

# **General forms of threats, perpetrators and tools**

---

## Table of contents

<b>1</b>	<b>Foreword</b> .....	Fehler! Textmarke nicht definiert.
<b>2</b>	<b>Threats</b> .....	Fehler! Textmarke nicht definiert.
<b>3</b>	<b>Classification of attackers</b> .....	Fehler! Textmarke nicht definiert.
<b>3.1</b>	<b>Advanced persistent threats (APTs)</b> .....	Fehler! Textmarke nicht definiert.
<b>3.2</b>	<b>Cybercriminal organisations – targeted attacks</b> .	Fehler! Textmarke nicht definiert.
<b>3.3</b>	<b>Cybercriminal organisations – opportunistic attacks</b> .....	Fehler! Textmarke nicht definiert.
<b>3.4</b>	<b>Hactivists</b> .....	Fehler! Textmarke nicht definiert.
<b>3.5</b>	<b>Individual perpetrators</b> .....	Fehler! Textmarke nicht definiert.
<b>4</b>	<b>Attack tools</b> .....	Fehler! Textmarke nicht definiert.

# 1 Foreword

This document provides an overview of common forms of threats and their classification, as well as the types of perpetrators behind these threats.

## 2 Threats

Threats from the internet to private individuals and private and public organisations are very diverse. The following pyramid represents a rough categorisation:

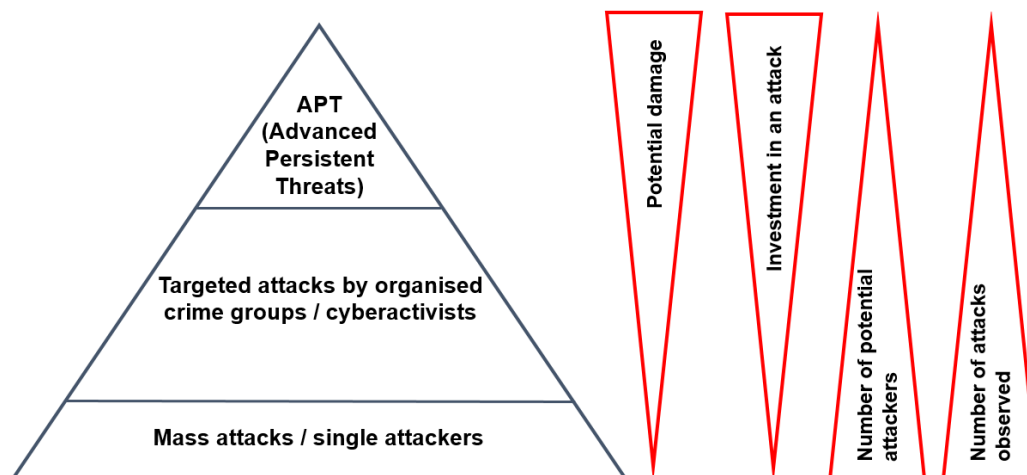


Figure 1: Simplified representation of the threat pyramid according to SANS<sup>1</sup>, Recorded Future<sup>2</sup>

At the top of the pyramid are the APTs (advanced persistent threat). This threat potentially causes a very high level of damage to an individual organisation or, in a political context, to the security interests of entire countries. Attackers are prepared to invest a great deal of time, money and knowledge in the attack and usually has large resources at their disposal. The attacker's aim is often to remain undetected for as long as possible and to entrench himself in the victim's network and thus obtain a constant flow of information that is of interest to him or her. In rare cases, sabotage (attempts) also takes place. There is a limited but steadily growing number of attackers in this category due to the high demand on resources and skills.

In the middle of the pyramid are cybercriminals and cyberactivists. Even though they usually have fewer resources at their disposal, the threat they represent should not be underestimated. As a rule, both the target selection and the attackers' persistence are lower than for APTs. It should be noted that the line between organised cybercrime and APTs is blurred. State attackers are also likely to use services on the cybercrime market to achieve their desired goals. In addition, state actors also commission cybercriminal organisations in order to be able to successfully deny their involvement in the event of detection.

The lowest level of the pyramid is made up of opportunistic mass attacks as well as individual perpetrators. Despite the limited resources used for such attacks, this threat alone is to be taken seriously due to the enormous volume of such attacks. Here, too, the line to the upper level is permeable, since mass attacks in particular are often carried out or at least commissioned by cybercriminal organisations. The permeability between the individual levels also shows that the underground market is organised according to the division of labour along the lines of a classic demand and supply market.

<sup>1</sup> [www.sans.org](http://www.sans.org)

<sup>2</sup> <https://www.recordedfuture.com/assets/prioritizing-cyber-threats-1.png>

### 3 Classification of attackers

In the following, attackers are classified according to their capabilities and motivation. This compilation serves to classify which aims an attacker could pursue with which resources and which level of persistence. It is a rough approximation with no claim to be exhaustive.

#### 3.1 Advanced persistent threats (APTs)

<b>Name</b>	State actors / advanced persistent threats /
<b>Description</b>	States or players with a mostly state connection act as attackers or commission the attack. As a rule, the purpose of these attacks is to obtain information within the scope of classic espionage or industrial espionage. In times of heightened political tensions or crises, attacks on critical infrastructures or targeted disinformation may also occur.
<b>Motivation</b>	Information gathering, disruption of critical infrastructures, influence campaigns
<b>Technical resources</b>	Countries and state-related actors are likely to have all the necessary technical capabilities at their disposal. The availability of resources can be classified as very high. At the same time, specialists in a wide variety of areas are available or can be recruited quickly.
<b>Financial resources</b>	Very high, as long as the expected result of the attack justifies the use of the financial resources from the attacker's point of view.
<b>Rationality of approach</b>	High
<b>Level of persistence</b>	High
<b>Starting points for defence</b>	<ul style="list-style-type: none"> <li>• Investment (including human resources) in detection</li> <li>• Increased visibility on end-user devices</li> <li>• Segmentation and monitoring of networks and all systems</li> <li>• Protection of the Active Directory</li> <li>• Use of tools such as AppLocker to execute only signed macros</li> <li>• Central security gateways through which all traffic must flow</li> <li>• Blocking of dangerous file types on gateways</li> <li>• Separation of sensitive tasks and browsing/emails</li> <li>• End-to-end two-factor authentication</li> <li>• Prompt and monitored patch management</li> <li>• Effective backup/recovery concept with offline and offsite backups in several generations</li> </ul>
<b>Starting points for prosecution</b>	Detailed analysis of attacks to enable attribution; internationally coordinated investigations are necessary. These may be influenced by political interests.
<b>Resistance to prosecution</b>	Very high
<b>Likely attack targets</b>	<ul style="list-style-type: none"> <li>• Systems with sensitive information</li> <li>• Business-critical information</li> <li>• Systems of key individuals or decision-makers</li> </ul>

- Backdoors in inconspicuous systems that are difficult to detect
- Targeted attacks on the confidentiality and integrity of systems.
- Attacks on the availability of critical systems, in the event of heightened political tensions or crises.
- Critical infrastructures

### 3.2 Cybercriminal organisations – targeted attacks

<b>Name</b>	Cybercriminal organisations – targeted attacks
<b>Description</b>	Cybercriminal organisations can conduct targeted attacks that are similar to an APT. They may attack governmental or private organisations with the aim of obtaining information to resell or use to their advantage. Very common targets include financial transaction systems. ATM cash-out attacks are a good example. Attacks with encryption Trojans are financially very lucrative from the attackers' point of view, which is why a shift towards such attacks has been observed recently. The attackers copy the data before encrypting it and threaten to sell it if the ransom demanded is not paid.
<b>Motivation</b>	Blackmail, obtain and sell information (industrial espionage), use financial transaction systems for their own purposes.
<b>Technical resources</b>	Medium to high, depending on the organisation
<b>Financial resources</b>	Medium to high, depending on the organisation
<b>Rationality of approach</b>	High
<b>Level of persistence</b>	Medium
<b>Starting points for defence</b>	<ul style="list-style-type: none"> <li>• Investment (including human resources) in detection</li> <li>• Increased visibility on end-user devices</li> <li>• Segmentation and monitoring of networks and all systems</li> <li>• Protection of the Active Directory</li> <li>• Use of tools such as AppLocker to execute only signed macros</li> <li>• Central security gateways through which all traffic must flow</li> <li>• Blocking of dangerous file types on gateways</li> <li>• Separation of sensitive tasks and browsing/emails</li> <li>• End-to-end two-factor authentication</li> <li>• Prompt and monitored patch management</li> <li>• Effective backup/recovery concept with offline and offsite backups in several generations</li> </ul>
<b>Starting points for prosecution</b>	Analysis of attack tools and infrastructure used, close cooperation with relevant police organisations and other intelligence services. Monitoring of current cybercriminal organisations.
<b>Resistance to prosecution</b>	Medium to high. However, prosecution disrupts attackers' activities, and they therefore try to stay under the radar of prosecution authorities
<b>Likely attack targets</b>	<ul style="list-style-type: none"> <li>• Systems with high availability requirements</li> <li>• Systems with confidential information that has a high resale value</li> </ul>

- 
- Systems with financial information
- 

### 3.3 Cybercriminal organisations – opportunistic attacks

<b>Name</b>	Cybercriminal organisations, opportunistic and non-targeted attacks
<b>Description</b>	This is cybercrime in its classic form. The attackers try to generate financial gain by attacking end-user devices. For example, they try to obtain access data, blackmail victims with DDoS attacks or send spam via infected devices. "Crimeware-as-a-service" (CaaS), which is traded on the black market, is often used for this purpose.
<b>Motivation</b>	Solely financial
<b>Technical resources</b>	Medium, attack components are often purchased as "crimeware-as-a-service" (CaaS)
<b>Financial resources</b>	Medium to high
<b>Rationality of approach</b>	High
<b>Level of persistence</b>	Low against individual targets
<b>Starting points for defence</b>	<ul style="list-style-type: none"> <li>• Investment (including human resources) in security</li> <li>• Use of security gateways, blocking of dangerous file types on gateways</li> <li>• Separation of sensitive tasks and browsing/emails</li> <li>• Two-factor authentication for all resources accessible via the internet</li> <li>• Prompt and monitored patch management</li> <li>• Effective backup/recovery concept with offline and offsite backups in several generations</li> </ul>
<b>Starting points for prosecution</b>	Sinkholing of relevant domains used for cybercriminal organisations. Analysis of the infrastructure and attack tools used. Analysis and prevention of relevant cash flows.
<b>Resistance to prosecution</b>	Medium to high. The international nature of most incidents makes efficient investigation difficult.
<b>Likely attack targets</b>	<ul style="list-style-type: none"> <li>• Poorly protected end-user devices</li> <li>• E-banking applications</li> </ul>

### 3.4 Hacktivists

<b>Name</b>	Hactivists, cyberactivists
<b>Description</b>	Cyberactivists use digital means to protest against decisions made by governments or companies that are not in line with their political and social interests. Examples of such groups include "Anonymous" and "LULZ".
<b>Motivation</b>	Disseminate own views and initiate discussions, gain attention and/or cause damage.
<b>Technical resources</b>	Technical resources and capabilities vary greatly. In the case of large-scale campaigns with a high level of interest, however, they can assume very considerable proportions.

<b>Financial resources</b>	Limited, but not of great importance to the attacker because these activities are usually conducted on a voluntary basis.
<b>Rationality of approach</b>	Low to medium, depending on the organisational form of the groups.
<b>Persistence</b>	Medium
<b>Starting points for defence</b>	<ul style="list-style-type: none"> <li>• Investment (including human resources) in security</li> <li>• Use of security gateways, blocking of dangerous file types on gateways</li> <li>• Separation of sensitive tasks and browsing/emails</li> <li>• Two-factor authentication for all resources accessible via the internet</li> <li>• Prompt and monitored patch management</li> </ul> <p>Effective backup/recovery concept with offline and offsite backups in several generations</p>
<b>Starting points for prosecution</b>	Cooperation with police organisations and intelligence services.
<b>Resistance to prosecution</b>	Medium
<b>Likely attack targets</b>	<ul style="list-style-type: none"> <li>• Systems with high visibility/level of attention</li> <li>• Availability of systems (DDoS), integrity (website defacements)</li> </ul>

### 3.5 Individual perpetrators

<b>Name</b>	Individual perpetrators
<b>Description</b>	Individual perpetrators act on their own initiative, with limited resources.
<b>Motivation</b>	Varies from individual to individual
<b>Technical resources</b>	Low
<b>Financial resources</b>	Low
<b>Rationality of approach</b>	Varies from individual to individual
<b>Persistence</b>	Low to high, depending on the attacker
<b>Starting points for defence</b>	<ul style="list-style-type: none"> <li>• Investment (including human resources) in security</li> <li>• Use of security gateways, blocking of dangerous file types on gateways</li> <li>• Separation of sensitive tasks and browsing/emails</li> <li>• Two-factor authentication for all resources accessible via the internet</li> <li>• Prompt and monitored patch management</li> <li>• Effective backup/recovery concept with offline and offsite backups in several generations</li> </ul>
<b>Starting points for prosecution</b>	Normal criminal prosecution
<b>Resistance to prosecution</b>	Low
<b>Likely attack targets</b>	<ul style="list-style-type: none"> <li>• Poorly protected systems in the case of "script kiddies"</li> <li>• Easily visible targets with high level of attention in the case of defacement campaigns</li> </ul>

## 4 Attack tools

In addition to a variety of tools (port scanners, penetration testing tools, etc.) that can serve equally legitimate purposes, there are several specifically malicious tools. All of these have in common that they are used at all levels of the pyramid (see chapter on Threats).

MITRE's knowledge base "ATT&CK" (<https://attack.mitre.org/>) provides an overview of tactics, techniques and procedures used in cyberattacks.

Malware is used to implement these tactics, techniques and procedures. MITRE maintains an extensive list of such malware (<https://attack.mitre.org/software/>).