



IT-Security (ITS) B1

DIKU, E2025



Today's agenda

Part 1.

Course overview & Security defined

Part 2.

Who hacks?

Security news

LATEST NEWS

NEWS

Sort by

Date desc ▼

Category



Alexander Martin

September 1st, 2025

Spanish government cancels €10m contract using Huawei equipment



James Reddick

August 29th, 2025

Scammer steals \$1.5 million from Baltimore by spoofing city vendor



Jonathan Greig

August 29th, 2025

Ransomware gang takedowns causing explosion of new, smaller groups



BRIEF Data breach at TransUnion impacts 4.4 million people

James Reddick

August 28th, 2025



Lectures

Lectures

Mondays and Fridays at 10-12 in AUD 01 AKB, Universitetsparken 13

Instructors

Boel Nelson (course organiser)

Troels Langkjær

Carsten Jørgensen



Lecture plan / topics

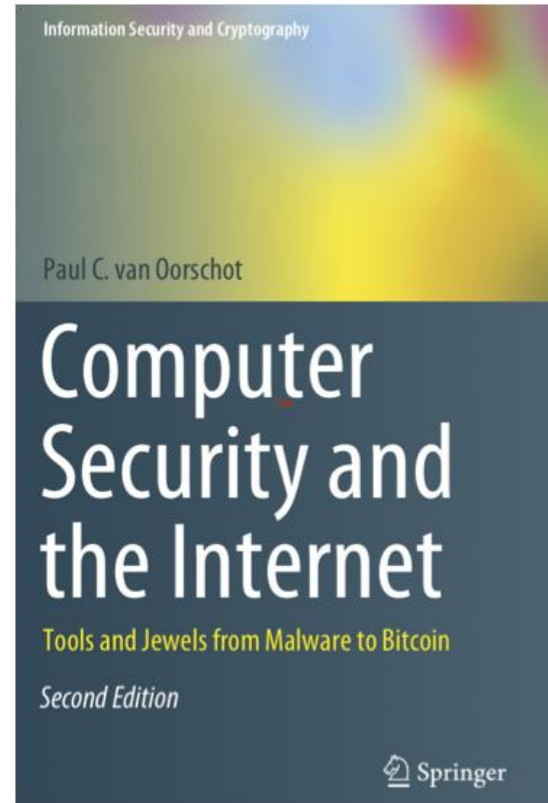
- | 36 | Security concepts and principles
- | | Cryptographic building blocks
- | 37 | Key establishment and certificate management
- | | User authentication, IAM
- | 38 | Operating systems security, web, browser and mail security
- | | IT security management and risk assessment
- | 39 | Software security - exploits and privilege escalation
- | | Malicious software
- | 40 | Firewalls and tunnels, security architecture
- | | Cloud and IoT security
- | 41 | Intrusion detection and network attacks
- | | Forensics
- | 42 | Fall Vacation - No lectures
- | 43 | Privacy and GDPR
- | | Privacy engineering
- | 44 | 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





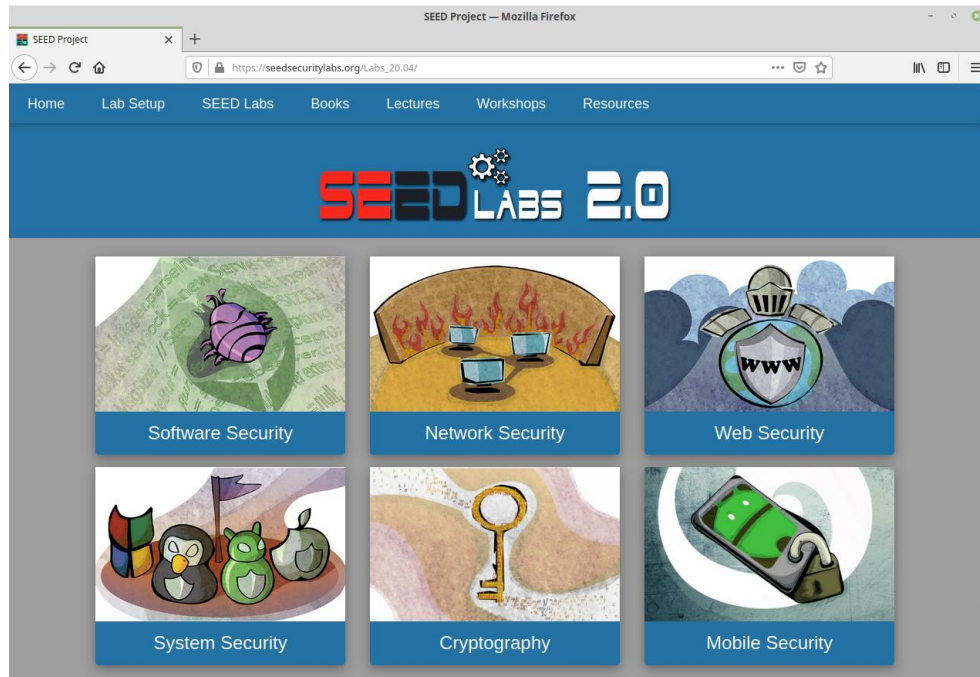
Assignments

There are 5 weekly assignments during the course.

36	No handin first week
37	Assignment 1 handin
38	Assignment 2 handin
39	Assignment 3 handin
40	Assignment 4 handin
41	Assignment 5 handin
42	Possible re-handin of one assignment (1-4)
43	No handin

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

SEED Labs





Exercise classes

Exercise classes

Tuesdays 13-17 in øv - bib 4-0-17, Universitetsparken 1-3, DIKU

TAs

Anders Friis Persson

Morten Lundorff



Exam

7 Nov 2025

4-hour written exam

All aids allowed except Internet

(Oral re-exam)



Course site

<https://github.com/diku-its/e2025>

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



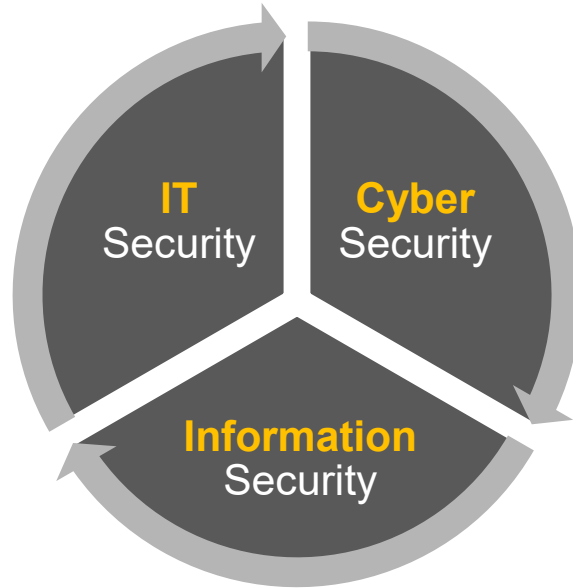
Fame, or infamous





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

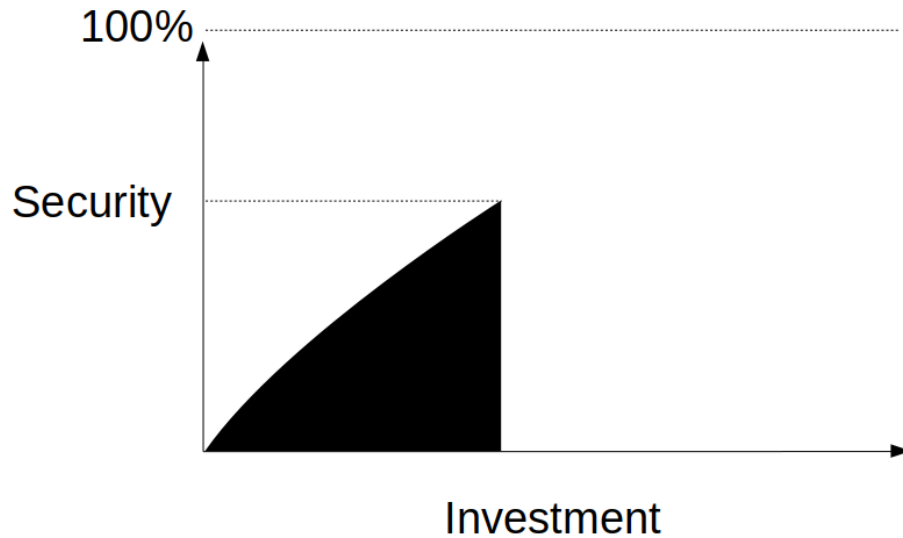
Threat models

Intrusion detection

Security management

And much more

100% security is an illusion





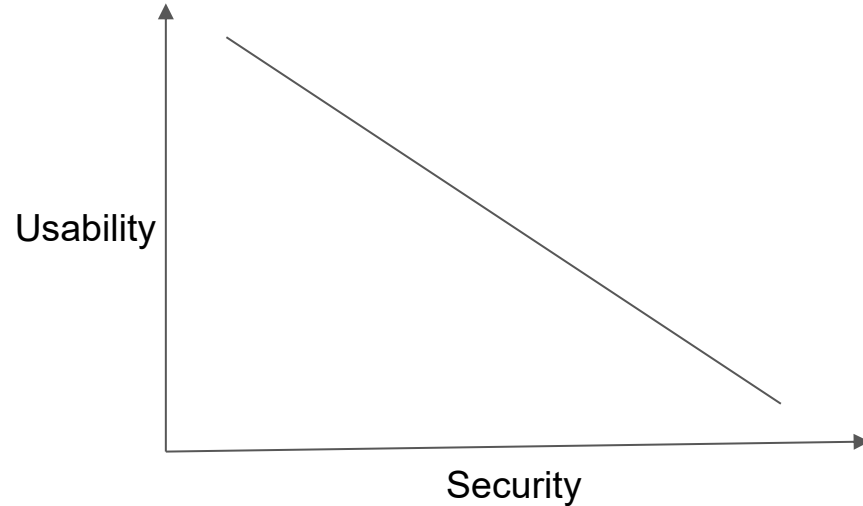
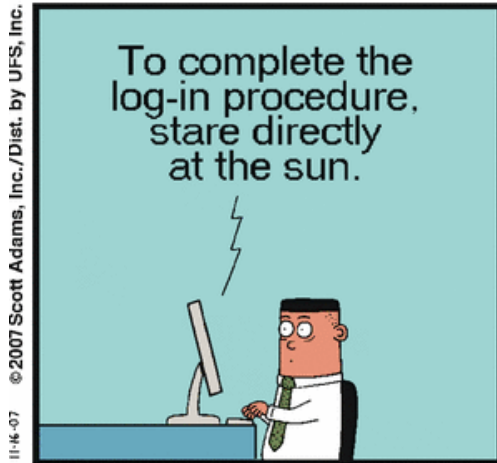
Even big-budget firms get hacked

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?



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?

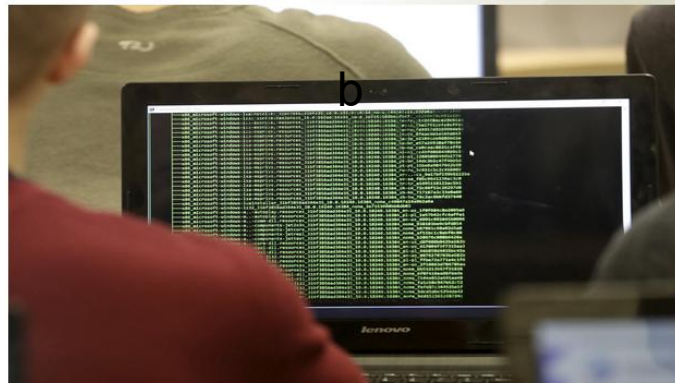
Massive Flooding Damages
Several NYC Data Centers



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.

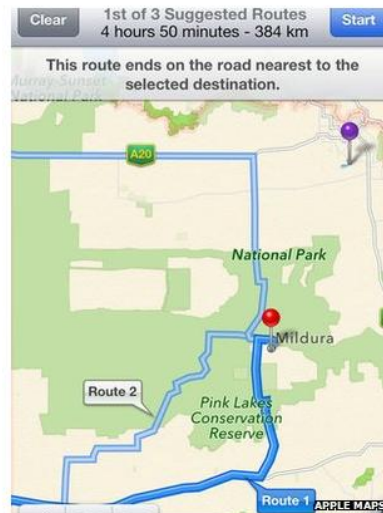
Some of the drivers had been without food or water for 24 hours.

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.



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**



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

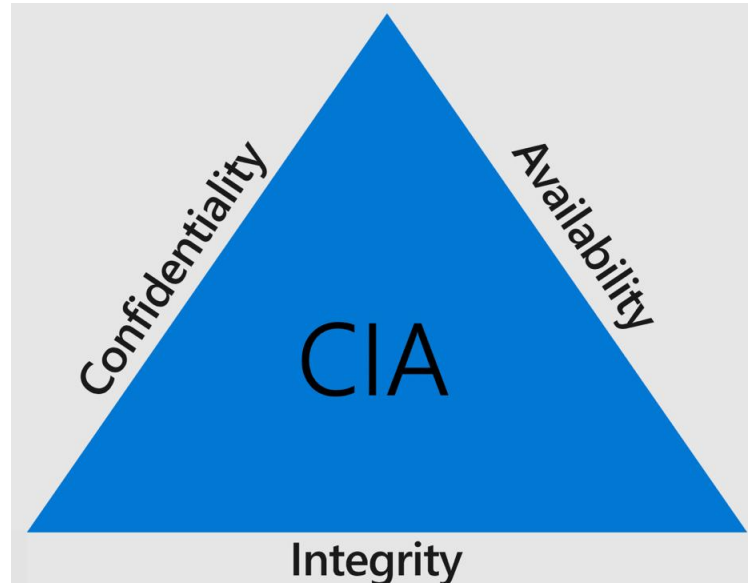


**Security is about computing in the presence of
an adversary**

A flat tire analogy



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



2020-2025



CFCS: the 'cyber threat' is very high



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

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



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.



Hackere stjæler cpr-numre gennem bibliotekscomputere

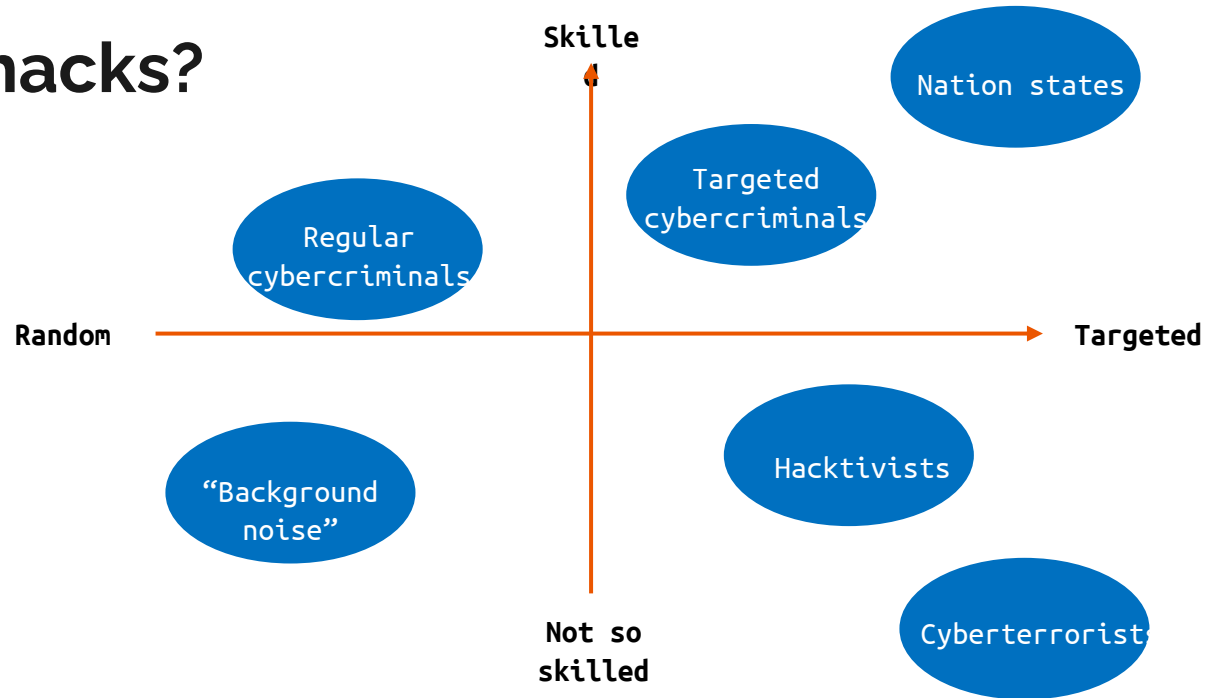
It-kriminelle har skaffet sig adgang til danske cpr-numre ved at hacke offentlige computere på biblioteker.



Sikkerhedsekspert: Hackere er blevet de store virksomheders værste fjender

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

Who hacks?





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.”

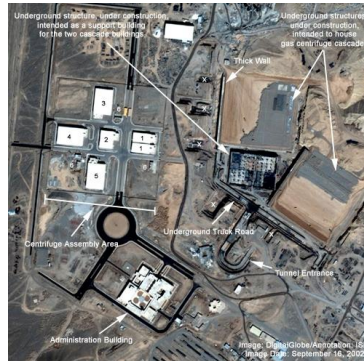
- Richard A. Clarke, tidl. White House Special Advisor



Estonia, 2007

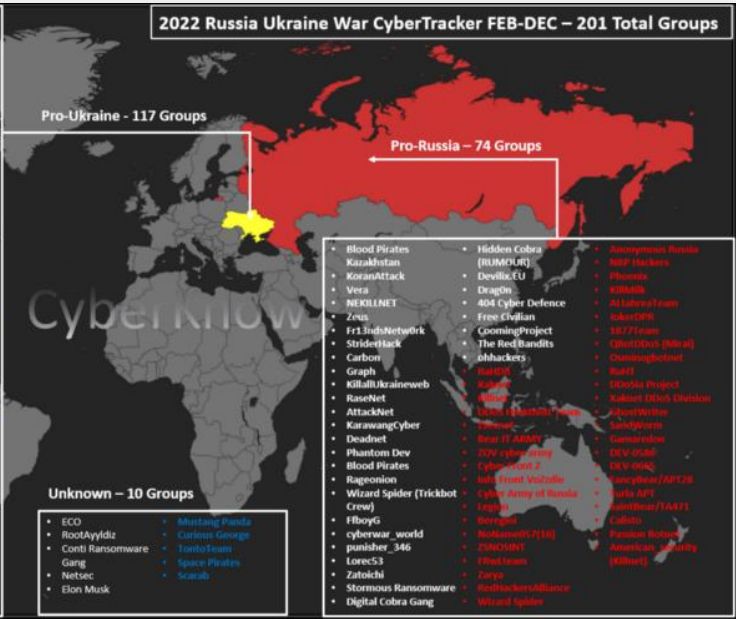


Iran, 2009/10



Palestine, 2019







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.”





Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hactivists

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



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**

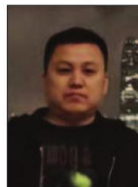


FBI's most wanted - APT10



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 "Baobellong" 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



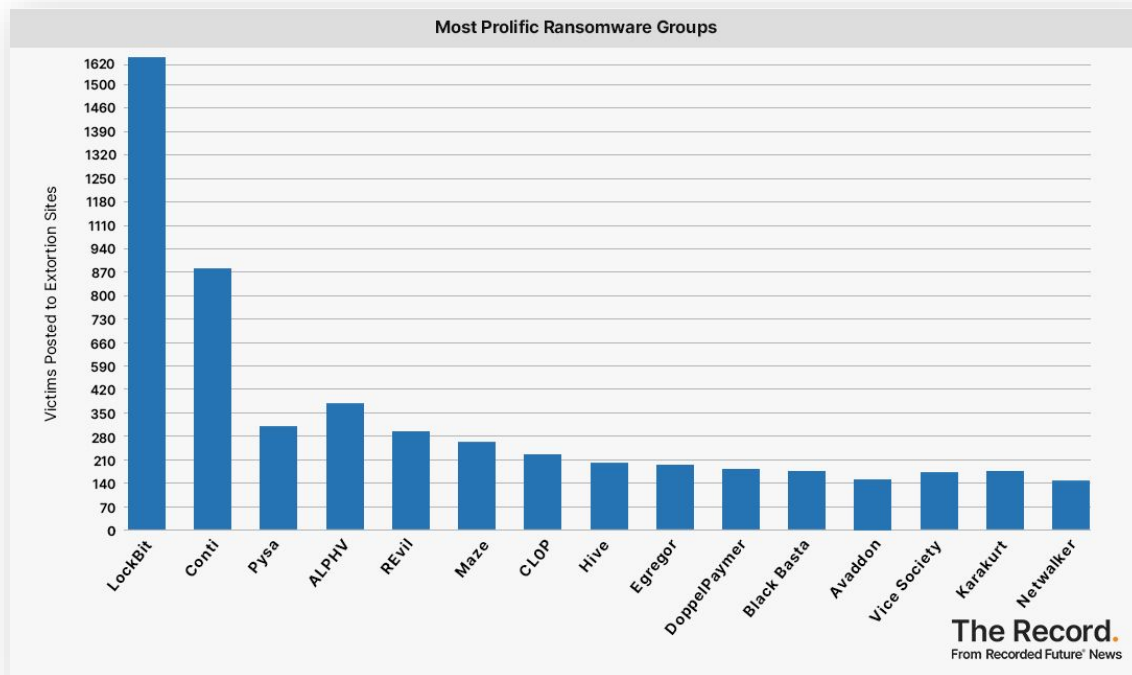
DESCRIPTION

Aliases: Evgeniy Bogachev, Evgeniy Mikhailovich Bogachev, "Lucky12345", "Slavik", "Pillington"	
Date(s) of Birth: 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.
NCK: W99098955	

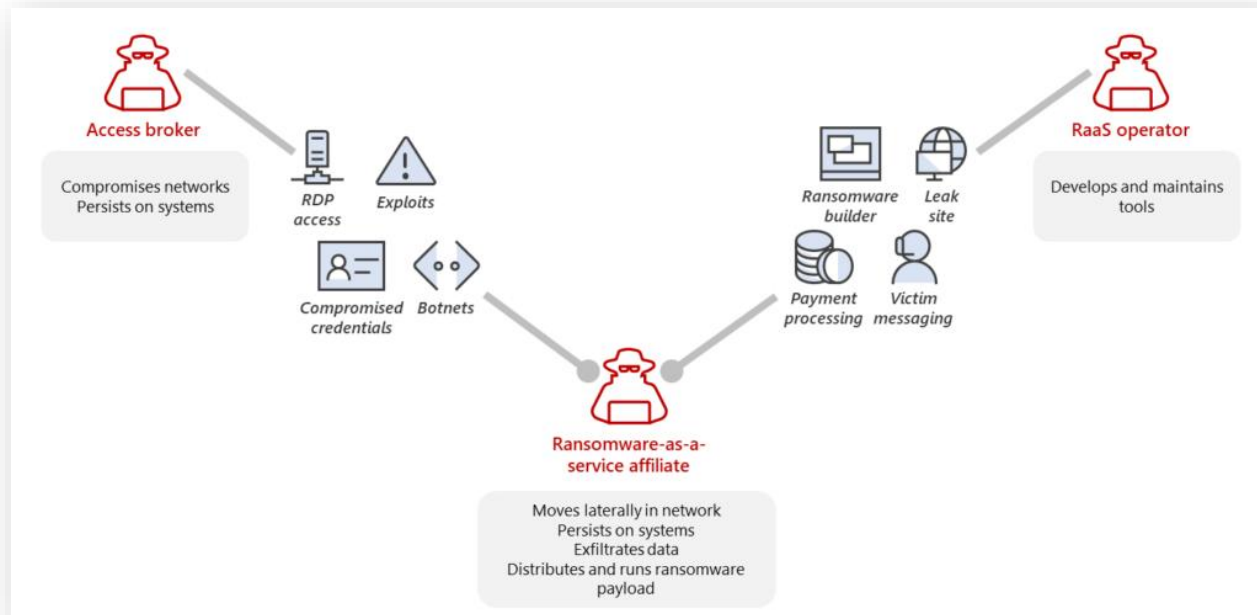
REWARD

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



Ransomware





Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

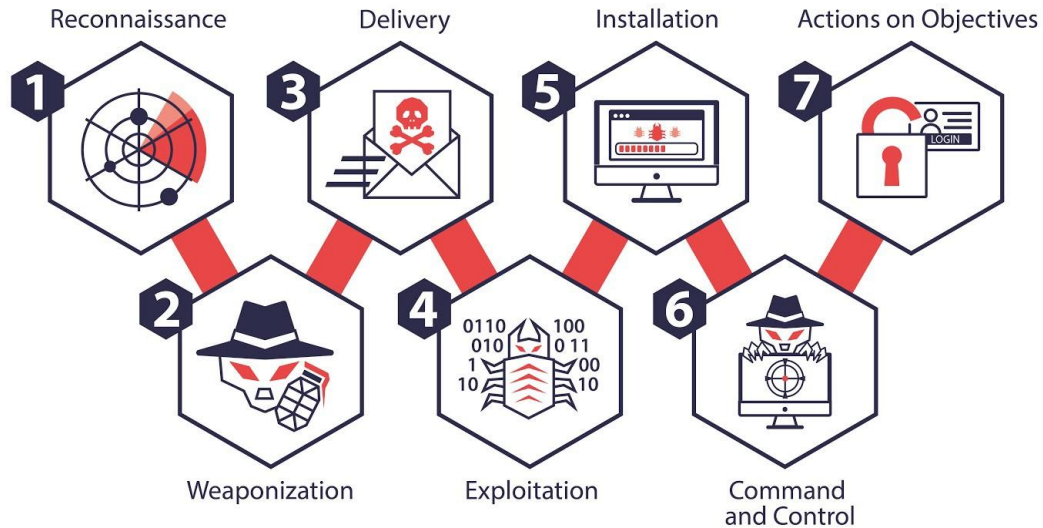
Espionage

Cyber crime



How hackers hack

The Cyber Kill Chain



MITRE ATT&CK

MITRE | ATT&CK™

Matrices

Tactics ▾

Techniques ▾

Mitigations ▾

Groups

Software

Resources ▾

Blog 📄

Contribute

Search 🔍

ATT&CK Matrix for Enterprise

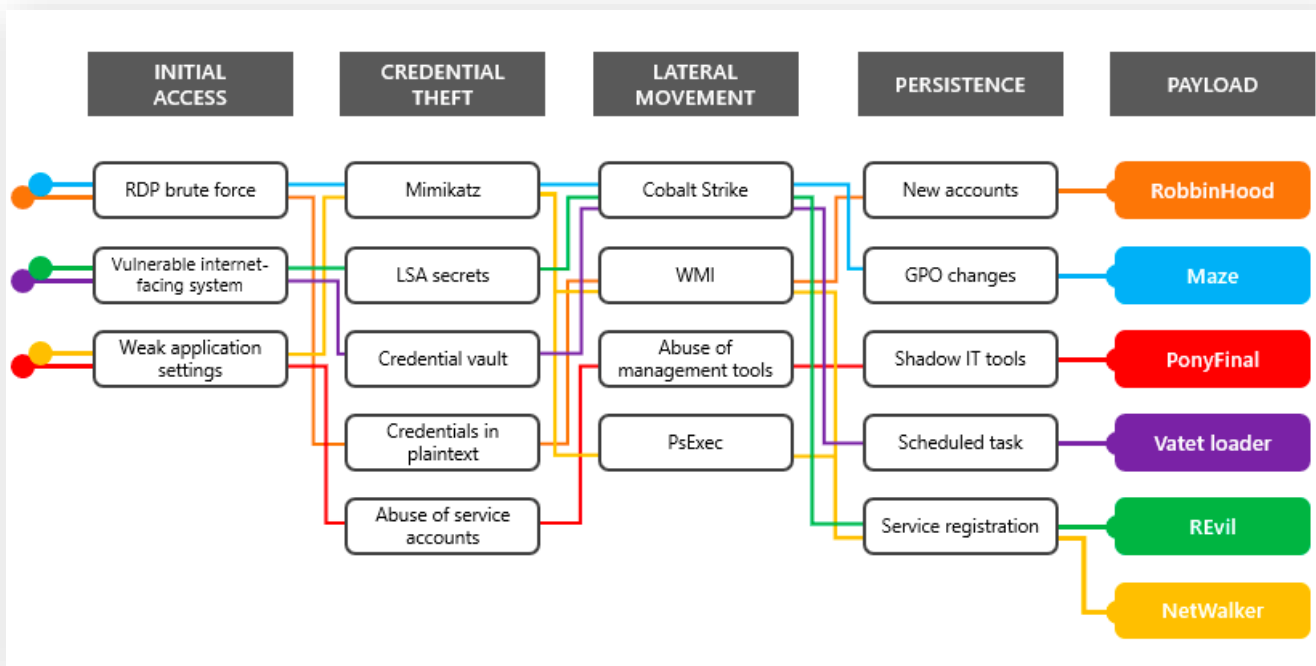
layouts ▾

show sub-techniques

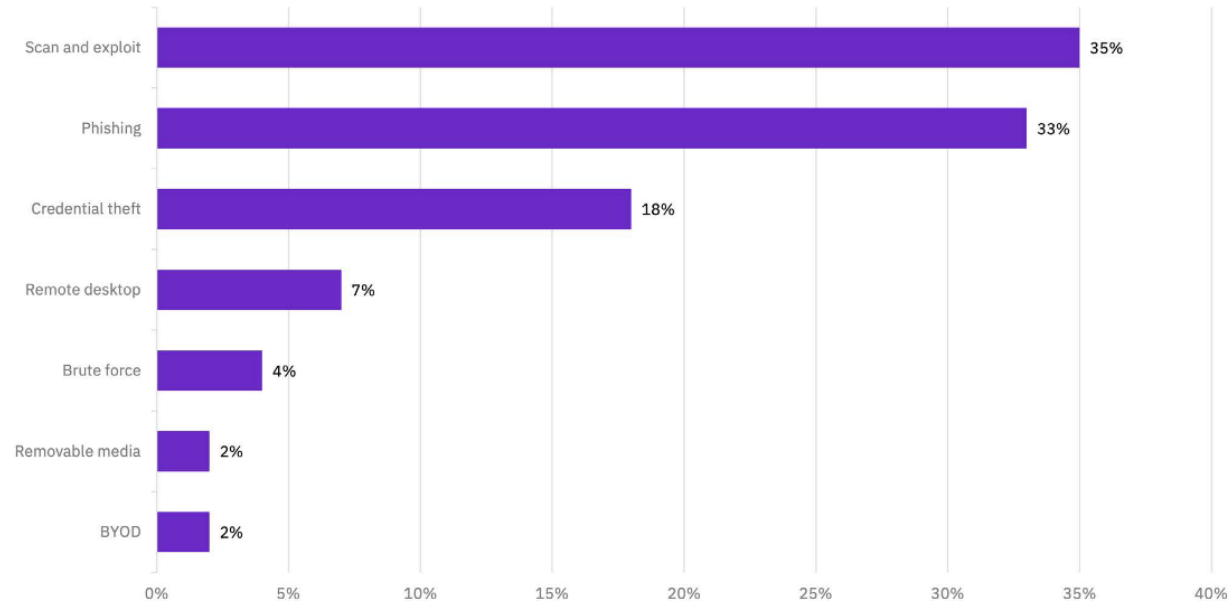
hide sub-techniques

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	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	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 (3)	Access Token Manipulation (3)	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 (3)	Boot or Logon Initialization Scripts (3)	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 (3)	Browser Extensions	Compromise Client Software Binary	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	Software Deployment Tools	Create or Modify System Process (4)	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 Other Network Medium (1)	Disk Wipe (2)
Supply Chain Compromise (2)	System Services (2)	Event Triggered Execution (13)	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 Physical Medium (1)	Endpoint Denial of Service (4)
Trusted Relationship	User Execution (2)	Event Triggered Execution (13)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Share Discovery	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Firmware Corruption	Inhibit System Recovery
Valid Accounts (4)	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (6)	OS Credential Dumping (8)	Password Policy Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
		Hijack Execution Flow (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal Application Access Token	Peripheral Device Discovery		Data Staged (2)	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
		Implant Container Image	Scheduled Task/Job (3)	Indicator Removal on Host (6)	Steal or Forge Kerberos Tickets (2)	Permission Groups Discovery (3)		Email Collection (3)	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
		Office Application Startup (6)	Valid Accounts (4)	Indirect Command Execution	Steal Web Session Cookie	Process Discovery		Input Capture (4)	Protocol Tunneling		System Shutdown/Reboot
		Pre-OS Boot (3)		Masquerading (6)	Two-Factor Authentication Interception	Query Registry		Man in the Browser	Proxy (4)		
		Scheduled Task/Job (3)		Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (6)	Remote System Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Server Software Component (3)		Modify Registry		Software Discovery (1)		Screen Capture	Traffic Signaling (1)		
				Obfuscated Files or		System Information Discovery		Video Capture	Web Service (3)		
						System Network Configuration Discovery					
						System Network Connections Discovery					

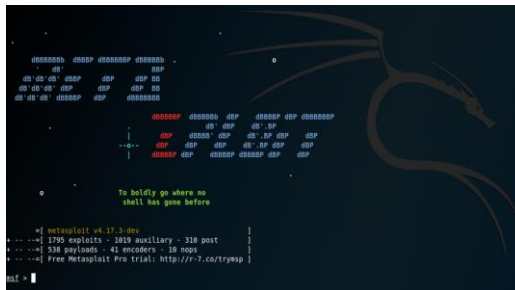
MITRE ATT&CK in action



Look at the numbers (initial access)



Try it yourself





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



Lecture plan / topics

- | 36 | Security concepts and principles
- | 37 | **Cryptographic building blocks**
- | 37 | Key establishment and certificate management
- | 37 | User authentication, IAM
- | 38 | Operating systems security, web, browser and mail security
- | 38 | IT security management and risk assessment
- | 39 | Software security - exploits and privilege escalation
- | 39 | Malicious software
- | 40 | Firewalls and tunnels, security architecture
- | 40 | Cloud and IoT security
- | 41 | Intrusion detection and network attacks
- | 41 | Forensics
- | 42 | Fall Vacation - No lectures
- | 43 | Privacy and GDPR
- | 43 | Privacy engineering
- | 44 | Final guest lecture and Exam Q/A