THALES

Building a future we can all trust

Press Kit

Thales Cyber Threat Handbook 2020:
Organised cybercrime

1. 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 (on a pro forma basis including Gemalto).

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.

In a world that is increasingly mobile, interconnected and interdependent, customers come to Thales with big ambitions to help them make life better and keep us safer thanks to digital technologies.

To be sure the new technologies can be trusted, Thales **secures the digital transformation of the most critical information systems and protects every stage of the data lifecycle, from capture to completion.**

Our 6,000 engineers in critical information systems and cybersecurity design and deliver a unique range of extraordinary high-technology solutions to meet the requirements of the most demanding customers — governments, institutions, large and critical infrastructure providers. To support their digital transformation, more than 50 countries and hundreds of enterprise customers **place their trust in Thales for their critical business processes and data security**.

When it comes to digital transformation, you can rely on Thales to secure your critical information systems and protect data wherever it resides.

2. Thales Cyberthreat Intelligence Capability

"The greatest ordeal is to fear what can be prevented." said Thales of Miletus, whose quote appears of the report cover. Cyberthreats are no longer a fatality: we can learn to fight hackers by knowing their objectives, their financial resources, their technics etc.

However in the field of cyber threats, knowing one's enemy can be extremely complex:

- By nature, many cyber attackers have a **clear desire to conceal** themselves;
- Cyberattacks are extremely **diverse**, some targeting sectors, geographical areas or organizations more or less precisely, with very different motivations and a variable "performance" depending on the attacker groups.

- *What cyberthreat intelligence is about*

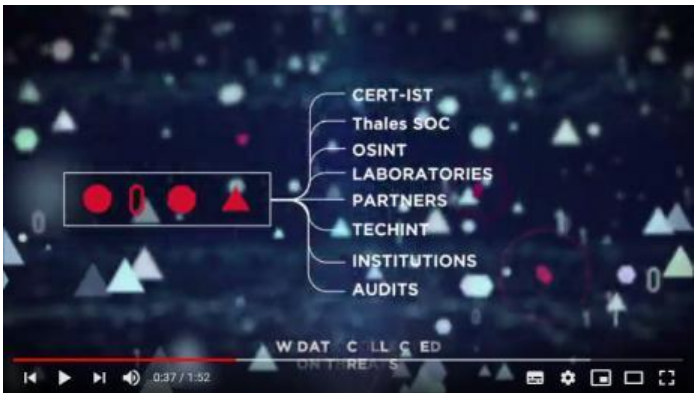
Thales' cyber threat intelligence service collects, analyzes, then sorts and correlates data related to each type of cyberattack, the attacker and its operating mode.

Thales' ambition is to **understand cyber threats in order to better detect them**: the purpose of this threat analysis is to interconnect with cyberattack detection tools (such as the detection probe and the SOC) and analyse threats in order to constantly adapt the relevance of detection rules.

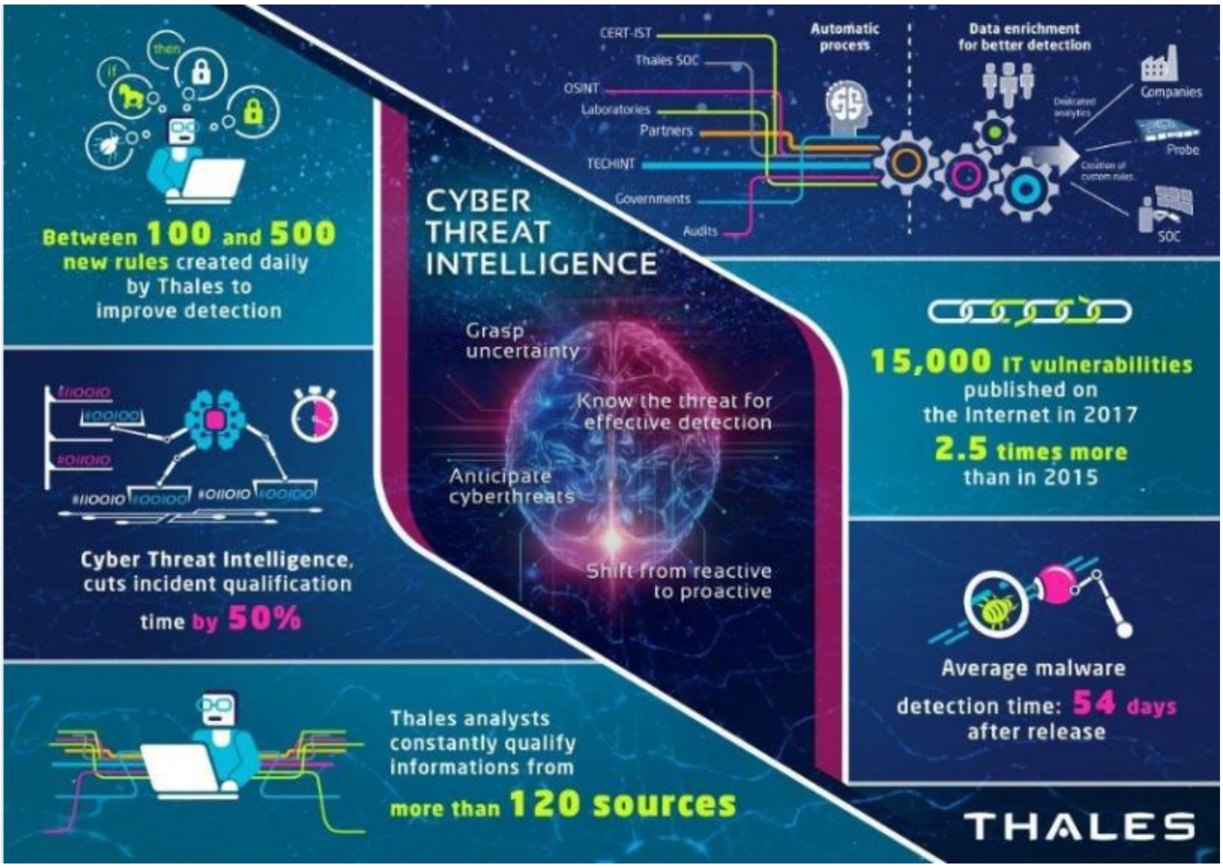
This service is based on data that is collected using a **large number of resources**, whether human, public, private, technical or not. This multi-source approach is also based on **international cooperation** (with companies such as Verint or ESET), which makes it possible to expand the number of sources and provide a global response to international cyber threats.

To that effect analysts continuously work on **data gathering, analysis and retrieval**. They also analyse malware in order to develop reports on the behaviour of hackers and to **provide feedback of information to clients under attack**. The service possesses a database that lists the attacks the methods and techniques that they use to inflitrate a system. Therefore the centre concentrates on the following questions: who attacks who? When and with which technique? What are their motivations?

By sharing their analyses of cyber criminals' behaviours and operating methods, Thales teams improve their knowledge of cyber threats, which helps strengthen detection abilities, anticipate new risks and better collectively combat cyberattacks.



Discover how CyberThreat Intelligence works on the following video:
https://www.youtube.com/watch?v=iTmCgHIyy8M&list=PLypm7oU4utZVyK3tWuEhEYLjBfQ5Fck9w&index=30



CYBER THREAT INTELLIGENCE

Between 100 and 500 new rules created daily by Thales to improve detection

Cyber Threat Intelligence, cuts incident qualification time by 50%

Thales analysts constantly qualify informations from more than 120 sources

15,000 IT vulnerabilities published on the Internet in 2017
2.5 times more than in 2015

Average malware detection time: 54 days after release

- *A day in the life of a CTI analyst*

ROMAIN
It's more important than ever to protect our infrastructure and systems

The service is divided into three bureaus: the Technical Analysis Bureau, the Strategic Context Bureau, and the Bureau of automatization and Delivery. The Technical analysis bureau conducts investigations on cyberattack campaigns that involve Thales and its partners, by examining events reported by Thales entities and by the cybersecurity Operation Center teams. The role of the Strategic Context Bureau is to render information on an attack to make it comprehensible to the entity under attack, by establishing links between the attacks and the events which may have triggered them (eg. Financial, legal, social events). And lastly, the Automatisation and Delivery Bureau collects Big Data which will subsequently places at the client's disposal.

You are willing to learn more about CTI? Meet our experts, Quentin, Nicolas and Romain, explaining how the Thales CTI capability operates on a daily basis.

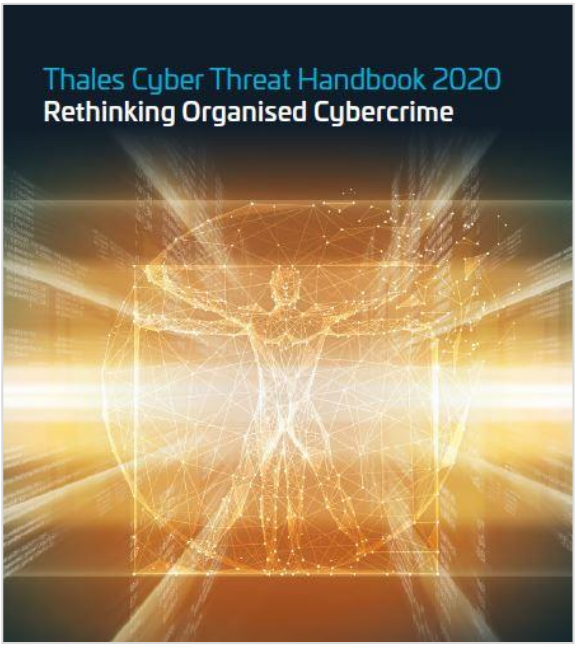
> Episode 1: Quentin talking about the Technical Analysis Bureau

> Episode 2: Nicolas talking about the Strategic Context Bureau

> Episode 3: Romain talking about the Bureau of automatization and Delivery

3. Thales' 2020 Cyber Threat Handbook, organised cybercrime

- *Introduction*


Thales Cyber Threat Handbook 2020
Rethinking Organised Cybercrime

Made by Thales, this new edition of the CyberThreat Handbook focuses on cybercrime to analyse and draw conclusions on this dangerous network to better understand the major risks it represents.

Organised cybercrime has now reached unprecedented levels of damage caused on a global scale. This demanding and incredibly complex phenomenon gives rise to as many questions as it does threats.

The damage caused to the global economy by organised cybercrime has risen to unprecedented levels since 2018, valued at a total of hundreds of billions of dollars.

According to many observers, including France's national agency for information system security (ANSSI), cybercrime will be the biggest threat we will face in the coming years. But how do we understand a phenomenon that is so diffuse, intertwined and ever-changing? How can we protect ourselves against a phenomenon that we don't completely understand, and whose outlines are blurred, at a time when the current threat level from cybercrime poses critical strategic risks for companies and organisations?

Thales's Cyber Threat Intelligence (CTI) team aims to explore this decisive question, in order to provide our partners and the general public with key insights into how organised cybercrime works. Ransom demands now run to millions or tens of millions of euros, instead of just thousands previously, and can threaten the very survival of strategic organisations.

These ransom demands have brought sweeping change to the cybercrime threat landscape, with attackers displaying characteristics similar to major State-sponsored espionage groups while retaining their core purpose of securing financial gain.

This new report is a reflection on the nature of cybercrime, its modes of operation, the world views which inspire it, and the roles of cybersecurity actors and businesses.

The report is intended as a guide to the concepts that should be borne in mind when analysing cybercrime, and as a call for a shared reflection on the best way to create new methods of analysis. It does not take a moral stance, or engage in criticism, but seeks to identify the most effective drivers that will help people understand cybercrime, so that together we can take proactive steps to ensure everybody's security. The report offers a new and different perspective, and seeks to propose a methodology that will help our partners and the general public to understand this extraordinarily complex phenomenon and support the development of effective response strategies.

- *A report dedicated to one of the most worrying cyberthreats in our society*

This phenomenon has reached even more worrisome proportions at global level. The United Nations and Accenture estimate that organised cybercrime will cost the global economy around $5.2 trillion between 2020 and 2025. Cybersecurity Ventures places the estimated cost at $6 trillion per year. This is equivalent to half of China's GDP being lost every year as a result of what we must now understand as organised cybercrime. The phenomenon has clearly assumed strategic proportions.

The phenomenon is also gaining in significance in terms of revenues. The Cybersecurity firm Bromium, and Dr Mike McGuire, a researcher in criminology at the University of Surrey (UK), estimate that revenues from cybercrime totalled $1.5 trillion in 2018. This means that cybercrime generates 1.5 times more income (as an annual average) than counterfeiting, and 2.8 times more than the illegal drugs trade (3.5 times more according to the highest estimate).

This is why Thales' experts have chosen to focus on cybercrime in this report, decrypting its organised network which allows cybercriminals to put in practice a highly performant and innovative modus operandi tending to hybride with other cyber families.

- *A very organised network*

Cybercrime operates as a united network of different groups of attackers. It should no longer be considered as an observable phenomenon, but as an organised, comprehensible construct. This emerging organisational process is key to understanding global cybercrime and its impact on companies.

This organized logic represents the biggest and fastest-changing threat to companies, critical infrastructure providers and institutions. It is not the colossal number of attacker groups that gives substance to organized cybercrime, but the tendency of these groups to interact. Interactions and permanent movements unite organised cybercrime and bring it to life.

This well-established organisation is headed by various groups of the most technically adept cyberattackers, with highly sophisticated compromise strategies and substantial financial resources. 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. We observed as much as $15 million in the latest campaigns of the operator MAZE, which had targeted Bouygues Construction in early 2020.

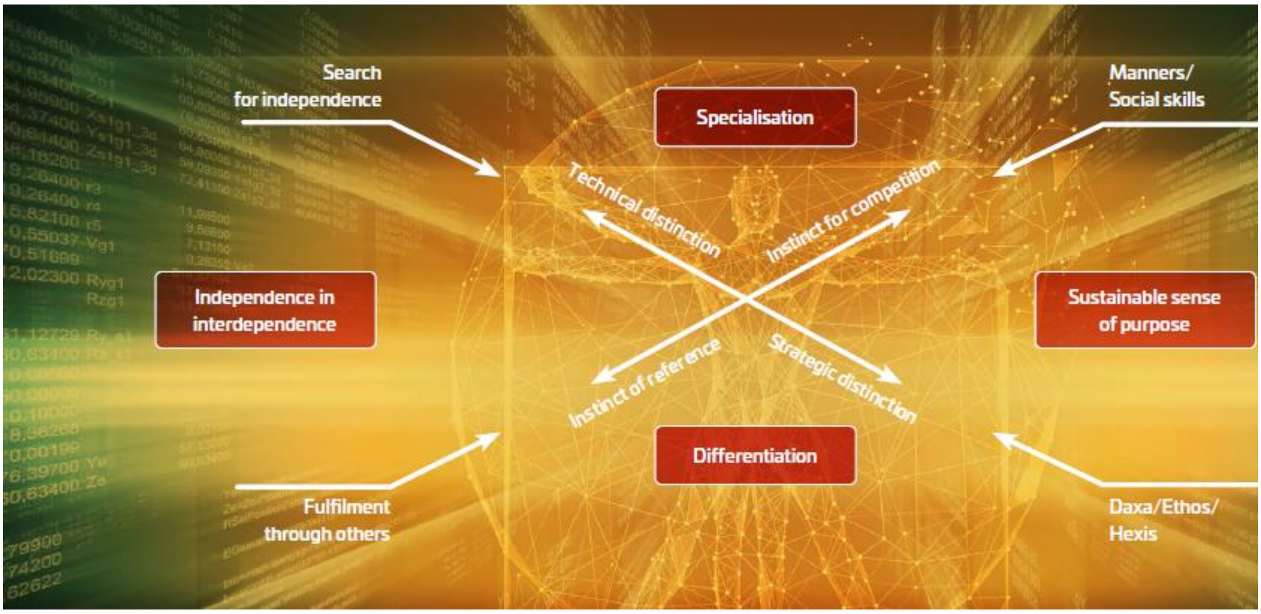
- *The concept of specialisation*

Attackers are constantly looking, albeit unconsciously, to differentiate themselves. The unconscious nature of this search for differentiation is linked to two types of instincts that can be found in other social spaces: the reference instinct, and the competitive instinct. These instincts are highly visible in the Big Game Hunting (BGH) arena, for example.

The reference instinct pushes attackers to monitor themselves continuously to check that they are not being left behind, and to ensure that they continuously improve their tactics, techniques and procedures (TTPs). The competitive instinct is the corollary of the reference instinct: although they are not in direct opposition, the fact that attackers are operating in the same space, and employing similar TTPs and arsenals, only serves to foster competition. These two instincts drive a process of differentiation, a search for improved performance, innovation, and sometimes even recognition.

The compulsive search for differentiation is intrinsically linked to the drive for specialisation. To exist as credible actors within the cybercrime universe, attackers have to specialise by displaying strategic distinction or technical distinction.

This organisational model allows cybercriminals to deploy increasingly sophisticated techniques capable of causing ever greater amounts of damage, the objective being always the same: a permanent search for a better endowment of financial, technical and reputation capital. The sheer pace of change and the ongoing drive for innovation, mean that there are few tools available to help understand and combat such threats.



- *Hackers' technics and modus operandi*

Since mid-2018, a significant new trend has been observed, involving a new form of attack focused in particular on ransomware in France and in other countries. The proliferation in ransomware attacks has taken place against the backdrop of the broader phenomenon of Malware-as-a-Service (MaaS), as well as more extensive interactions between major cybercriminals.

High-level MaaS capabilities are emerging to support the practice of Big Game Hunting (BGH), which is explained in this report and presents a major threat to organisations.

A number of Ransomware-as-a-Service operations also proved to be particularly effective in 2019. One of the best known, GandCrab (developed by Pinchy Spider), announced that it was shutting down operations the same year, having achieved total earnings of $150 million in twelve months , to be replaced by other services such as Sodinokibi (likely developed by the same group).

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.

While some sectors – media, healthcare, local authorities – are more sensitive than others, cybercriminals take an opportunistic approach to targeting, focusing on vulnerable companies (such as M6 or Rouen University Hospital) rather than predefined targets. Attackers scan a company's entire network to detect and exploit vulnerabilities. They also have extensive observation and media analysis capabilities (specialist reports are a particular area of focus) to help them identify new ways of mounting attacks.

The performance of their modus operandi is strengthened by their significant adaptability capabilities. From the very beginning of the COVID-19 crisis, organized cybercrime players were the first to use the theme in their lures for phishing, the first to imitate legitimate sites linked to COVID-19 (imitating the dynamic mapping used by Azorult malware operators to monitor the epidemic at John Hopkins University, for example), the first to develop compromised phone applications or to compromise legitimate applications linked to COVID-19.

- *Our Cyberthreat intelligence team’s recommendations*

To achieve their objectives, cybercriminals use a combination of technical know-how 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. Organisations which are the target or victim of an attack should contact the competent authorities immediately, rather than paying a ransom straight away.

To prevent the threat, it is highly recommended to anticipate and improve the crisis management strategy. This is why companies and organisations have to put appropriate measures in place to anticipate and respond to an attack, combining technical solutions with attack response capabilities, crisis management systems, insurance arrangements, etc. Raising awareness among employees is also part of this virtuous circle: any individual can be viewed by cybercriminals as a potential entry point into an organisation. Anyone can be unwittingly affected by cybercrime, by downloading an attachment at the office, by using an online service, or simply by providing a means of gaining access to large companies or government authorities.

In case of an attack, instead of paying straight away the ransom, Thales’ experts strongly advise to get immediately in touch with the appropriate authorities and to follow the advice of the French national agency for information system security (ANSSI):

- To reduce the risks of an attack by ransomware:
  - Save your data
  - Regularly update your software and systems
  - Use antivirus software and update them regularly
  - Partition your information system
  - Limit the users rights and authorisations on the applications
  - Manage internet accesses
  - Manage and supervise logs
  - Raise awareness among employees
  - Evaluate the need to subscribe to a cyber insurance
  - Prepare and deploy a response to attack plan
  - Anticipate a potential crisis communications strategy

- To have an appropriate reaction during an attack
  - Adopt good practices
  - Lead the cyber crisis management
  - Get technical assistance
  - Communicate at the right level
  - Never pay a ransom
  - File a complaint
  - Restore the systems from legit sources

- *Download the full report in English*

For more information, download the full report here: https://thalesgroup-myfeed.com/WPTHALESCyberThreatHandbook2020EN

4. A few examples of cybercriminals

- *Maze*

The MAZE group, one of the Big Game Hunters, brought about a step change in the rules in late 2019 (attack against the US firm Southwire) when it started using disclosure blackmail, unleashing a slew of imitations among competitors. The latter began systematically incorporating the tactic into their TTPs, while referencing Maze, which only served to accentuate the phenomenon of differentiation. On the morning of January 30, 2020, Bouygues Construction was attacked by Maze. The group demanded a ransom of 10 million euros in return for not disclosing the 200 GB of data that appeared to have been stolen. This attack made disclosure blackmail a recurrent component of Maze's modus operandi.

- *FIN6*

In 2019, FIN6 deployed its Ryuk ransomware to target the bio-analysis firm Eurofins. The company reported a loss of 62 million euros linked to the attack in its quarterly results. The same group, which also targeted three hospitals in Alabama, the city of New Orleans, and the firms Altran (which lost 20 million euros) and Norsk Hydro (75 million euros) with its LockerGoga ransomware, is closely linked to another major cybercrime group, TA505, which this year used its Cl0p ransomware to attack Rouen University Hospital.

- *Mummy Spider*

The first group, FIN6, uses the FlawedAmmyy malware developed by the second group, TA505. These existing links were subsequently strengthened by the emergence of another group, Mummy Spider, and its loader malware, Emotet which downloads other malware to the machines that it has infected, and simply sits in place to manage the download process. However, the number of machines infected by Emotet across all sectors of the economy is huge. Until recently, Emotet downloaded several different items of malware, in particular TrickBot, itself sometimes used by the Ryuk ransomware from FIN6.

Although we don’t know the precise nature of the links between the three cybercrime groups FIN6, TA505 and Mummy Spider – in other words whether they are of a commercial nature or based on mutual support – this convergence of interests certainly has the potential to create an extremely powerful network. Emotet, strengthened by this link with TA505 and FIN6, is capable of dropping ransomware with devastating consequences.

- *Indrik Spider*

In October 2019, the M6 Group, France's largest privately-owned multimedia company, was hit by the BitPaymer ransomware created by Indrik Spider. BitPaymer demands ransoms of up to 216 bitcoins (equivalent to approximately 2 million euros at October 2019 values). A number of attacks on city authority networks were also observed, including certain networks that are of critical importance for local populations but are very poorly protected.

- *FIN7*

FIN7 is a financially motivated group that is active since at least 2013, which primarily targets the retail, hospitality and restaurant sectors, mainly in the US. Its main goal is to steal financial assets from companies, such as debit cards, or to get access to financial data or computers of finance department employees in order to conduct wire transfers to offshore accounts. The group's often use phishing as their main attack vector, including tailored spear-phishing campaigns.

5. Other Cyberthreat Intelligence reports made by Thales

Thales – Verint 2018: The Threat Landscape Report

The 'Threat Landscape Report' is the first fruit of the collaboration between Thales and Verint, the strategic partnership between worldwide key players in the cybersecurity industry. Both companies combined their vast knowledge and expertise in order to provide meaningful insights into the dynamic cyber threat landscape and growing diversity in cyber security threats in Europe. The report looks at new and technologically advanced cyber threat capabilities which are forcing companies to adopt a more proactive security posture

Download the report: http://www.thalesgroup-events.com/ReportThalesVerint

Thales - Sekoia 2019 - Report on financial sector cyber threats

The financial sector is one of the favorite targets of cyberattackers. Cash dispensers, financial transactions, bank data theft, etc..; cybercrime causes the loss of billions of dollars for the global financial industry, a risk that sector stakeholders can no longer take. In their report on cyberfinancials, Thales and SEKOIA bring a detailed light on cyber threats in the financial sector.

Download the report: http://www.thalesgroup-events.com/ReportTHALESSEKOIA

Key findings: https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/thales-and-sekoia-release

Thales – Verint 2019: CyberThreat Handbook

Powered by the cutting-edge technologies and products of Thales and Verint, the two companies are pleased to present The Cyberthreat Handbook, a report of unprecedented scope designed to provide a classification and basis for further investigation of major groups of cyberattackers, including cybercriminals, cyberterrorists, hacktivist groups and state-sponsored hackers. As part of the strategic partnership to create a comprehensive, state-of-the art Cyber Threat Intelligence technologies, threat intelligence analysts from Thales and Verint have worked together to provide this unique 360° view of the cyberthreat landscape, with detailed descriptions of the activities of about sixty particularly significant groups, including their tactics and techniques, their motives and the sectors targeted from analysis of multiple data sources such as web and threat intelligence.

Download the report: https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK

Thales 2019: Remote working in a time of crisis

In the midst of an unprecedented global health crisis, malicious actors are taking advantage of the situation to attack the information systems of companies, organisations and individuals. To minimise the risks of a cyber-pandemic, everybody needs to be especially careful. Thales is offering free access to a new study by its Cyber Threat Intelligence centre to help organisations understand and prevent these risks at this difficult time.

Download the study: https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/covid-19-new-weapon-cyber

6. Any questions?

PRESS CONTACT

Thales, Media Relations
Constance Arnoux
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

FOR MORE INFORMATION

Thales Group
Cybersecurity
@Thalesgroup