

Thales alerts on the risks linked to cybercrime in its new edition of the “*CyberThreat Handbook: organised cybercrime*”

- The United Nations and Accenture estimate that organised cybercrime will cost the global economy around \$5.2 trillion between 2020 and 2025. With this in mind, Thales' cybersecurity expert alert on cybercrime, stating it is one of the most dangerous threats today for companies, organisations and institutions.
- With the cybercrime edition of its annual CyberThreat Handbook, Thales decrypts this well-organised network which allows cybercriminals to mix cyber techniques and attacks with other forms of criminalities.
- To face these risks and be better prepared, Thales' experts present through this new report the cybercriminals' modus operandi and the ways to counter them.



For the 2020 edition of Les Assises de la Sécurité, Thales launches the newest edition of its CyberThreat Handbook, this year dedicated to cybercriminals. Thales' experts unveil their analysis and conclusions when it comes to cybercrime, an extremely dangerous network with a large number of hackers groups. Interactions and permanent movements unite organised cybercrime and bring it to life. Without protection or proactive means, the attacks of cybercriminals will create each time more damage. To face their always-

evolving technics, a better understanding of the threat is key; advanced tools and services such as Threat Intelligence are an asset to anticipate this threat as much as possible.

By interacting as a network of cybercrime groups, cybercriminals are able to function increasingly effectively: each group specialises in a particular area, and the different groups collaborate to benefit from each other's expertise. It is this specialisation that makes cybercriminals more effective, allowing them to concentrate on a given type of attack, while drawing on know-how from within the network.

Various groups of the most technically adept cyber attackers, with highly sophisticated compromise strategies and substantial financial resources, head this organisation. These are the "Big Game Hunters", whose tactics, techniques and procedures (TTPs) and technical infrastructure are similar to certain state-sponsored hacking groups. They attack specific targets, such as political institutions and major companies, using ransomware to demand large sums.

To achieve their objectives, cybercriminals use a combination of technical expertise and the panic that they sow in companies and institutions. Panic can have a devastating impact in terms of the consequences of an attack. It is vital not to give in to threats or blackmail. Cybercriminals' targets are extremely diverse and opportunistic; any organization can suffer from it. Thales' experts strongly recommend bearing in mind that anyone can be a target in order to be prepared and to adopt a clear and detailed cyber crisis strategy.

Surprisingly, 60% of these huge revenues come from illegal online markets, 30% from theft of intellectual property and trade secrets and only 0.07% from ransomware which however do the most damage. With revenues estimated up to \$1.5 trillion a year ¹ – meaning 1.5 times more income (as an annual average) than counterfeiting, and 2.8 times more than the illegal drugs trade – this network is a whole economic system that can now endanger any company or organization with severe consequences on the world's economy.

For more information, download [the press kit here](#) and [the report here](#).

About Thales

Thales (Euronext Paris: HO) is a global technology leader shaping the world of tomorrow today. The Group provides solutions, services and products to customers in the aeronautics, space, transport, digital identity and security, and defence markets. With 83,000 employees in 68 countries, Thales generated sales of €19 billion in 2019.

Thales is investing in particular in digital innovations — connectivity, Big Data, artificial intelligence and cybersecurity — technologies that support businesses, organisations and governments in their decisive moments.

¹ Research by the Cybersecurity firm Bromium, and Dr Mike McGuire, a researcher in criminology at the University of Surrey (UK)

PRESS CONTACT

**Thales, Media relations
Security**

Constance Arnoux

+33 (0)6 44 12 16 35

constance.arnoux@thalesgroup.com

FOR MORE INFORMATION

[Thales Group](#)
[Cybersecurity](#)

