ParIdigi MasterClass
Grosser Rat Bern

Cybersecurity

Bern, 11. März 2024

Prof. Dr. Endre Bangerter, Co-Leiter Institute for Cybersecurity and Engineering, BFH

Dr. Melanie Knieps, Forscherin Digital Society Initiative, UZH

Eine Veranstaltung von:

Universität Zürich[UZH]
Digital Society Initiative

Parldigi

Unterstützt durch:

Stiftung Mercator Schweiz

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Cyberattacken – Ein Blick hinter die Schlagzeilen

Grosser Rat Bern, 11.3.24

Endre Bangerter

▸ Technik und Informatik

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Expert, unbiased reporting from Gaza, Israel and the Middle East.
Try the FT's comprehensive coverage for just £1

US Treasury bonds

Ransomware attack on ICBC disrupts trades in US Treasury market

Chinese bank says it has contained a hack that affected some fixed income and equities transactions

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — AMERICA'S CYBER DEFENSE AGENCY

Search

Topics Spotlight Resources & Tools News & Events Careers About

Home / News & Events / News

BLOG

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years

Digital | Hack-Angriff: Ransomware-Gruppe Play erpresst NZZ und CH Media

Hacker-Gruppe Play erpresst «NZZ» – zittern vor Veröffentlichung im Darknet

«Mehr vertrauliche Daten gestohlen als angenommen»

Die Nervosität bei «NZZ» und CH Media steigt. Die beiden Verlage werden von der Hacker-Gruppe Play erpresst. Nun ist klar: Der Schaden ist grösser als vermutet. Die Hacker habe mehrmals gedroht, das Material zu veröffentlichen. Neuster Termin: Mittwoch, 3. Mai.

Russischer Cyber-Angriff

Beim RUAG-Hack wurden vertrauliche Daten geklaut

Belgacom Attack

Britain's GCHQ Hacked Belgian Telecoms Firm

The Washington Post
Democracy Dies in Darkness

TECH POLICY

Microsoft warns Russia has escalated its hacking campaign

The company says Russia's SVR foreign intelligence unit is behind the widening attacks

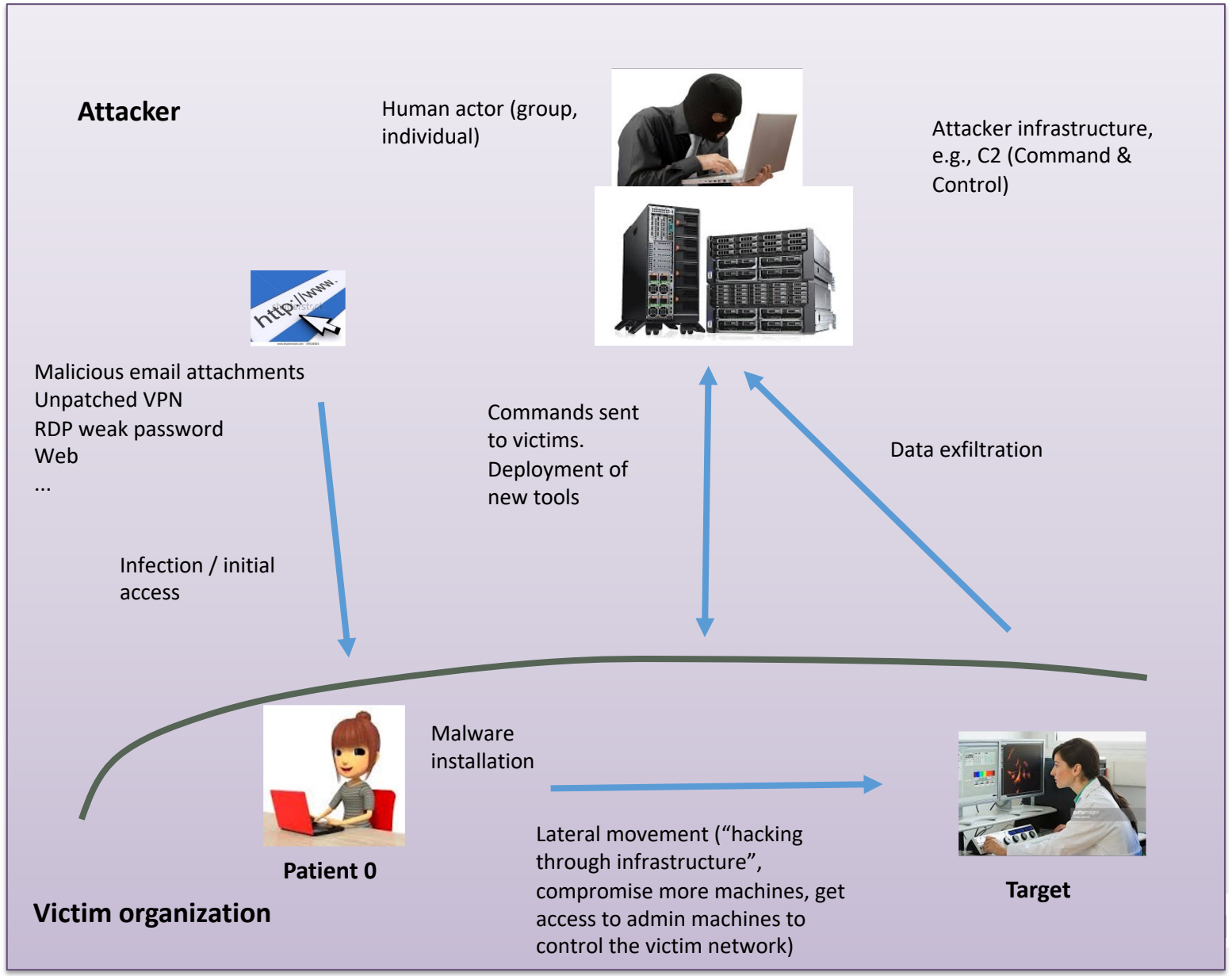
By Joseph Menn

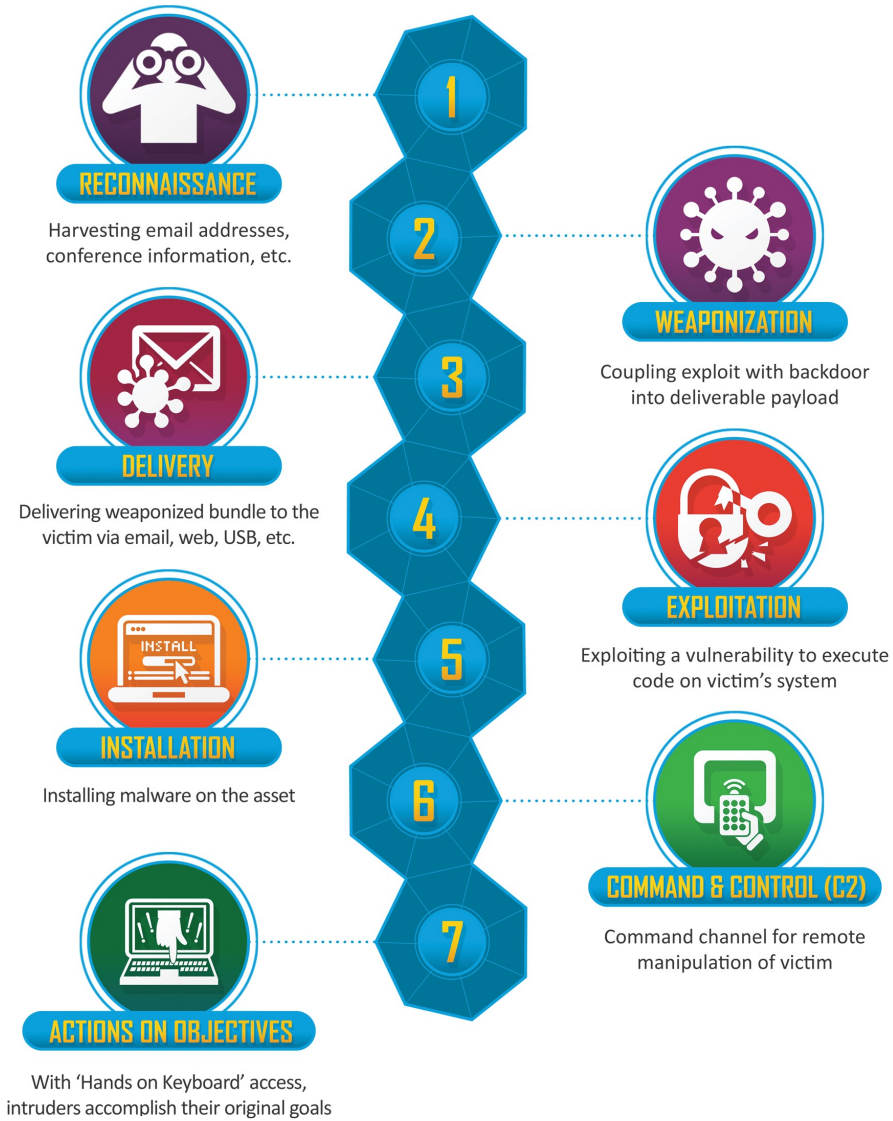
March 8, 2024 at 5:43 p.m. EST

Reasons for prevalence of cyber attacks

- Digital society and economy offer new opportunities for cybercrime, espionage etc.
- Connectivity allows attacker to be anywhere, attribution is hard, risks for attacker are low.
- Asymmetry between attacker and defender.
- All IT systems are vulnerable, and all defence can be bypassed given enough time and skills.
- Human vs human - creativity of attackers, social engineering of victims
- IT security is below state of the art, companies, organizations, individuals don’t care enough about IT security.

Anatomy of cyberattacks - Cyber kill chain





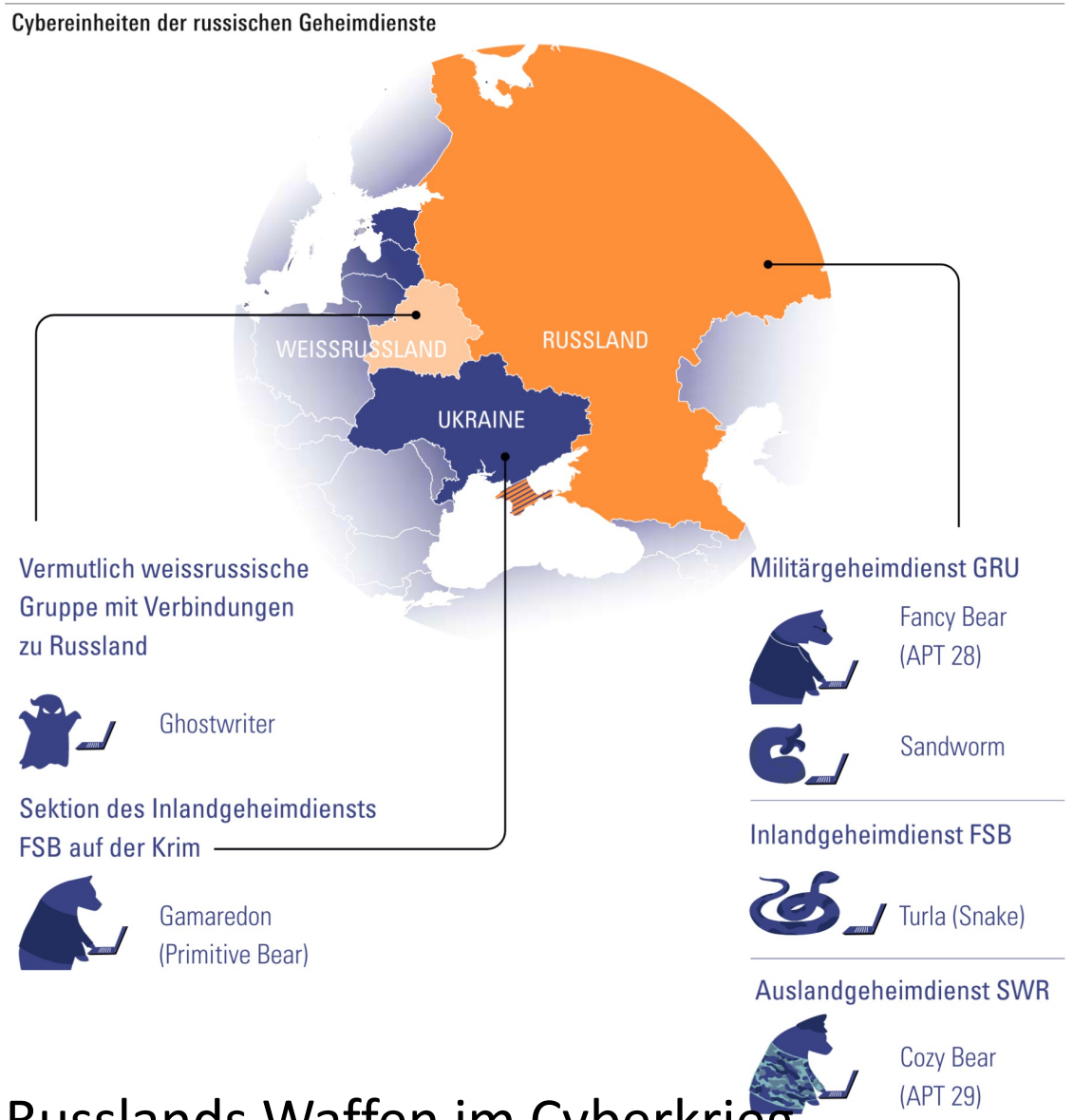
https://www.lockheedmartin.com/en-us/capabilities/cyb
kill-chain.html

Actor categories

	Cybercriminals	Law enforcement	Intelligence	Military	Unknowns
Objectives	Money	Surveillance of criminals, bypass encrypted communication	Information theft, influence operations, disinformation	Disruption or destruction of civil-, or military infrastructure	
Targeting	Opportunistic, weakly targeted	Highly targeted	Highly to medium targeting, depending on tasking	Targeted	
Victims	Mostly companies, sometimes individuals.	Criminals	Government, companies, NGOs, individuals (e.g., journalists)	Civil and military infrastructures, society at large	
Target platforms	Mainly Windows, some Linux, some Linux, some MacOS	Cell phones, laptops etc.	Any, including some exclusive like routers	Any, possibly including weapon systems	
Capabilities & funding	Medium to advanced	State funding, medium, funding depends on state	State funding, usually high	State funding, usually high	
Operating principle	Rather short term, until they get money	Defined by tasking	Long term, keep coming back		
Attack tools	Proprietary, tools traded in cybercrime underground, commercial tools, free tools	Often commercial attack tooling bought from spyware vendors Systematic access to zero-days through spyware vendors	From highly exclusive and advanced to free tools. Systematic access to zero-days	From highly exclusive and advanced to free tools. Systematic access to zero-days	
Defense	Commonplace techniques	Advanced security to none	Advanced security to none	Advanced security to none	

Based on Slides by Recuritiy Labs, ACM CCS 2013

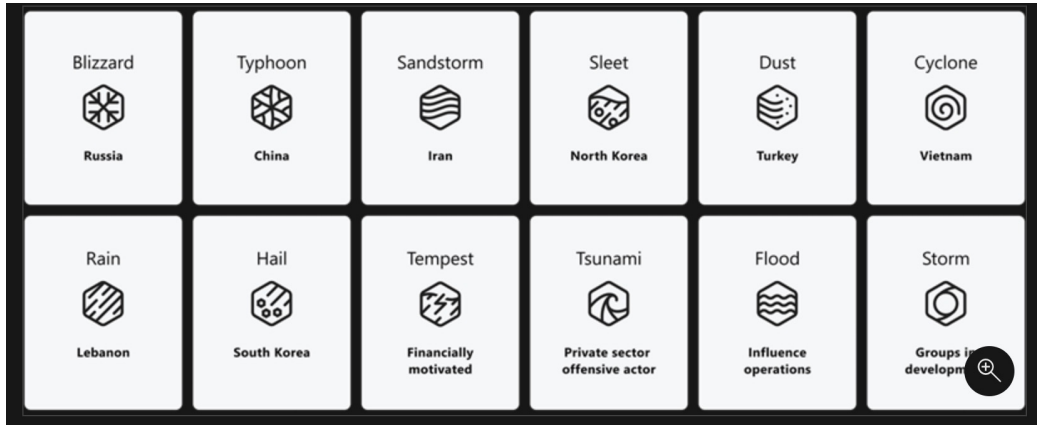
Espionage – Russian Actors



NZZ 4.2.23 FancyBear, CozyBear, Sandworm – Russlands Waffen im Cyberkrieg

Actor tracking

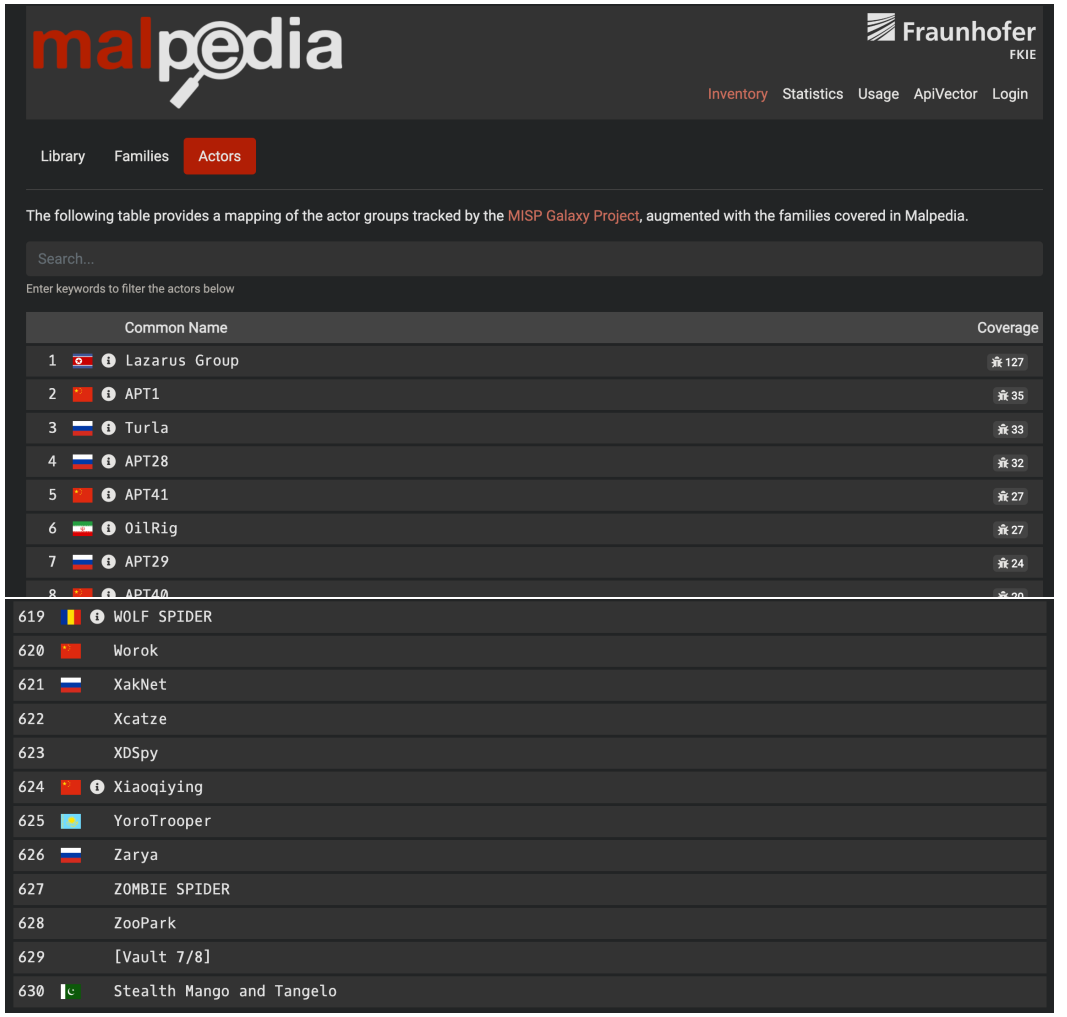
Microsoft publicly tracks 100+ actor groups



Actor category	Type	Family name
Nation-state	China	Typhoon
	Iran	Sandstorm
	Lebanon	Rain
	North Korea	Sleet
	Russia	Blizzard
	South Korea	Hail
	Turkey	Dust
	Vietnam	Cyclone
Financially motivated	Financially motivated	Tempest
Private sector offensive actors	PSOAs	Tsunami
Influence operations	Influence operations	Flood
Groups in development	Groups in development	Storm

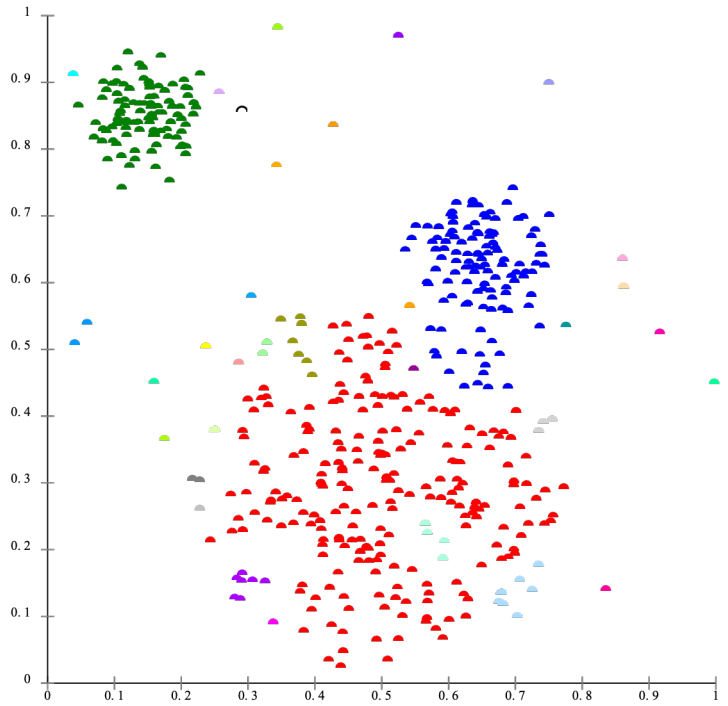
https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-threat-actor-naming?view=o365-worldwide

Malpedia documents 600+ groups from OSINT

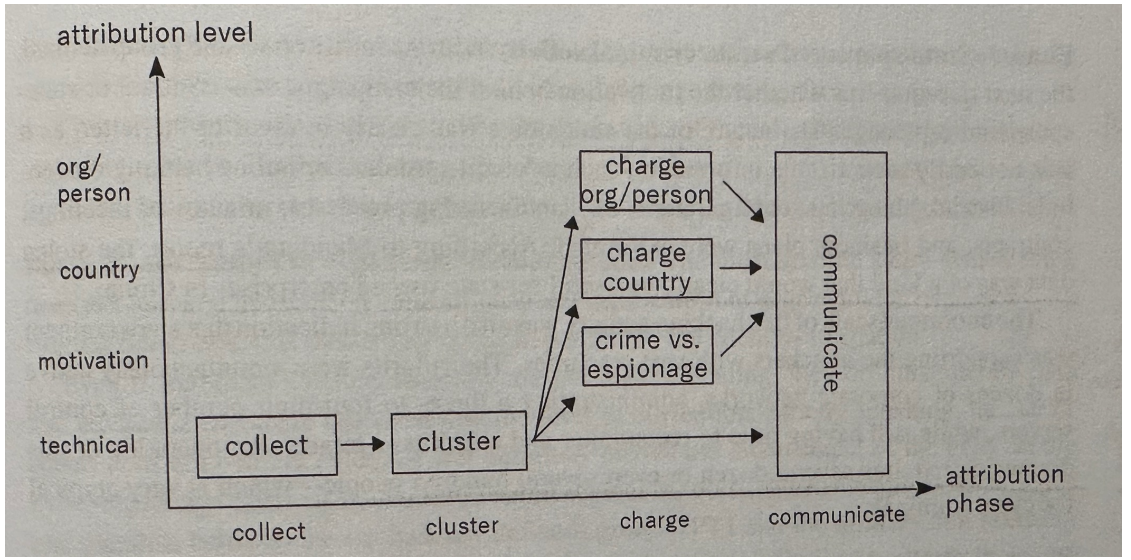


https://malpedia.caad.fkie.fraunhofer.de/actors

What is an actor, how are they identified



Attack clustering



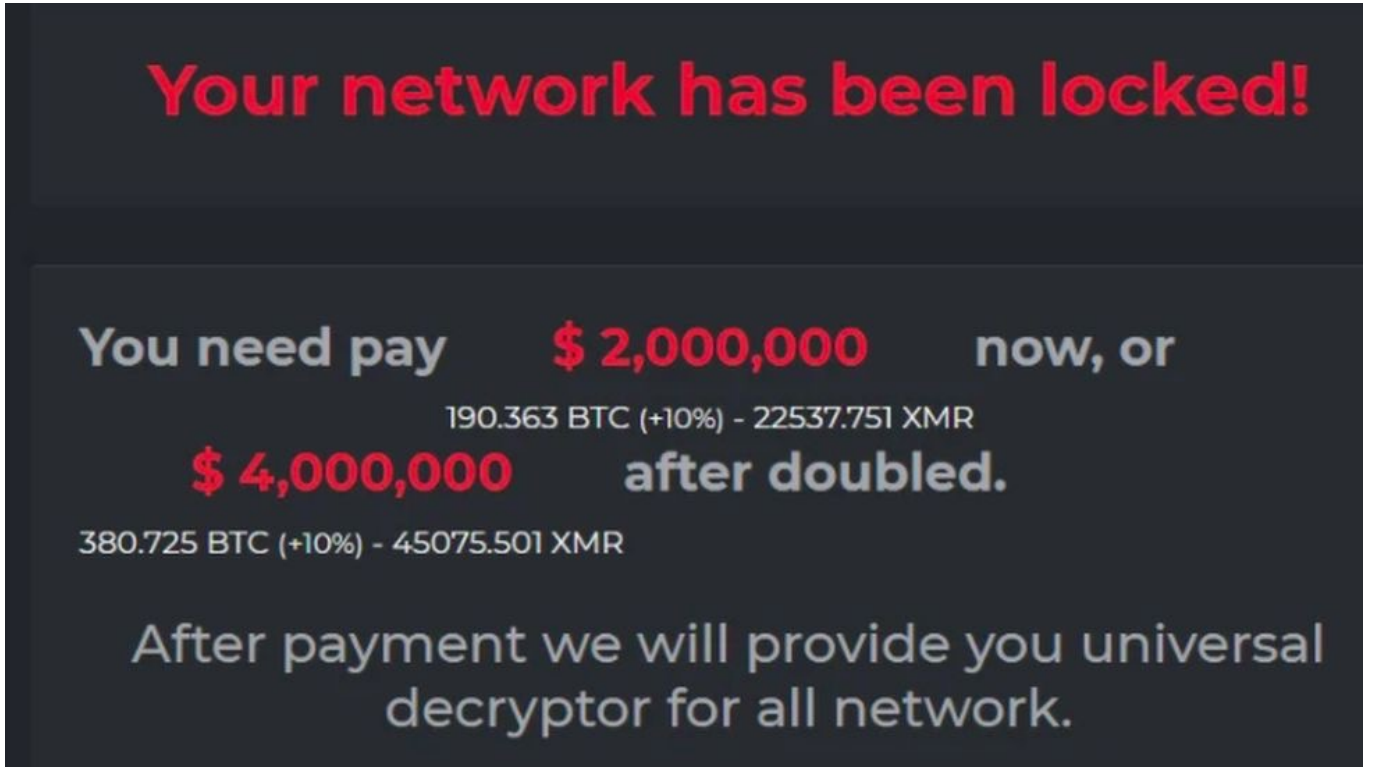
Attribution of Advanced Persistent Threats, Timo Steffens

International | Spam, scam, scam, scam

New technology has enabled cyber-crime on an industrial scale

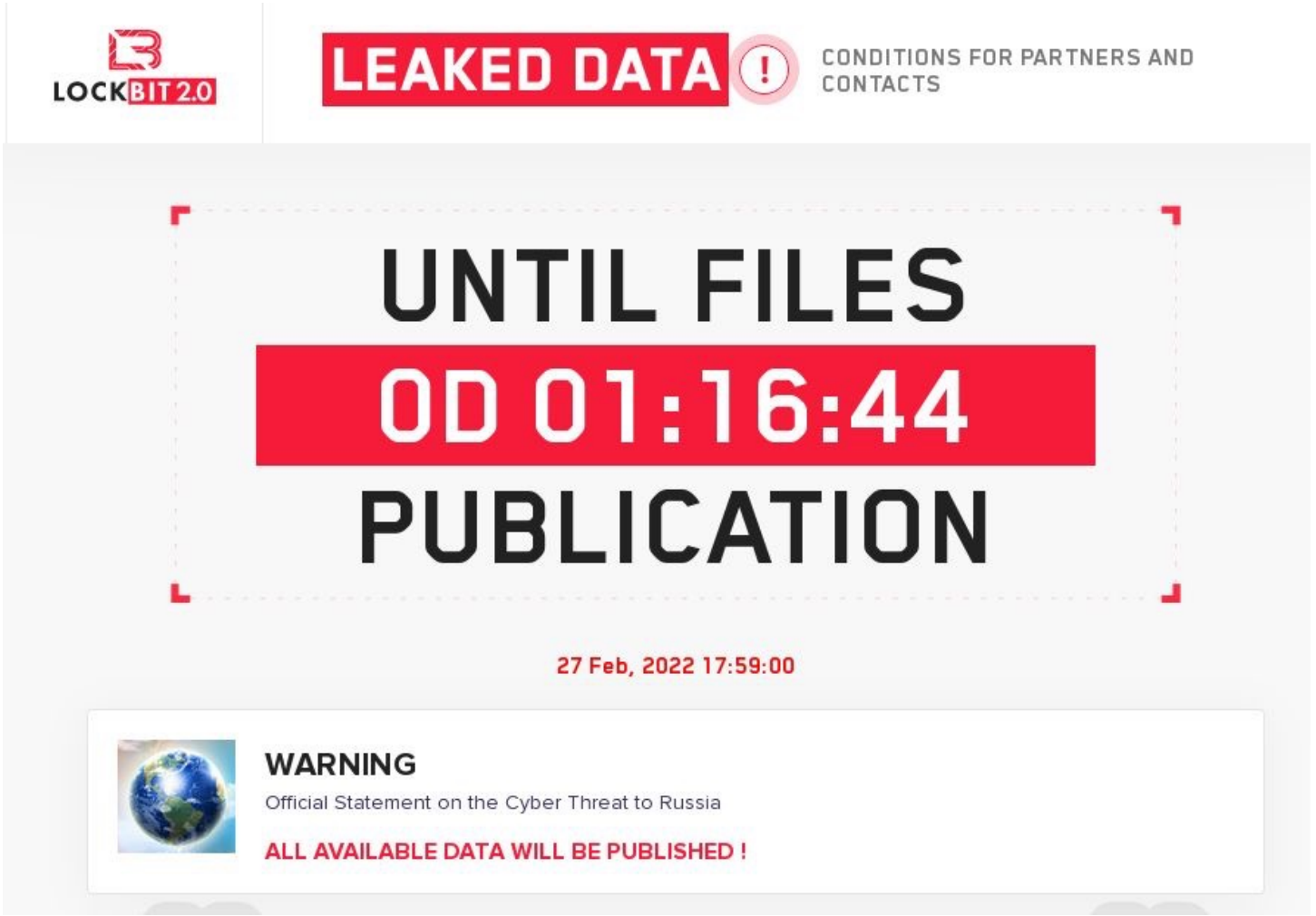
A decentralised dark economy makes cyber-crooks more effective and harder to catch

Ransom notice – decryption of files

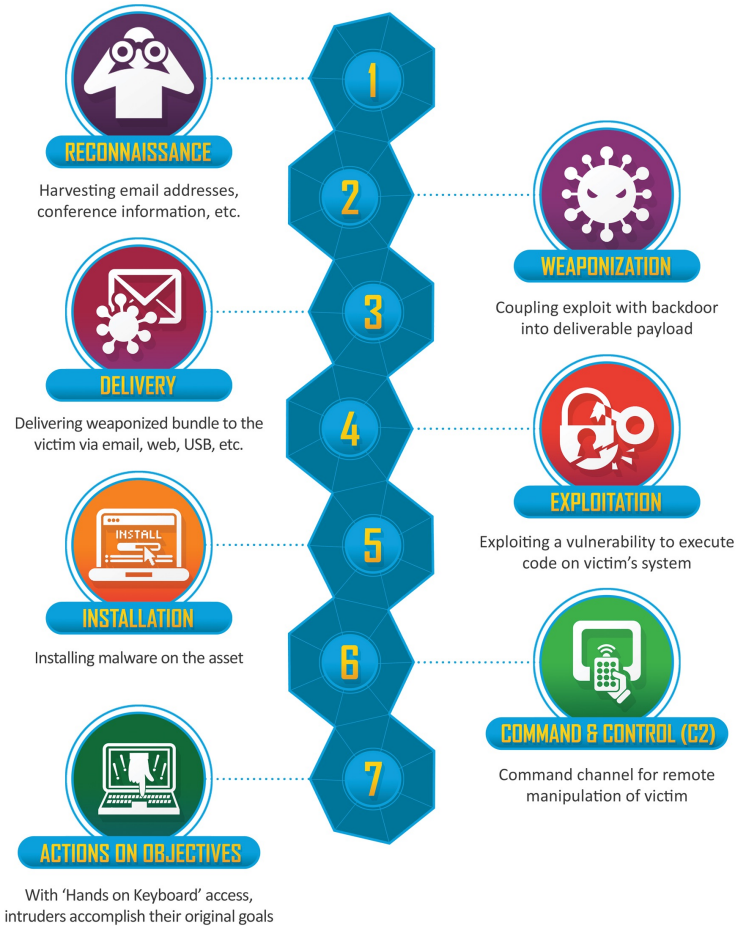


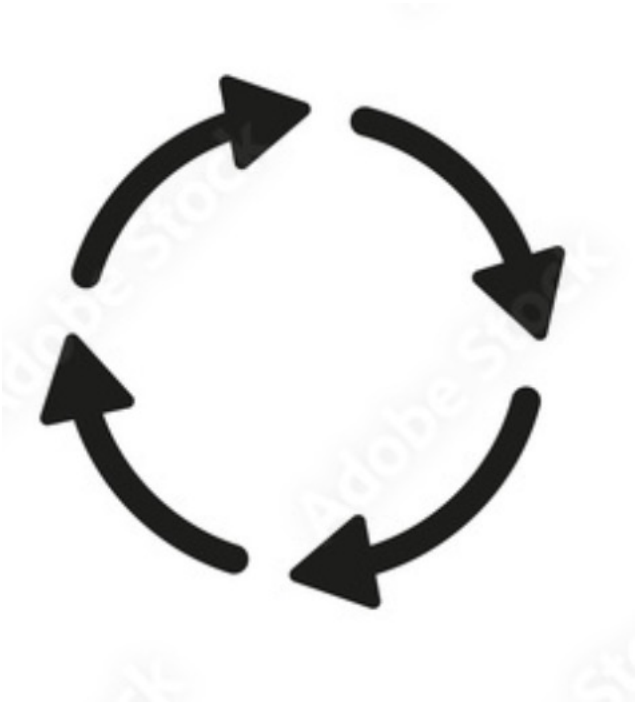
https://www.bbc.com/news/technology-57063636

Ransom notice – leakage of stolen data



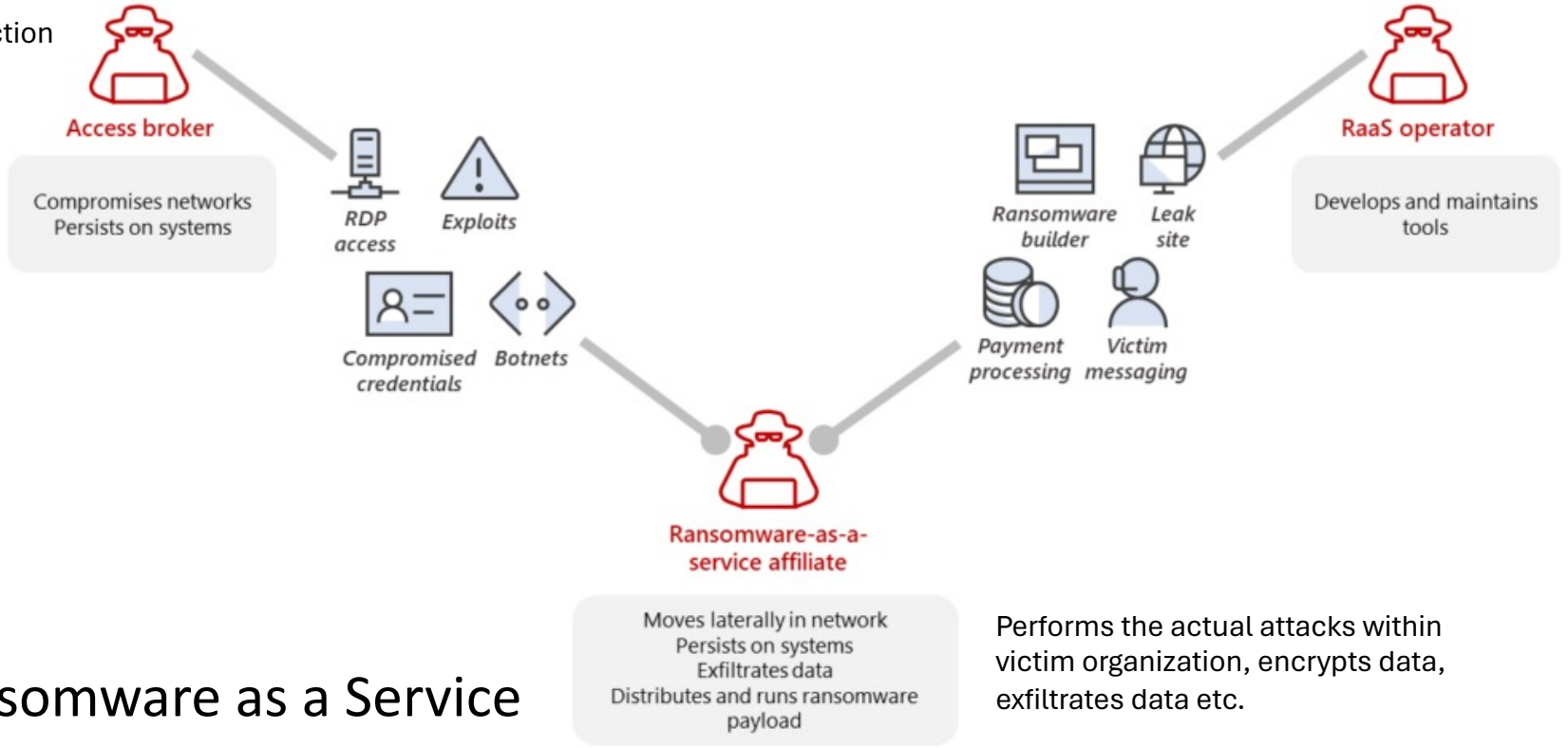
Industrialization of Ransomware attacks





Ransomware – RaaS industrialization of cybercrime

Initial access / infection



Provides tooling (malware) as well as infrastructure / services to get ransom

Performs the actual attacks within victim organization, encrypts data, exfiltrates data etc.

RaaS = Ransomware as a Service

https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Cyber security is possible

100% security is not possible, it is about reducing risks, like in all adversarial settings

Cyber security is multi faceted problem, no silver bullet solution in sight

Reasons for prevalence of cyber attacks

- Digital society and economy offer new opportunities for cybercrime, espionage etc.
- Connectivity allows attacker to be anywhere, attribution is hard, risks for attacker are low.
- Asymmetry between attacker and defender.
- All IT systems are vulnerable, and all defence can be bypassed given enough time and skills.
- Human vs human - creativity of attackers, social engineering of victims
- IT security is below state of the art, companies, organizations, individuals don't care enough about IT security.

Berner Fachhochschule | Haute école spécialisée bernoise | Bern University of Applied Sciences

Cyber Security at BFH

- BFH is a pioneer in cyber security education since 2005, long before the cyber security hype
- Bachelor IT security specialization
  - Very popular among students
  - 300+ graduates over past years
- Continuing education, 500 course participants in last 5 years

MAS Cyber Security
MAS Digital Forensics

CAS Networking & Security
CAS IT Security Management
CAS Security Incident Management Prevention & Detection
CAS Security Incident Management Analysis & Reaction
CAS Cyber Threat intelligence
CAS Linux Cyber Security
4 CAS und 17 Fachkurse im Thema Digital Forensics

- Institute for Cyber Security and Engineering
- Applied R&D
  - Smart phone security
  - Secure e-voting
  - Identity and access management
  - Cyber threat intelligence
  - Wireless Communications, secure Internet of Things, hardware security
  - GNU Taler – privacy firendly payment systems
- Ransomware sensibilization campaign for SMBs
- More information https://www.bfh.ch/en/topics/cyber-at-bfh/

ParIdigi MasterClass

Grosser Rat Bern

Eine Veranstaltung von:

Universität Zürich[UZH]

Digital Society Initiative

Parldigi

Unterstützt durch:

Stiftung Mercator Schweiz