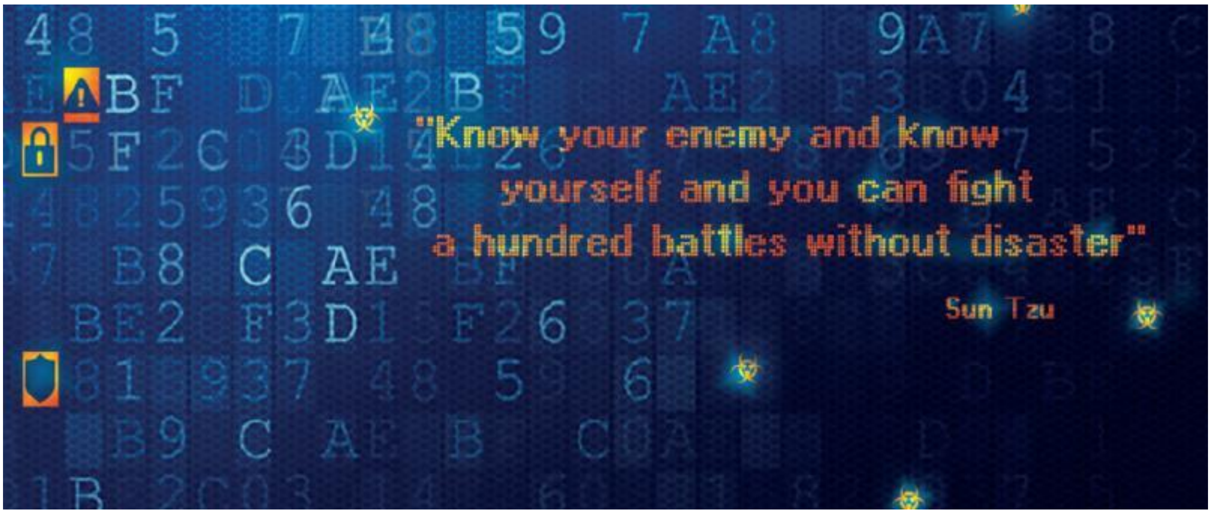
PRESS RELEASE
7 Octobre 2019
Paris La Défense

The Cyberthreat Handbook: Thales and Verint release their "Who's Who" of cyberattackers

- In our hyperconnected world, threat intelligence is crucial to our ability to better detect and prevent cyberattacks. This is the purpose of *The Cyberthreat Handbook* produced by Thales and Verint to provide insights into the most significant groups of cyberattackers through detailed rating cards.
- After a year-long investigation, teams of analysts from two of the market leaders in cybersecurity technology have produced detailed profiles of about 60 major groups of cyberattackers by studying 490 attack campaigns they have perpetrated throughout the world.
- With the release of *The Cyberthreat Handbook*, Thales and Verint are publishing their observations about the attack techniques used, the sectors most frequently targeted and the motives of the attackers, and offering recommendations to cybersecurity stakeholders for the coming years.


"Know your enemy and know yourself and you can fight a hundred battles without disaster"
Sun Tzu

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.

As cybersecurity grows in importance, Thales and Verint have worked together to find out more about cyberattackers and the techniques they employ, the purpose being to help organisations in the private and public sectors to better detect and anticipate future attacks. The cyberthreat landscape is extremely diversified, and knowing one's enemies can be particularly complex in this world of subterfuge and deception.

"The Thales and Verint teams are immensely proud to release this report today as part of its technology and domain expertise cooperation. Unique in its breadth and depth, it is the culmination of many months of research, investigation and painstaking analysis and correlation of relevant data. As cyberthreats proliferate and evolve, cybersecurity clearly has a major role to play, particularly for critical infrastructure providers. It is our duty to analyse, understand and describe the techniques employed by cyberattackers so that our customers and all other businesses and organisations are better prepared to detect and anticipate future attacks." ***Marc Darmon, Executive Vice President, Secure Communications and Information Systems, Thales***

“Joining forces with Thales strengthens our mutual ability to deliver comprehensive knowledge of potential threats, and thus provide the necessary cyber security protection,” said ***Elad Sharon, President, Verint Cyber Intelligence Solutions.*** *“Verint Cyber Intelligence leverages years of intelligence domain expertise, embedded within investigation methodologies and technologies critical to prevent cyber-attacks before they get into the gateway of the organization. This report generates unique insights and knowldege to cyber and security experts to mitigate and foresee cyberattacks”.*

Analysts from Thales and Verint have defined four major categories of attackers based on their motives and ultimate objectives. Out of approximately sixty major groups of attackers analysed, 49% are state-sponsored groups often aiming to steal sensitive data from targets of geopolitical interest. 26% are ideologically motivated hacktivists, closely followed by cybercriminals (20%) who are driven by financial gain. In fourth position, cyberterrorists account for 5% of the groups analysed.

All the world's major economic, political and military powers are priority targets of cyberattackers. The 12 countries in the world with the highest GDP are all at the top of the list of targets, headed by the United States, Russia, the European Union (particularly the United Kingdom, France and Germany) and China, followed by India, South Korea and Japan.

The sectors most targeted by these major attacks are States and their defence capabilities, followed by the financial sector, energy and transportation. Attacks towards medias and health industry are increasing fast.

Last but not least, a growing number of groups of attackers are now focusing on vulnerabilities in the supply chain, and in particular on smaller partners, suppliers and service providers that are used as trojans to access major targets.

Notes to editors - Methodology

This report does not set out to be an exhaustive inventory of cyberattackers but rather to shed light on the major groups of attackers that have been identified over the last 10 years. The sixty-odd groups and 490 attack campaigns analysed in the report were selected because they are considered emblematic in terms of their impact, attack techniques, scope, target profiles, historical nature or recent emergence. The entire analysis is based on the MITRE Att&ck matrix, a knowledge base of adversary tactics and techniques. More details can be found in the press kit.

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 80,000 employees in 68 countries, Thales generated sales of €19 billion in 2018 (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

About Verint Systems Inc.

Verint® (Nasdaq: VRNT) is a global leader in Actionable Intelligence® solutions with a focus on customer engagement optimisation, security intelligence, and fraud, risk and compliance. Today, over 10,000 organisations in more than 180 countries—including over 80 percent of the Fortune 100—count on intelligence from Verint solutions to make more informed, effective and timely decisions. Learn more about how we're creating A Smarter World with Actionable Intelligence® at www.verint.com.

About Verint Cyber Intelligence.

Verint Cyber Intelligence is a leading global provider of security and intelligence data mining software. Our broad and deep product portfolio is deployed in over 100 countries, helping government, critical infrastructure and enterprise organizations to neutralize and prevent terror, crime and cyber threats for a safer world.

PRESS CONTACT

Thales, Media relations and social media Security
Constance Arnoux
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com

Verint
SVP Marketing
Amit Daniel
+97299624843
amit.daniel@verint.com

PLEASE VISIT

Thales Group
Download photos
Download the report

@Thalesgroup