THREAT LANDSCAPE

Prof. Dr. Bernhard Tellenbach

Goals

- You know what a threat landscape is and why it is important to track it
- You can pinpoint sources of information for tracking the threat landscape
- You know about the most relevant threats in the past two years and can point out some trends
- You can explain terms and concepts often heard when talking about the threat landscape, especially advanced persistent threat and the cyber kill chain

Definition - Threat Landscape

- A collection of threats, threat actors (threat agents) and observed trends
- Tracking it means you know:
  - the threat agents and their capabilities
  - the weapons and tactics used
  - what threats exist and which are considered most relevant
  - trends and emerging threats and actors
- Why relevant?
  - Know your enemy - prepare for current and emerging threats
  - Provides motivation for investments in security controls

Threat Landscape – What does it mean?

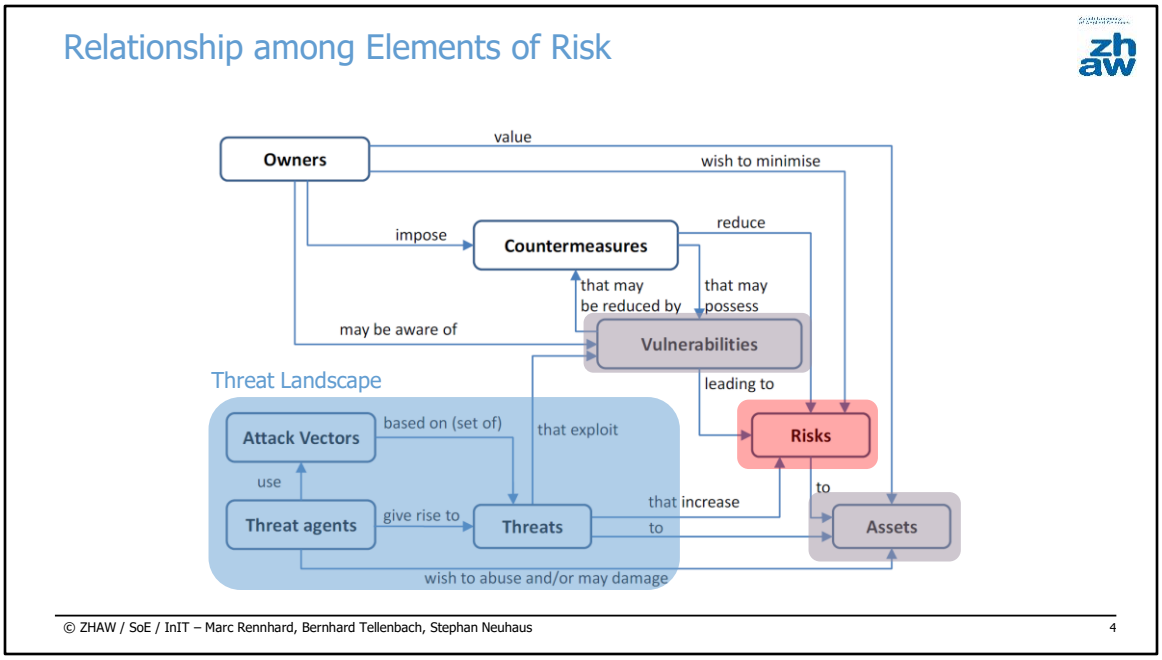
Even though the term "threat landscape" is used a lot, definitions of what a threat landscape is or contains are hard to find. **ENISA** defines it as follows:

*"*The ENISA Threat Landscape provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends."

Source: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

ENISA – European Union Agency for Cybersecurity

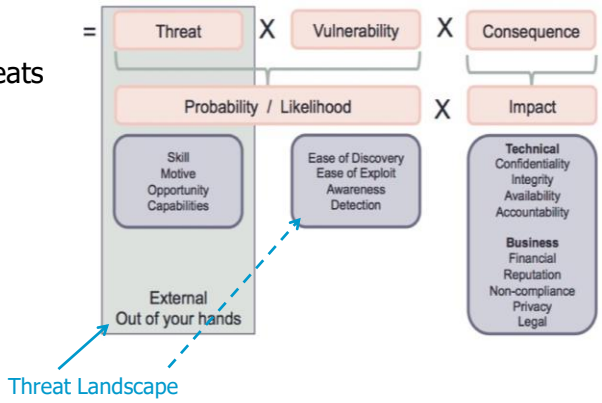
The name of the agency originates from its former name, the **E**uropean **N**etwork and **I**nformation Security **A**gency.



Relationship of the Threat Landscape and the Elements of Risk
This diagram taken from ISO 15408:200550 shows the relationships among all elements of risks. This level of granularity is sufficient to illustrate the main elements of threat and risk mentioned in the ETL. The entities “Owner”, “Countermeasures”, “Vulnerabilities”, “Risks” and partially “Assets” are not considered in the ETL. However, this figure shows their context regarding threats. The notion of attack vector and the entities *threat agent* and *threat* are part of the ETL. This is quite natural as these entities make up the kernel a threat landscape.

Importance of the Threat Landscape for Risk

- Understanding and estimating the risk faced by an organization
  - Risk = Likelihood x Impact
- The probability / likelihood of threats to pose a relevant risk heavily depends on the current threat landscape



The evolution of the threat landscape is hard to predict as it depends on factors like local and/or international politics (e.g., conflicts/war), local and/or international events (e.g., a pandemic), the behavior of companies, advances in hacker tools or defensive measures.

An example for how important it is to know the threat landscape and to prepare accordingly is the attack on PostFinance, the financial services arm of Swiss Post in 2010 . Many more and far more recent examples could be given. For example, check out the many incidents related to ransomware. Many companies underestimated this threat and/or did not react to it in a timely fashion.

Example: In December 2010, the **PostFinance** site went down at around 10.30 pm local time on Monday and was still closed 24 hours later. The reason was that supporters of WikiLeaks founder Julian Assange, who was arrested in London in that week, attacked PostFinance for PostFinance's decision to close Assange's account. While the reason for the closing of the account - false indications regarding his place of residence"; Assange had declared Geneva his place of residence – was probably ok from a legal standpoint, the timing was hardly a coincidence. As a bank with accounts from people that are of public interest, PostFinance should know that they must be careful when dealing with such people and that they should have known about the hackers supporting Assange.

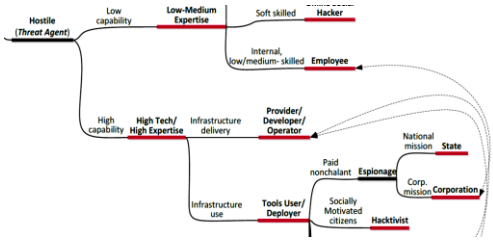
See also: https://www.swissinfo.ch/eng/wikileaks-supporters-attack-postfinance-site/28971816

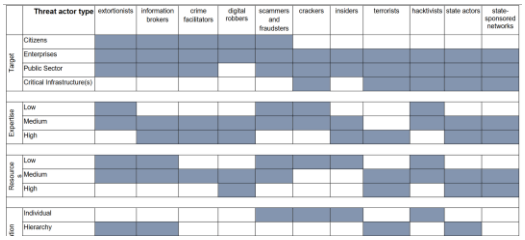
Threat Landscape – Important Elements

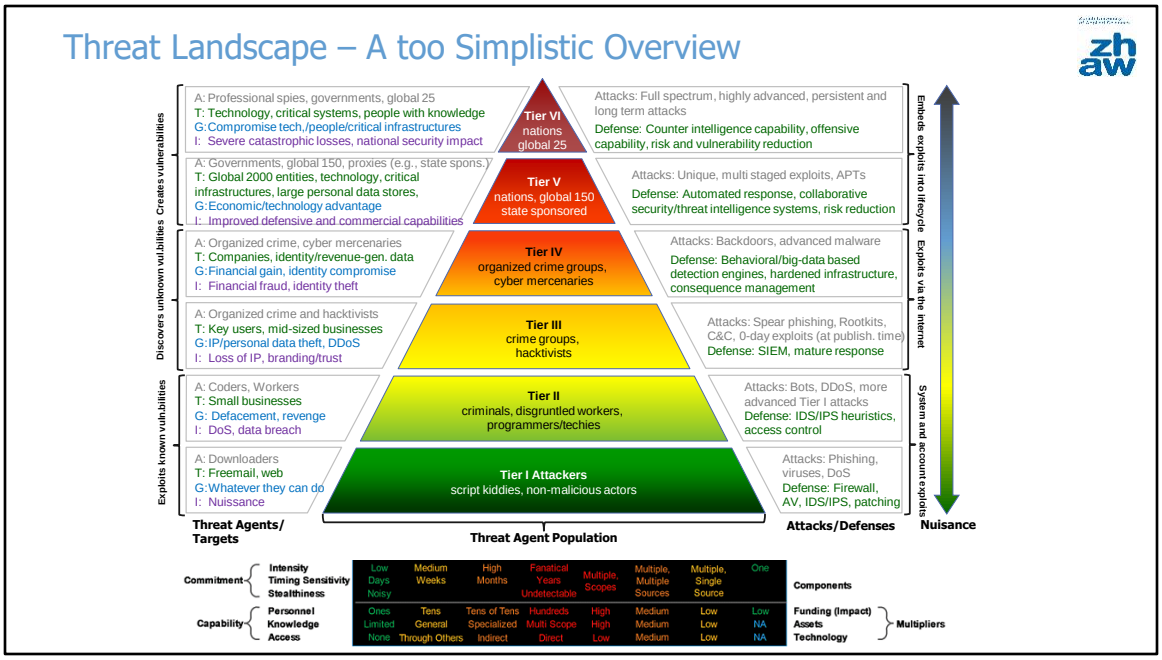
- Threat actors
  - State actors, cyber criminals, insiders,…
  - Attributes to characterize them
    - Motivation (financial, ideological, …)
    - Skill and resources (low, medium, high)
    - Organization (individual, collective, …)
    - Tactics
    - …
- Threats:
  - Threat type and description (e.g., ransomware, phishing, insider threat, …)
  - Targeted assets (e.g., users in the home office, websites of online casinos, CISOs, …)
  - Attack vectors
    - What are the procedures/methods/tools used?
    - Often split in different phases (=> cyber kill chain)

Challenge

- There is no standardized way to characterize or document it
- For threat actors: What threat actors exist and how are they characterized?
  - Examples (many more exist):
    - Definition in ENISA ETL 2015 (top right)
    - Definition by the National Cyber Security Center Netherlands (bottom right)
- For threats: What categories of threats exist and how are they characterized?
- In many cases the lines between threat actors/threat types are blurred
- Companies often define their own threat categories and vocabulary







Source (modified): https://www.peerlyst.com/posts/today-s-threat-landscape-the-defenders-nightmare-1-derek-krein

The diagram summarized the threat landscape by showing the most relevant building blocks and their relation:

- A: Threat Agents and how the Tier impacts on the size of the threat agent population
- T: Targets / targeted assets
- G: Goal
- I: Impact
- Examples of attacks that are typically attributed to a certain Tier
- Examples of defenses that can be used to defend against threat agents of a certain Tier

Important Notes:

This is a heavily simplified view of the threat landscape:

- Assignment of Threat Agents to Tiers: This is not a 1:1 assignment in practice. For example, not all hacktivists are Tier III Threat Agents, there are also Tier I hacktivists.
- Capabilities/Skills: Here, the vulnerability-related capabilities/skills serve as an example for the increase in skill/capability toward the tip of the pyramid. There are many other domains, for example if and how they interact with people or how skilled they are in circumventing defenses.
- Attacks assigned to a Tier: This is not a 1:1 assignment in practice. For example, a DDoS attack might also be used by Tier III attackers, for example to distract the defenders from the actual attack.

Furthermore, defenses are usually not considered to belong to the threat landscape. They are listed here to illustrate what level of sophistication is required to defend against threat actors of a certain tier.

Examples of Attacks:

- **Tier VI (Nations): Stuxnet.** In June 2010, computer security researches discover a computer worm called Stuxnet designed to attack programmable logic controllers in industrial machinery. The worm is thought to have been created by the U.S. and Israeli cyberwarfare teams to attack Iran's Natanz uranium enrichment plant. The worm seems designed to alter the speed of uranium enrichment centrifuges in a way that generates vibrations strong enough to destroy them. Other reports suggest that Stuxnet damaged around 1,000 centrifuges, reducing the number in operation in Iran from 4,700 to 3,900 [1]. The attack relied on **four different zero-day exploits** [2] – this is exceptional and has since then not been observed anymore in the wild.
- **Tier V/VI (Nations): Crypto AG case.** Since the Fall of 1993, the Strategic Intelligence Service (German: Strategischer Nachrichtendienst or SND) managed to get reliable information about Crypto AG. It learned that the company was owned by foreign intelligence agencies and exported "weak" devices, the encryption of which could be broken with a realistic effort. In order to be able to break the encryption of such devices itself, the SND began to gather technical information about their encryption methods and customer lists. Later, when the SND had become a civilian office, it managed to get enduring access to this knowledge with the consent of the American intelligence agencies.
- **Tier V (Nations/State sponsored): Sony-hack.** In December 2014, a series of leaked internal documents and spreadsheets containing information and data of the company's employees and senior executives have been leaked to the public by a hacker group who call themselves *Guardians of Peace*. However, the attribution of this event is difficult, and several theories and "evidence" exists (FBI sees North Korean government as the attacker) [1]. Furthermore, the level of sophistication is supposedly not as high as in the case of Stuxnet. While not mentioning Sony by name in its advisory, the US-CERT reported on an attack referring to the victim as a "major entertainment company". The US-CERT said that the attackers used a Server Message Block (SMB) Worm Tool to conduct the attacks. According to the advisory, the SMB Worm Tool is equipped with five components, including a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool. The SMB worm propagates throughout an infected network via brute-force authentication attacks and connects to a command and control (C2) infrastructure with servers located in Thailand, Poland, Italy, Bolivia, Singapore and the United States [3]. The entry vector for the malware is supposedly phishing attacks (statement by Mr. Comey, FBI) where victims have somehow got infected by malware. But other attack vectors like an insider, exploitation of an unpatched vulnerability or a zero-day exploit have also been mentioned.
- **Tier IV (Organized Crime Group): Home-Depot Hack.** The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials. Then they exploited a vulnerability in Windows, which was patched only after the breach which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment. [Remark: Note that it is unclear whether the patch was available before the attack, and they were not patching it immediately or whether it was a "zero-day". There are sources for but without any real "proof"]. Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014) using a decade-old vulnerability which has not been patched. This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014). The stolen payment

cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns [4].

- **Tier III (Hacktivists): Iran Airport Hack.** In May 2018, an anti-government group hacked the airport system at an Iranian international airport in protest of military activities in the region. The group took control of the airport monitors and replaced it with anti-government content and a call to protests. They also took control of the email account of a civil aviation head to spread the news. Earlier this month, a group again disrupted an international airport, this time in Tabriz, by turning the monitors off. This is all occurring during a time of heightened censorship in Iran, including the recent extension of the ban on Telegram [5].
- **Tier I: German Politicians Hack.** Throughout December 2018, God, or "G0d", to use his Twitter handle, had leaked the phone numbers, addresses and, in some cases, private photos and credit-card details of nearly 1,000 German politicians, celebrities and journalists. For weeks no one noticed. But panic set in once the news emerged on January 3rd. Was this an expert group of cyber-anarchists hell-bent on destroying the system? Was it the handiwork of Vladimir Putin? God turned out to be a 20-year-old amateur hacker living with his parents in a small western German town. In fact, the culprit, arrested in the town of Homberg (Ohm) on January 6th, turned out to be a determined "script kiddie" (slang for a hacker who uses code written by others), apparently acting alone. He seems to have obtained the data by guessing passwords, cracking address books and so on. Asked to explain his motivation, he told police that he was "annoyed" by politicians (apart from those of the far-right Alternative for Germany, whom he spared) [6].

Sources:

1. 2001-2013: Survey and Analysis of Major Cyberattacks, Tavish Vaidya, http://arxiv.org/abs/1507.06673 http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know
2. David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab Tracked down the Malware That Stymied Iran's Nuclear-Fuel Enrichment Program," IEEE Spectrum, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-Stuxnet
3. Alert (TA14-353A) - Targeted Destructive Malware, US-CERT, https://www.us-cert.gov/ncas/alerts/TA14-353A
4. Case Study: The Home DepotData Breach, Brett Hawkins, SANS Institute https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367
5. The Growing Reach of Anti-Government Hacktivism: Is the World Cup Next?, Endgame. Blog, June 2018 https://www.endgame.com/blog/technical-blog/growing-reach-anti-government-hacktivism-world-cup-next
6. Germany finds God - A young hacker spooks the German establishment, The Economist, 12.01.2019 https://www.economist.com/europe/2019/01/12/a-young-hacker-spooks-the-german-establishment
7. The report of a Swiss investigation into the case of Crypto AG https://www.electrospaces.net/2020/12/a-swiss-parliamentary-investigation.html

Threat Actors

What's next?

- Profile of the following threat actors in more detail:
  - State-sponsored, Cybercrime, Hacker-for-hire, Hacktivist, Insider, Script-Kiddy
- Profile lists "typical" parameters:
  - Motivation: E.g., intelligence, money, destruction, fame, …
  - Resources: Low, medium or high in terms of time and/or money
  - Skill level: Low, medium or high
  - Role: Developer (e.g., developer of a malware)
    Provider (e.g., provider offering access to a botnet)
    Operator (e.g., operator of a botnet)
    User
- Discuss a recent example for the first four threat actors
  - Most relevant ones in 2020/2021 in Europe according to ENISA ETL
- Lab: More detailed insights and examples in the ENISA ETL

Meaning of Low, Medium, and High

Note that attributes like the resources or the skill level are often quite fuzzy. This stems from the fact that it is quite difficult to specify the skill levels of threat agents in a generic fashion.

Here, regarding the skill, low medium and high can be interpreted roughly as follows:

- Low: Little overall subject matter knowledge, can follows receipts/instructions, sometimes naïve, struggles circumventing most non-basic/standard protections
- Medium: Good overall subject matter knowledge, can adapt receipts/instructions to specific scenarios/victims and circumvent most protections
- High: Expert-level subject matter knowledge, can invent completely knew attack vectors and strategies, finds a way to circumvent all protection mechanisms (given enough time/money)

Regarding the resources, low, medium and high can be roughly interpreted as follows:

- Low: Opportunistic. No fixed/dedicated resources, individuals and groups where this is not their "main business".
- Medium: Budget and personnel like a small company
- High: Budget and/or personnel like a medium-sized to large company

Risk rating methodologies like the one from **OWASP** sometimes provide **more detailed information what the skills** of a threat agents at different skill-levels **have to be**.

In the OWASP methodology, threat agents can have a skill level between 1 and 10 (most skilled). A skill level of 9 requires security penetration skills, a skill level of 6 requires network and programming skills and a skill level of 5 is the level of advanced computer users. However, the OWASP skill levels are still quite fuzzy and rather "technical" and tuned to the kind of vulnerabilities that OWASP is focused on. Does e.g., skill level 10 mean that this attacker has the resources/skills to find and exploit a zero-day vulnerability?

Cybercrime Actors

- Cybercrime actors obtain profit from illegal/criminal activities in cyberspace
- Collaboration and professionalization
  - Ecosystem with service providers and users (*-as-a-Service, see notes)
- Tactics resulting in the best return of investment (ROI)
  - Use of Ransomware – Single, double or triple extortion
    - Largely automated attack and infection process (for the masses)
    - Human-operated ransomware (aka Big Game Hunting) for high, value targets
  - Social Engineering – Exploiting the human factor
  - Exploitation of work-from-home technologies (remote access services)
  - Attacking "low-hanging" fruits for maximum ROI
    - SMEs with low security expertise and budget
    - Novel technologies – e.g., poorly secured and managed cloud deployments
  - Attacking managed service providers as high-value targets
- Challenges:
  - Often cross-boarder activities - different legal frameworks makes fighting cybercrime difficult
  - Blocking/taking down their infrastructure is not very sustainable

Profile	
Motivation	Money
Resources	Medium to High
Skill	Low to High
Roles	User Dev/Prov/Op

Some services offered:

- **Main types:** access brokers, phishing kits, credit/debit card testing services, malware packing services, web inject kits, ransomware, loaders, (bulletproof) hosting and infrastructure, DDoS attack tools, anonymity and encryption, counter antivirus service/checkers, …
- **Distribution services:** social network and instant messaging spam, exploit kit development, spam e-mail distribution, purchasing traffic and/or traffic distribution systems (TDS)
- **Monetization services:** money mule and cashing services, reshipping fraud networks, ransom payments and extortion, wire fraud cryptocurrency services …

Ransomware – Extortion

To put pressure on their victims and force them to pay, some cybercriminals use double extortion tactics:

- First, the systems and data of an organization are encrypted, and a ransom is requested,
- Second, the organization's sensitive data are exfiltrated and the criminals threaten to publish the exfiltrated data on "public shaming websites"

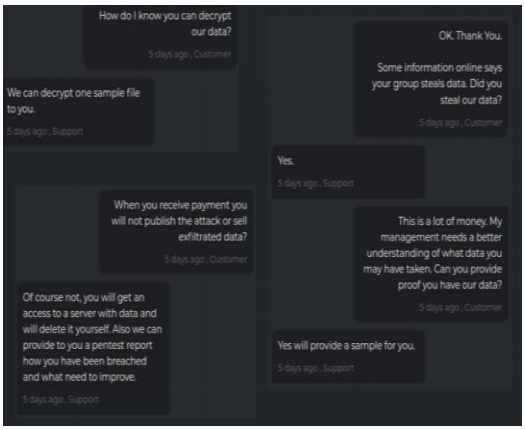
Furthermore, additional steps might be observed to monetize the attack or to put additional pressure on the victim:

- Monetization of the stolen information through data auctions in the dark web
- Media amplification of their victim's compromise by contacting journalists
- Cold calling victims if they begin the ransomware recovery process without paying the ransom
- Reaching out to business partners, investors, board members and other stakeholders disclosing information about the attack
- Conducting DDoS attacks against the victim in order to add more pressure to pay the ransom
- Reaching out to victim's customers and clients to action and demand a ransom payment
- Calling and harassing employees
- Turning to revenge porn as an extortion tactic

Source: ENISA ETL 2021 Report

Cybercrime Actors – Example

- DarkSide RaaS operation
  - Associated with an cybercrime group becoming active in 2013 called CARBON SPIDER by crowdstrike
  - The RaaS business with DarkSide started in 2020
- Colonial Pipeline incident
  - May 2021 - Attack that caused a shut down of 5,550 miles of pipe for 6 days, prompting fuel shortages, a spike in gasoline prices and chaos at airlines.
  - Billing system was crippled => no charging possible => pre-emptively shut down of pipeline operation
  - Approximately 100GB of data were stolen
  - ~$5 million in Bitcoins paid to a *DarkSide* affiliate
- Aftermath:
  - FBI traced 75 Bitcoins paid by Colonial Pipeline and was able to seize 63,7 of them
  - DarkSide shutdown a few days after the Colonial Pipeline attack because of unspecified "pressure" from the United States (unclear, what really happened)



Sources and more details on RaaS:

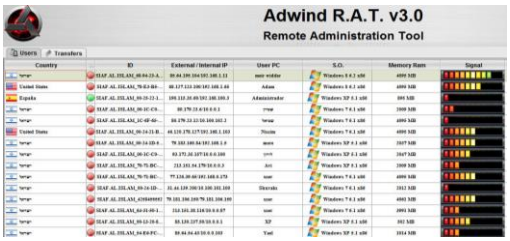
- https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
- https://www.upguard.com/blog/what-is-ransomware-as-a-service

Sources and more details on the Colonial Pipeline incident and the takedown:

- https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html
- https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/
- https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/

Cybercrime Actors – *-as-a-Service

- For example, develop, rent or sell malware and C&C services
  - Guaranteed updates / evasion of anti-virus
  - Service Level Agreements
- What does it cost?
  - 8$ - Credentials for a hacked iTunes account
  - 40$ - Sending 20k SPAM emails using a botnet
  - 100$ - For using an infection service and a max of 1k installs
  - 1000$ - For doing a DDoS attack of 1 month
  - 40'000$ - For buing a malware with a bootkit
  - 400'000$+ - For GovWare

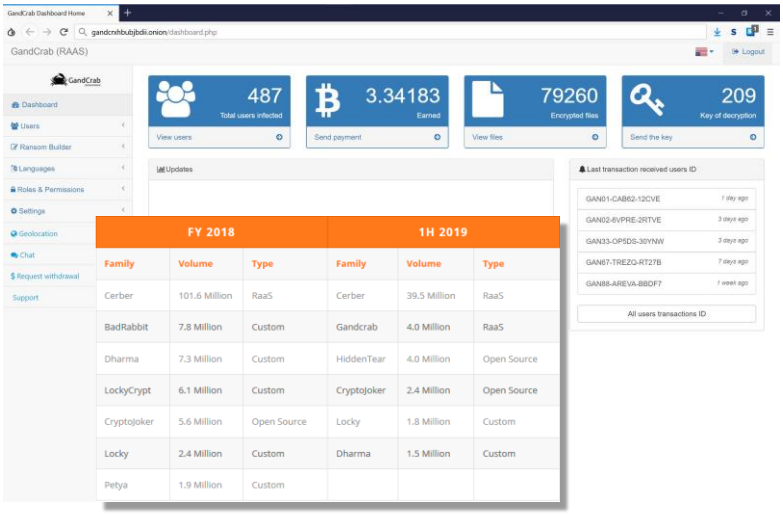


Numbers might vary from day to day and are indicative only.
They give an idea of what prices have been at some point but do not necessarily reflect todays prices.

They might now be much higher or lower, depending on many factors like availability, difficulty of compromising the targets etc.
For more details including the sources of these numbers, please check out:
http://resources.infosecinstitute.com/cybercrime-as-a-service/
and Google for information about current prices on the "black market".

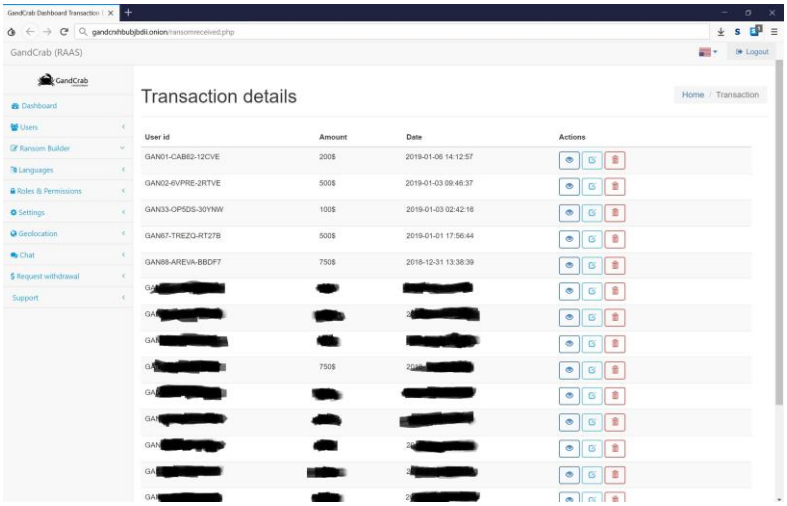
GovWare - In German-speaking countries, spyware used or made by the government is sometimes called *govware*. An insightful article about one of the most notorious GovWare providers on the planet - Hacking Team – can be found here:
http://www.forbes.com/sites/thomasbrewster/2015/07/06/us-gov-likes-hacking-team/#7fb92f855244

Example: Ransomware-as-a-Service (1)

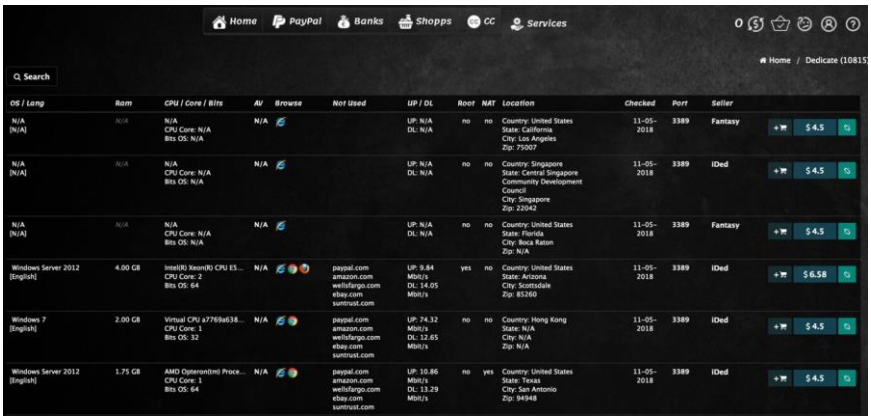


GrandCrab Story (shutting down in June 2019):
https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

Example: Ransomware-as-a-Service (2)



Example – Selling Remote Access as a Service



"While researching underground hacker marketplaces, the McAfee Advanced Threat Research team has discovered that access linked to security and building automation systems of a major international airport could be bought for only US$10.
The dark web contains RDP shops, online platforms selling remote desktop protocol (RDP) access to hacked machines, from which one can buy logins to computer systems to potentially cripple cities and bring down major companies.
RDP, a proprietary protocol developed by Microsoft that allows a user to access another computer through a graphical interface, is a powerful tool for systems administrators. In the wrong hands, RDP can be used to devastating effect. The recent SamSam ransomware attacks on several American institutions demonstrate how RDP access serves as an entry point. Attacking a high-value network can be as easy and cheap as going underground and making a simple purchase. Cybercriminals like the SamSam group only have to spend an initial $10 dollars to get access and are charging $40K ransom for decryption, not a bad return on investment."

Full story and details (July, 2018):
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/organizations-leave-backdoors-open-to-cheap-remote-desktop-protocol-attacks/

Nation States / State-Sponsored Actors

- Nation state employees and state-backed individuals or groups that act in the interest of a nation state
  - In contrast to hacker-for-hire actors, they usually operate in secret and support one nation state only
  - Main targets are state/military secrets, data on intelligence and capabilities to threaten the critical infrastructure (water, electricity, food, …) of opponents
- Tactics involve long-term and novel and highly sophisticated attack vectors
  - Zero-day vulnerability research and usage
  - Use of Advanced Persistent Threats (APT)
  - Supply chain attacks (indirect attacks)
  - Compromise of Industrial Control Systems (non-standard hard- and software)
  - Exploration and use of Artificial Intelligence to support their activities
  - Hack-and-leak (information warfare / public opinion)
- Trend: State-sponsored actors also engage in activities for personal gain
  - Blurring of the line between cyberespionage and cybercrime
- Challenges:
  - Activities are legal from the actor's perspective, sanctions and "name and shame" become more popular to deter opponents
  - Use of false flags, mimic other threat actors and use standard tools

Profile	
Motivation	Strategic objectives (espionage, competitive adv.)
Resources	High
Skill	High
Roles	User Dev/Op

Critical Infrastructure

What is considered to be part of the critical infrastructure of a nation varies slightly from country to country.

- **Switzerland:** The Federal Office for Civil Protection (FOCP) lists 9 sectors (energy, transportation, food and water, waste disposal, public safety, public health, finances, information & communication, public administration) divided into 27 sub-sectors as critical
  https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html
- **USA:** The Cybersecurity & Infrastructure Security Agency (CISA) of the US considers 16 sectors to be critical.
  https://www.cisa.gov/critical-infrastructure-sectors

Sanctions

In recent years, the EU has scaled up its resilience and its ability to prevent, discourage, deter and respond to cyber threats and malicious cyber activities in order to safeguard European security and interests.
In June 2017, the EU stepped up its response by establishing a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "**cyber diplomacy toolbox**"). The framework allows the EU and its member states to use all CFSP measures, including restrictive measures if necessary, to prevent, discourage, deter and respond to malicious cyber activities targeting the integrity and security of the EU and its member states.

In **July 2020**, the EU imposes the **first-ever sanctions** against cyber attacks. The EU Council decided to impose **restrictive measures** against **six individuals** and **three entities** responsible for or involved in various **cyber-attacks**. These include the attempted cyber-attack against the **OPCW** (Organisation for the Prohibition of Chemical Weapons) and those publicly known as **'WannaCry'**, **'NotPetya'**, and **'Operation Cloud Hopper'**.

The sanctions imposed include a **travel ban** and an **asset freeze**. In addition, EU persons and entities are forbidden from making funds available to those listed.

Source: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

Nation States / State-Sponsored Actors

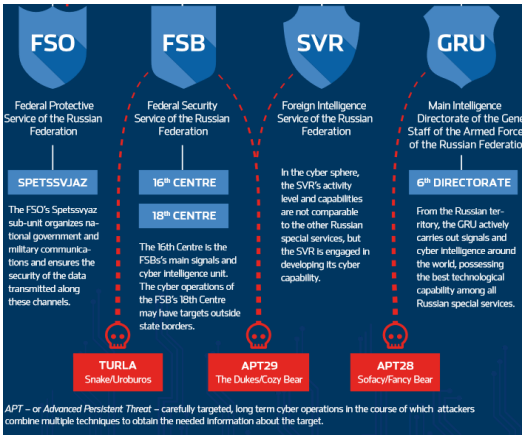
Many countries can and do carry out cyber-attacks, with a significant part being in the **area of intelligence/counter-intelligence**. Even within allies, **no clear no-spy policies exist**. Considering resources and budget availability, hostile cyber-activities of nation states (and corporations) are a severe threat that can cause **high defence costs**, while creating severe impact both at governmental and corporate levels. Main targets of this threat actor **are state secrets**, **military secrets**, **data on intelligence**, as well as threatening the **availability of critical infrastructures**. The degree to which performed attacks are successful can be considered as rather high. As it is the case with espionage in general, nation state activities aim at the creation of intelligence, strategic, psychological and political advantages.

Over time, many of these activities became known because the actors' activities were detected, the actors suffered data breaches or because of whistle blowers. Probably the most famous whistle blower is Etward Snowden (born June 21, 1983). He is an American former computer intelligence consultant who leaked highly classified information from the National Security Agency (NSA) in 2013, when he was an employee and subcontractor. His disclosures revealed numerous ***global surveillance programs***, many run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments and prompted a cultural discussion about national security and individual privacy.
See: https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present) for details.

Source: https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

Nation States / State-Sponsored Actors - Example

- SolarWinds hack (SUNBURST) – Attack on the supply chain
  - Compromise of SolarWind's Orion Plugin for its IT monitoring and management software
  - Compromise of customers via trojanized updates
  - Attribution: Russia
    - U.S./UK: Kremlin's APT29 ('cozy bear') crew
    - Kaspersky: Turla (resembles Kazuar malware from this crew)
- Timeline
  - 09/2019: Malicious code added to SolarWinds's Orion Software
  - 02/2020: Main phase of the attack and breach of nine U.S. government agencies and >100 companies
  - 06/2020: Attackers remove the SUNBURST malicious Code from SolarWinds systems.
  - 12/2020: Attack discovered and published by FireEye
- Some details:
  - Initial dormant period of up to two weeks
  - Retrieves and executes commands (e.g., transfer and execute files, profile the system, and disable services)
  - Masquerading: Orion Improvement Program (OIP) network protocol and plugin configuration files for storing data.
  - Use of multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.
  - See: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor



Source: http://web.archive.org/web/20191119034728/https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

SolarWinds hack:

- https://www.kiuwan.com/solarwinds-hack-timeline/
- https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor
- https://securelist.com/sunburst-backdoor-kazuar/99981/

More details on Russia's cyber espionage actors:

- http://web.archive.org/web/20191119034728/https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

Hacker-for-Hire Actors

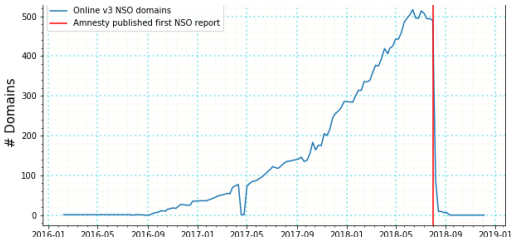
- Individuals or companies that offer offensive cyber capabilities
  - Vulnerability Research
  - Exploitation
  - Malware development
  - Technical command and control platforms
  - Operational Management
  - Training and Support
- Offerings bundled as a ready to be used service
  - Access-as-a-Service (AaaS)
  - Ransomware-as-a-Service (RaaS)
  - Phishing-as-a-Service (PaaS)
- Clients are usually governments (but not only)
  - Cyber espionage operations, get access to advanced offensive cyber capabilities
  - Get plausible deniability by using them as a proxy
- Challenges:
  - Hacker-for-hire companies operate legally in their country of operation
  - Prediction of activities difficult as it depends on the tasks their client's order
  - Use of false flags, mimic other threat actors and use standard tools

Profile	
Motivation	Work/Job
Resources	High
Skill	Professionals
Roles	Dev/Pro/Op

- **Access-as-a-Service (AaaS):** Get remote access to a certain infrastructure along with the required management tools
- **Ransomware-as-a-Service (RaaS):** Have ransomware and a dashboard to manage installations as software as a service
- **Phishing-as-a-Service (PaaS):** You must provide a list of targets and configure the phishing campaign according to your goals.

Hacker-for-Hire Actors - Example

- NSO Group Technologies
  - Israelian, founded in 2010, 750 employees (2021)
  - Mission: "NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe."
- Best known for Pegasus spyware:
  - C&C endpoints first disclosed in 2016 (Citizen Lab)
  - Various infection vectors seen over time
    - SMS messages with links to exploit domains
    - Network injection, e.g., alter the target domain
      - Collaboration with network operator or using rogue cell towers (2018/19, Morocco)
    - Zero-click – No user interaction required
      - E.g., 07/2021 zero-day for fully patched iPhone 12
- NSO group's customers use Pegasus for spying on government critics, journalists, politicians
  - Usage in Switzerland legal for law enforcement since 2018 (rev. BÜPF). 12 (2019), 13 (2020)
- Future unclear, lawsuit(s) and bans
  - E.g., WhatsApp sued NSO group in the US



Registration dates of domains attributed to Pegasus C&C infrastructure. Identification possible because of unique set of TLS cipher suites (similar to JA3S fingerprint). Internet-wide scan in 2018.

Source: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

BÜPF: Federal Act on the Surveillance of Post and Telecommunications
- In German: **B**undesgesetz betreffend die **Ü**berwachung des **P**ost- und **F**ernmeldeverkehrs

Main source for this slide:
- https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Other good reads:
- Political dimension: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
- Pegasus and Switzerland (in German, use translator): https://www.watson.ch/digital/schweiz/898591433-so-haeufig-verwendet-die-schweiz-israelische-spyware-vom-typ-pegasus

Hacktivist Actors

- Individuals or loosely organized groups or networks of activists (e.g., Anonymous) who use cyberspace to debate and drive social, political or other change
  - Criminals or saviors? Depend on which side you are
  - Honker Union vs. Anonymous?
    - Both sides use the same, usually illegal tactics
- Tactics usually old school and focusing on:
  - Disrupt availability - (Distributed) Denial of Service attacks
  - Defacements - modify visual appearance websites
  - Release sensitive data
- Challenges:
  - Activity is hard to predict because it is driven by events (local, regional, and global, e.g., war in Ukraine)
  - Crowd-sourcing and attracting public participation has the potential of a huge leverage for their activities
  - Movements in the domain of environmental protection, anti-war, and anti-discrimination are likely to develop/strengthen hacktivism side-tactics

Profile	
Motivation	Work
Resources	Low*
Skill	Low to Medium
Roles	User [Dev/Pro/Op]

Honker Union: A group known for hacktivism, mainly present in China. Literally the name means "Red Guest", as compared to the usual Chinese transliteration of hacker.
Source and more details: https://en.wikipedia.org/wiki/Honker_Union

Anonymous: A decentralized international activist- and hacktivist collective and movement primarily known for its various cyberattacks against several governments, government institutions and government agencies, corporations and the Church of Scientology.
Source and more details: https://en.wikipedia.org/wiki/Anonymous_(hacker_group)

Hacktivists - Example

- Various hacks by Swiss hacktivist Tillie Kottmann (they/them) and their collective Advanced Persistent Threat 69420
- Verkada «Hack»:
  - Footage from more than 150,000 of the companies' surveillance cams exposed
  - Cams in prisons, hospitals, schools, police stations, and companies (e.g., cams in Tesla factories)
- Methods used:
  - Google dorking (see pentesting)
  - Credentials for privileged login found publicly exposed on the Internet (from a code repository?
- Consequences*:
  - Raid by Swiss authorities in 03/2021 but was related to another hack by them
  - Charged by the U.S. DOJ for breaking into several organizations and publishing and disclosing information thereby acquired

- Motivation

  "lots of curiosity, fighting for freedom of information and against intellectual property, a huge dose of anti-capitalism, a hint of anarchism — and it's also just too much fun not to do it"

  "I don't want to help companies," … "The whole hacker thing, in my opinion, should be more about trying to improve the world"
- Methods

  "Why do complex things when you can do things that require absolutely zero effort?"

  (T. Kottmann)

DOJ = Department of Justice

***Consequences**

The raid in Switzerland and the charges by the DOJ include different hacking/break-in activities from 2019 to 2021. The Verkada «Hack» was not (yet?) part of the charges. Among the more critical charges are the break-in into Intel and the publication of 20 GB of source code and other documents from Intel.

Sources:

- https://www.theverge.com/2021/3/19/22339625/tillie-kottmann-swiss-hacker-verkada-charged-us-government-verkada
- https://www.swissinfo.ch/eng/bloomberg/swiss-police-raid-apartment-of-verkada-hacker--seize-devices/46444018
- https://www.republik.ch/2021/04/21/die-vereinigten-staaten-gegen-tillie-kottmann (in German)

Insider Actor

- Types of activities:
  - Unintentional threats – e.g., lax handling of security procedures
    - Address with Data Leak Prevention (DLP)
  - Intentional threats – e.g., steal or leak information or sabotage
- Challenges
  - They have legitimate access to systems
  - They know the protections in place
- Important:
  - Identify unhappy employees
  - Spot knowledge-gaps to lower risks from unintentional threats
  - Monitor for unusual activities and limit access

Profile	
Motivation	Extortion, revenge, sabotage or profit
Resources	Low
Skill	Low to Medium
Roles	User

Employees (current, ex, internal and external): Motivated by extortion, revenge, sabotage or profit, this group has a significant role in the materialisation of cyber threats, especially those that lead to data breaches. Referred to as Insider Threat, this threat group embraces both own and contracted employees, i.e. staff, contractors, operational staff, former employees, etc. Threats emanating from this target group may be both intentional and unintentional (i.e. i.e. lax handling of security procedures, user error or even malicious intent). The effort required to protect assets against such threats can be quite high. Therefore it is important to identify employee unhappiness, spot knowledge-gaps and get alerted when attacks abuse publicly unknown vulnerabilities.

Some other infamous Threat Actors

- Scrippt Kiddy
  - Runs stuff without knowing (much) about stuff
  - Use of free or purchased hacking tools and services
  - *-as-a-Service might contribute toward more activity of this threat actor
  - Offer alternatives to learn and have fun, e.g., cyber challenges/competitions
- Cyber Terrorists
  - Narrow: Deployments of disruption attacks against information systems for the primary purpose of creating alarm and panic by known terrorist organizations
    - no significant event until now
  - Broad: Intentional use of computer, networks, and public internet to cause destruction and harm for political or ideological objectives
  - No commonly accepted definition exists
  - Might become more of a problem in the near future
- Question: Can script kiddy carry out an SQL injection attack?

Script Kiddies: This target group consists of young individuals who might be thrilled about achievements and skills of tech savvy individuals who assumedly gave a lesson to persons, organisations or brands considered outrageous. Due to the ease of obtaining malicious tools, tech savvy teenagers might purchase and use them. Consequently, due to potentially low level of knowledge about the use of hacking tools, low threshold of self-control, overestimation of own skills and the consequences of their activities, script kiddies may achieve great impact.

Cyber Terrorists: The cyber terrorist threat agent is a controversial one and sometimes confused with cyber fighters or hacktivists. Depending on how narrowly one interprets the term, there are no publicly known attacks by this threat agent.

- *Narrow:* deployments of disruption attacks against information systems for the primary purpose of creating alarm and panic **by known terrorist organizations**
- *Broad*: intentional use of computer, networks, and public internet to cause destruction and harm for political or ideological objectives

Supposedly, cyber terrorists are targeting large-scale sabotage to harm national security and society, mainly aiming at critical infrastructure. Characteristic of this threat agent group is the indiscriminate use of violence in order to influence decisions/actions of states towards their politically or relationally motivated objectives. However, a clear and **commonly accepted definition** of this threat agent **does not seem to exist**.

Threats

Knowing the Threats – Why?

- As a basis to draw a roadmap with aspects that need to be addressed in the future by policy, businesses and research
- Learn about new threats and their attack vectors
  - CEO/CIO and co.
    - Are there developments that change risks relevant to the business?
  - CISO:
    - What to focus on in security trainings / awareness trainings
    - Do we need new security controls?
    - Do we need to modify existing security controls?
  - Security operations expert:
    - Do we need to modify existing security controls?
    - Do we need to search for new patterns and evidence?
    - What are indicators of a threat/attack vector?

What threats are there?

- Threat taxonomy to the rescue - a threat taxonomy is a classification of threat types at various levels of detail
  - Fosters common understanding and language for talking about threats
- There is not one but many taxonomy proposals:
  - Open Threat Taxonomy
  - ENISA Threat Taxonomy
  - NIST Risk Assessment Threat Exemplary
  - Taxonomy of Operational Cyber Security Risks
  - The Cambridge Risk Framework
  - …
- All have their pros and cons, very difficult to have a one-fits-all taxonomy
  - Check out https://csiac.org/articles/evaluation-of-comprehensive-taxonomies-for-information-technology-threats/
- Here: We won't look at a taxonomy but you will study the most relevant threats in the lab about the ENISA Threat Landscape Report

Before talking about threats, it makes sense to make sure that people have a **common understanding** of threats and the types of threats.

A **threat taxonomy** is a classification of threat types and threats at various levels of detail. The purpose of such a taxonomy is usually to establish a point of reference for threats encountered, while providing a possibility to shuffle, arrange, amend and detail threat definitions. To this extend, a threat taxonomy is a living structure that is being used to maintain a consistent view on threats on the basis of collected information.

Example – Open Threat Taxonomy

PHYSICAL THREATS

Includes:
Threats to the confidentiality, integrity, or availability of information systems that are physical in nature. These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.

RESOURCE THREATS

Includes:
Threats to the confidentiality, integrity, or availability of information systems that are the result of a lack of resources required by the information system. These threats often cause failures of information systems through a disruption of resources required for operations.

PERSONNEL THREATS

Includes:
Threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization's personnel. These threats can be the result of deliberate or accidental actions that cause harm to information systems.

TECHNICAL THREATS

Includes:
Threats to the confidentiality, integrity, or availability of information systems that are technical in nature. These threats are most often considered when identifying threats and constitute the technical actions performed by a threat actor that can cause harm to an information system.

Threat ID	Threat Action Name	Threat Rating
TEC-007	Credential Discovery via Sniffing	4.0
TEC-008	Credential Discovery via Brute Force	4.0
TEC-009	Credential Discovery via Cracking	4.0
TEC-010	Credential Discovery via Guessing	2.0
TEC-011	Credential Discovery via Pre-Computational Attacks	3.0
TEC-012	Misuse of System Credentials	3.0
TEC-013	Escalation of Privilege	5.0
TEC-014	Abuse of System Privileges	4.0
TEC-015	Memory Manipulation	4.0
TEC-016	Cache Poisoning	3.0
TEC-017	Physical Manipulation of Technical Device	2.0
TEC-018	Manipulation of Trusted System	4.0
TEC-019	Cryptanalysis	1.0
TEC-020	Data Leakage / Theft	3.0
TEC-021	Denial of Service	2.0

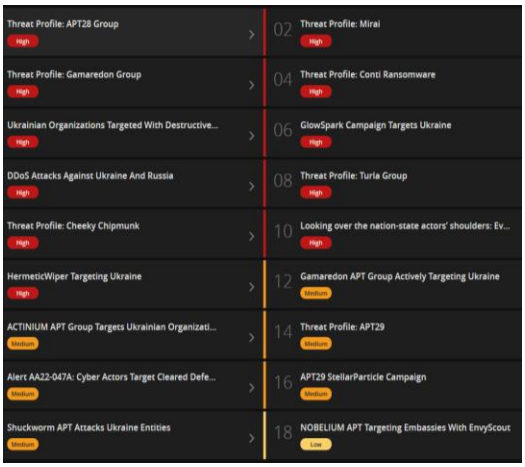
Threat Landscape
Sources of Information

Sources of Information – Long Term

- Threat reports published once or a few times per year
  - To make strategical/tactical decisions
- Many such reports exist
  - ENISA Threat Landscape Report
  - Fortinet Threat Landscape Report
  - Bitdefender Threat Debrief
  - Proofpoint Threat Report
  - McAfee Enterprise Advanced Threat Research Report
  - …
- Some reports describe threats only and do not assess the threat landscape as a whole

Sources of Information – Short Term (1)

- Focus on old-school "Real-time" information
  - Articles on news portals
    - News articles with information on new threats
    - Heise Security, DarkReading
  - Security mailing lists
    - E.g., signup to lists related to your software and hardware products
- Threat intelligence service providers
  - Advisories and actionable information in text and machine readable form
    - E.g., advisories from Computer Emergency Response Teams (CERTS)
    - E.g., threat information feed from the Open Threat Exchange platform OTX
  - Web-pages with real-time information on current threats
    - E.g., the McAfee MVISION Insights (=>) https://www.mcafee.com/enterprise/en-us/lp/insights-preview.html



Sources of Information – Short Term (2)

- Threat intelligence platforms
  - Aggregation and correlation of threat data from threat intelligence service providers
  - Actionable/machine readable data to be fed to systems like IDS/IPS or a SIEM
    - E.g., actionable information on threat actors (domain, IP address,…)
  - Exchange data formats:
    - Structured Threat Information Expression (STIX)
    - Trusted Automated Exchange of Indicator Information (TAXII)
    - … and many more …

Some of the frameworks, tools, standards, and working groups to be considered for exchanging threat intelligence are, as follows:
OpenIOC – Open Indicators of Compromise framework
VERIS – Vocabulary for Event Recording and Incident Sharing
CybOX – Cyber Observable eXpression
IODEF – Incident Object Description and Exchange Format
TAXII – Trusted Automated eXchange of Indicator Information
STIX – Structured threat Information Expression
MILE – Managed Incident Lightweight Exchange
TLP – Traffic Light Protocol
OTX – Open Threat Exchange
CIF – Collective Intelligence Framework

Source: https://nigesecurityguy.wordpress.com/tag/stix/

Threat Landscape
APT and Cyber Kill Chain

Advanced Persistent Threats (APT)

- Advanced – Use of advanced technologies and techniques
  - Penetrate existing defences
    - e.g., using vulnerabilities known to the attacker only
  - Operators develop more advanced tools as required
  - Multiple targeting methods, tools, and techniques to reach and compromise a target and maintain access to it
- Persistent
  - Maintain long-term access
  - Keep trying until it gets in / achieves its goals
    - For example: Lateral movement wait for suitable vulnerability => Why wait for a "public" vulnerability?
  - Hides from detection until it attains its objective
- Threat
  - Coordinated human actions, not mindless and automated pieces of code
  - Operators have a specific objective, are skilled, motivated, organized and well-funded

Note that definitions of precisely what an APT is can vary. Also note that depending on the definition of APT, almost no APT's are known. By definition they are very hard to detect.

Most of the time, when people talk about APTs, they are actually referring to **Advanced Targeted Attacks (ATA)** – An attack tailored to a certain target system or person but usually without the persistency part and with a (much) lower sophistication level than APTs.

The following provides a summary by their named requirements:

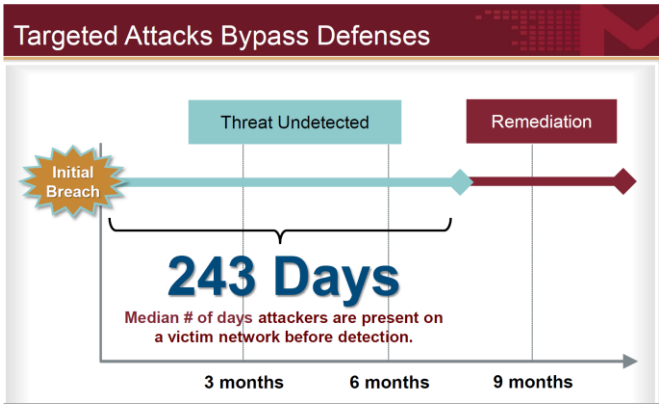
- Advanced – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to

it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.

- Persistent – Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task.

- Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded.

APTs - How Bad is it?



Cyber Kill Chain

- Preparation and execution of a «typical» attack follows the Cyber Kill Chain
  - Developed by Lockheed Martin
  - The model identifies what the adversaries must complete in order to achieve their objective
  - Intrusion-centric - Does not easily fit all types of attacks
- Illustrates Defender advantage:
  - An attack is only successful, if all steps are successful
  - Defenders can (try to) disrupt the chain at any step
- Tool to think about suitable defensive measures for the different steps/stages of an attack

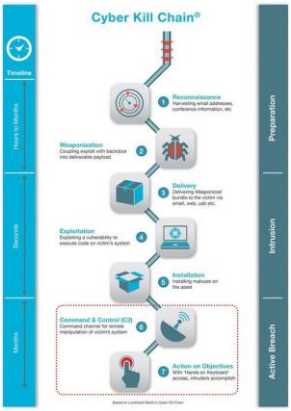


Image source: http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542

Kill Chain (Origin)

The term **kill chain** is a military concept which identifies the structure of an attack. It consists of:

- Identification of target
- Dispatching of forces to target
- Initiation of attack on target
- Destruction of target

Conversely, the idea of "breaking" an opponent's kill chain is a method of defense or preemptive action.

Source: https://en.wikipedia.org/wiki/Kill_chain

Critique on Cyber Kill Chain and the Unified Kill Chain

Among the critiques of Lockheed Martin's cyber kill chain model as threat assessment and prevention tool is that the first phases happen outside the defended network, making it difficult to identify or defend against actions in these phases. Similarly, this methodology is said to reinforce traditional perimeter-based and malware-prevention based defensive strategies. Others have noted that the

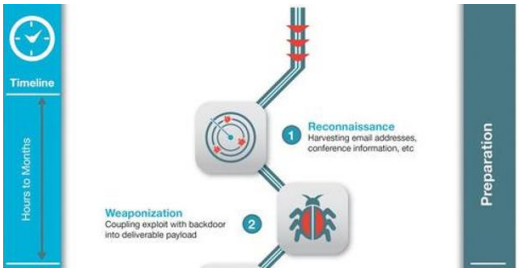
traditional cyber kill chain isn't suitable to model the insider threat. This is particularly troublesome given the likelihood of successful attacks that breach the internal network perimeter, which is why organizations "need to develop a strategy for dealing with attackers inside the firewall. They need to think of every attacker as potential insider".

The unified kill chain consists of 18 unique attack phases that can occur in advanced cyber attacks. The Unified Kill Chain was developed in 2017 by Paul Pols in collaboration with Fox-IT and Leiden University to overcome common critiques against the traditional cyber kill chain, by uniting and extending Lockheed Martin's kill chain and MITRE's ATT&CK framework. The unified version of the kill chain is an ordered arrangement of 18 unique attack phases that may (or may not) occur in end-to-end cyberattack, which covers activities that occur outside and within the defended network. As such, the unified kill chain improves over the scope limitations of the traditional kill chain and the time-agnostic nature of tactics in MITRE's ATT&CK. The unified model can be used to analyze, compare, and defend against end-to-end cyber attacks by advanced persistent threats (APTs). A subsequent whitepaper on the unified kill chain was published in 2021 (https://www.unifiedkillchain.com/).

Source: https://en.wikipedia.org/wiki/Kill_chain

The Way of the Hacker - Preparation

- Step 1: Reconnaissance
  - Gathers information on the target before the actual attack starts
    - Looking for publicly available information on the Internet
- Step 2: Weaponization
  - Uses an exploit and create a malicious payload to send to the victim

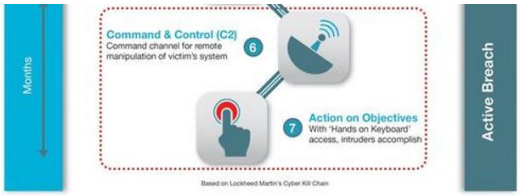


The Way of the Hacker - Intrusion

- Step 3: Delivery
  - The attacker delivers the malicious payload to the victim (e.g., using Email, USB sticks, a website or other means)
- Step 4: Exploitation
  - Exploitation of a vulnerability to automatically execute the delivered payload
  - Only relevant when the attacker uses an exploit to execute the malicious payload
- Step 5: Installation
  - Installation of malware on the victims machine (can be in-memory only)
  - Only relevant if the attacker uses malware as part of the attack

The Way of the Hacker

- Step 6: Command and control
  - Creation of a command and control channel to continue to operate internal assets remotely.
  - This step is relatively generic and relevant throughout the attack, not only when malware is installed.
- Step 7: Action on objectives
  - Steps to achieve the actual goals inside the victim's network.
  - This is the elaborate active attack process that can take months, and hundreds of steps, in order to achieve the objectives.



Summary

- Many different threat agents exist with different motivations, tactics, skill levels, resources, and roles
- Organizations must consider what threat agents are likely to be most relevant to their business
- Information on the threat landscape is available in many forms and helps to plan and organize current and future defensive measures
- The cyber kill chain explains the different steps and phases of an attack; to "kill" an attack, defenders can kill it at any of the steps
- Advanced Persistent Threat => You're hacked…
- Threats: The threat landscape gets more complex
  - Actors get smarter and change tactics
  - Not a fair game (?):
    - Attacker - Find one security hole
    - Defender – Find and fix all of them

c't, Thomas SAUR