets (3) | Password Policy Discovery | | Email Collection (3) | Non-Standard Port | | Resource Hijacking |
| | | Implant Container Image | Valid Accounts (4) | Impair Defenses (6) | Steal Web Session Cookie | Peripheral Device Discovery | | Input Capture (4) | Protocol Tunneling | | Service Stop |
| | | Office Application Startup (6) | | Indicator Removal on Host (6) | Two-Factor Authentication Interception | Permission Groups Discovery (3) | | Man in the Browser | Proxy (4) | | System Shutdown/Reboot |
| | | Pre-OS Boot (3) | | Indirect Command Execution | Unsecured Credentials (6) | Process Discovery | | Man-in-the-Middle (1) | Remote Access Software | | |
| | | Scheduled Task/Job (5) | | Masquerading (6) | | Query Registry | | Screen Capture | Traffic Signaling (1) | | |
| | | Server Software Component (3) | | Modify Authentication Process (3) | | Remote System Discovery | | Video Capture | Web Service (3) | | |
| | | | | Modify Cloud Compute Infrastructure (4) | | Software Discovery (1) | | | | | |
| | | | | Modify Registry | | System Information Discovery | | | | | |
| | | | | Obfuscated Files or | | System Network Configuration Discovery | | | | | |
| | | | | | | System Network Connections Discovery | | | | | |

# MITRE ATT&CK in action



# Look at the numbers (initial access)



https://www.ibm.com/security/data-breach/threat-intelligence

# Try it yourself

KALI
BY OFFENSIVE SECURITY

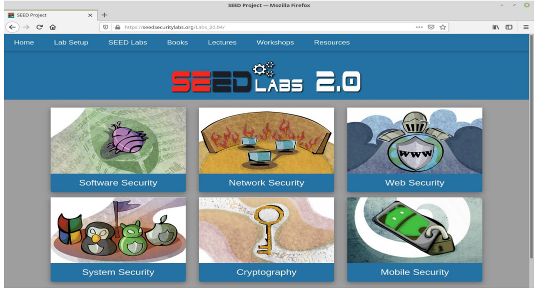
metasploit®

```
                  To boldly go where no
                   shell has gone before


       =[ metasploit v4.17.3-dev                         ]
+ -- --=[ 1795 exploits - 1019 auxiliary - 310 post      ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

SEED LABS



# What to do?

Study the body of knowledge

Study how breaches occur

Implement the right security controls for your situation

That matches the likelihood and consequences of the threats that you face

## And most importantly:

## Keep coming to class! ;)

# Lecture plan

| Week | Date | Topic |
| ---- | ---- | ----- |
| 36 | 02 Sep | Security concepts and principles |
| | 06 Sep | Cryptographic building blocks |
| 37 | 09 Sep | Key establishment and certificate management |
| | 13 Sep | User authentication, IAM |
| 38 | 16 Sep | Operating systems security, web, browser and mail security |
| | 20 Sep | IT security management and risk assessment |
| 39 | 23 Sep | Software security - exploits and privilege escalation |
| | 27 Sep | Malicious software |
| 40 | 30 Oct | Firewalls and tunnels, security architecture |
| | 04 Oct | Cloud and IoT security |
| 41 | 07 Oct | Intrusion detection and network attacks |
| | 11 Oct | Forensics |
| 42 | | Fall Vacation - No lectures |
| 43 | 21 Oct | Privacy and GDPR |
| | 25 Oct | Privacy engineering |
| 44 | 28 Oct | Final guest lecture and Exam Q/A |