# H1 Adversarial mindset

## Summarizing Hutchings Kill Chains (Hutchings, Cloppert, Rohan)

* Advanced Persistent Thread (APT) is the newest techniques to break through economic, proprietary or national security to achieve substantial benefits by fraud.
* Kill chain the most known attack types are email attachments, web pages and removable USB.
* The “kill chain” means in this case of structure of intrusion and model to corresponding model to analysis and inform actionable security intelligence.
* Intelligence-driven CND is risk management strategy against the “kill chain” kind of threats.
* Kill chain is a process to get adversary doing desired actions.
* Collect data against adversaries, to improve intrusion protection.
* It is important to see what is on intruder mind to identify threats.
* One of the most common intrusion method is email attack.

## Summarizing ATT&CK Enterprise matrix (Mitre ATT&CK)

* ATT&CK is knowledge place of cyber adversary’s attack methods and actions.
* ATT&CK covers two different aspects such as Enterprise or mobile attacks.
* ATT&CK has large, collected database which is directed to improve enterprises information security.

## Compering the solutions

Both methods try to strive adversary’s mindset and that way gather and develop methods to prevent attacks. The most important question using the models are to keep up with attacker’s mind and try to bypass it to make attackers’ attempts useless.

Based on the documents the Kill chain methods relies more of reveal the attacker’s mindset and develop methods by that way. ATT&CK is targeted more like Enterprise or mobile system’s whilst Kill chain is used by institutions such as national security and highly sensitive economy. The ATT&CK Enterprise matrix is a set of already made techniques which are directed to enterprises to improve their information security.

The models based same kind of ideas but are targeted little bit different audiences. For better or for worse, the benefit of the models goes to both adversaries and enterprises, institutions and every else who use the methods to prevent attacks.

At technical point of view seems like ATT&CK Enterprise matrix is focused on cloud systems as well, but there could be more deeply covered cloud sections. There is own information for Microsoft Azure, but still there would more comprehensive areas of other cloud vendors. Still, I would hope to see more information of nowadays technologies and how does the models are focused those ones.

## Incidents analyze: EP 111: ZeuS

This topic is about to analyze one of the most known banking trojan ZeuS with Kill Chain matrix. The story begins when young Russian guy who used alias Slavik was following the internet and online banking processes for long time seeking money to steal. After a while, he started building malicious code which seeks usernames and password from the user systems to send them back to the hacker. The Hacker sending the ZeuS through spam emails into victim’s computer. When installed, it seeks banking account details such as usernames and passwords and many other information to send them back to the hacker’s computer. The original malware was spread and reused to develop itself even worse.

At some point Slavik has gotten more contacts from other adversaries. They developed malware to a spy and use botnets for spreading the ZeuS. The malware had many different names, but eventually it was named ZeuS by the creek mythology and it was called the god of all banking viruses. The trojan was used by hacker during victim’s banking session. The money transfer into hacker’s bank accounts happened same time as victim does the banking business online.

From the starting point, the malware has developed a lot and had got multiple features to develop and spread all over the world. Even so, the hackers may decide what kind of things the malware do in certain cases in victim’s computer. At some point Slavik sell copies of the Zeus per 3000$. Even 5000 customers bought it. FBI started investigating the cases when victims noticed that money had lost from their bank accounts. After all, the trojan horse ZeuS has developed a huge and complex which was able to hack very complex systems and securities. Slavik had three different ways to make money with ZeuS: steal banking details, renting out the botnet and selling copies of the ZeuS(EP 111).

## Sources:

EP 111: ZEUS, 2022, [ZeuS – Darknet Diaries](https://darknetdiaries.com/episode/111/) Read: 30.10.2022

Hutchings, E. Cloppert, M. Rohan, M. Lockheed Martin Corporation, Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, [LM-White-Paper-Intel-Driven-Defense.pdf (lockheedmartin.com)](https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf), Read: 29.10.2022

Mitre ATT&CK, 2022, [Matrix - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/matrices/enterprise/)