EuRepoC

ADVANCED PERSISTENT THREAT profile

Threat Level Index

The Threat Level Index used for the APT profiles is a composite indicator compiling five individual sub-indicators into a single index:

(1) Intensity of the APT's attacks
(2) Sectorial scope of the APT's attacks
(3) Geographical scope of the APT's attacks
(4) Frequency of the APT's attacks
(5) Use of zero days

Methodology:

Each of the five sub-indicators is calculated using data from the EuRepoC database of cyber incidents. Only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. That is, cyber incidents that a) affected political or state actors/institutions, b) have been associated with state-actors as the actual "masterminds," or c) have been "publicly politicized, regardless of the affected target". Each APT may therefore be responsible for many additional cyber incidents that were not publicly reported nor had a political dimension.

(1) Intensity of the APT's attacks

This indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity (see here)

The average is subsequently converted to a five-level scale:

Average "Weighted Cyber Intensity" between:	Converted score:
0-3	1
3-6	2
6-9	3
9-12	4
12-15	5

By Camille Borrett
with contributions from Jakob Bund and Kerstin Zettl-Schabath

October 2022

(2) Sectorial scope of the APT's attacks

This indicator is calculated in two steps:

a) The average number of (unique) targeted sectors per attack attributed to the APT is calculated. This average is then converted to a four-level scale.

Average number of targets per incident:	Converted score:
≤ 1	1
>1 - ≤1.45	2
>1.45 - ≤1.7	3
>1.7	4

This scale accounts for the practice of other APT groups, as it is based on the quartiles of the scores of all APTs covered by EuRepoC between 2000 and May 2022. Quartiles divide a range of data into four equal parts. Around 25% of the values in a range of data are below the first quartile, while approximately 25% are above the third quartile. In this case, this means that all averages below 1 represent the 25% lowest scores across the APTs covered by EuRepoC, while averages above 1.69 represent the 25% highest scores.

b) Multipliers are introduced to account for the broader societal impact of the APTs targets, weighing targets critical for the functioning of societies higher. If the majority of attacks attributed to the APT group targeted state institutions/political systems and/or critical infrastructure, the score obtained in step (a) is multiplied as follows:

Percentage of attacks targeting political systems/critical infrastructure	Multiplier
≤ 53%	0.5
>53% - ≤81%	1
>81% - <100%	1.5
100%	2

Scale based on the quartiles of the range of scores obtained for all APT groups covered by EuRepoC between 2000 and May 2022.

(3) Geographical scope of the attacks

This indicator is calculated in three steps:

a) Each type of targeted entity is attributed a code, as follows:

Type of geographical entity	Code
Individual country	1
International organisation	2
Region	5
Continent	10
Worldwide	15

b) For each incident attributed to an APT group, the codes for all targeted geographical entities are summed up. The average across all incidents is subsequently calculated to obtain a single score.

Example:
Two incidents are attributed to APT A, with the following geographical targets:

- ***Incident 1:***
  Germany; UK; US; France; Africa → 1 + 1 + 1 + 1 + 10 → total: 14
- ***Incident 2:***
  Northern Europe; US → 5 + 1 → total: 6

APT A overall score: 10

c) The averages obtained in step (b) are converted to a four-level scale:

Average score of targeted geographical entities	Converted score
≤1	1
>1 – ≤2.65	2
>2.65 - ≤4.72	3
> 4.72	4

Scale based on the quartiles of the range of scores obtained for all APT groups covered by EuRepoC between 2000 and May 2022.

(4) Frequency of the APT's attacks

This indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale:

Number of incidents per year of activity	Converted score
≤ 0,38	1
>0,38 - ≤0,67	2
>0,67 – ≤1	3
>1	4

Scale based on the quartiles of the range of scores obtained for all APT groups covered by EuRepoC between 2000 and May 2022.

(5) Zero-days used

This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero-days. The obtained score are then converted to a three-level scale:

Percentage of incidents using zero-days	Code
0	0
>0 - ≤5%	1
>5 - ≤11%	2
>11%	3

Scale based on the quartiles of the range of scores obtained for all APT groups covered by EuRepoC between 2000 and May 2022.

Overall Threat Level Index

The overall Threat Level score is calculated as the sum of all (converted) scores obtained from the above indicators, leading to a maximum score of 24:

**Intensity score + Sectorial scope + Geographical scope +
Frequency of attacks + Use of Zero days**

The overall scores are then converted to a four-level scale to enable meaningful interpretation of the score through an assigned label.

Threat level score	Label
≤ 6 ⚡	Low level threat
>6 - ≤12 ⚡⚡	Moderate level threat
>12 - ≤18 ⚡⚡⚡	High level threat
>18 – 24 ⚡⚡⚡⚡	Very high-level threat

Last updated: 06.12.2022

www.EuRepoC.eu

@EuRepoC

contact@eurepoc.eu

October 2022