INTRINSEC

Innovative by design

Cyber Threat Intelligence

Cybercrime Threat Landscape May 2023

www.intrinsec.com

INTRINSEC
Innovative by design

Key elements

29M €

of revenue in 2022

Sustainability

of the company's project ensuring the continuity of our partnerships

250

Staff members

7

Regional Offices

24 / 7

International Service

10%

of annual sales invested in innovation

Trustful

3 ANSSI qualifications
- Audit PASSI LPM
- PRIS Incident Response
- PACS Consulting (Experimental Phase)

Leader

Pure Player in cyber security & Vanguard of the industry

Cybersecurity Pure-Player

With over 28 years of experience, Intrinsec strives to be a reliable partner and a benchmark in safeguarding against diverse cyber threats. Leveraging our extensive comprehension of cybersecurity challenges, we actively foster the protection of your organization and preserving your business by proactively meeting your cybersecurity requirements.

Focus on ransomware compromises

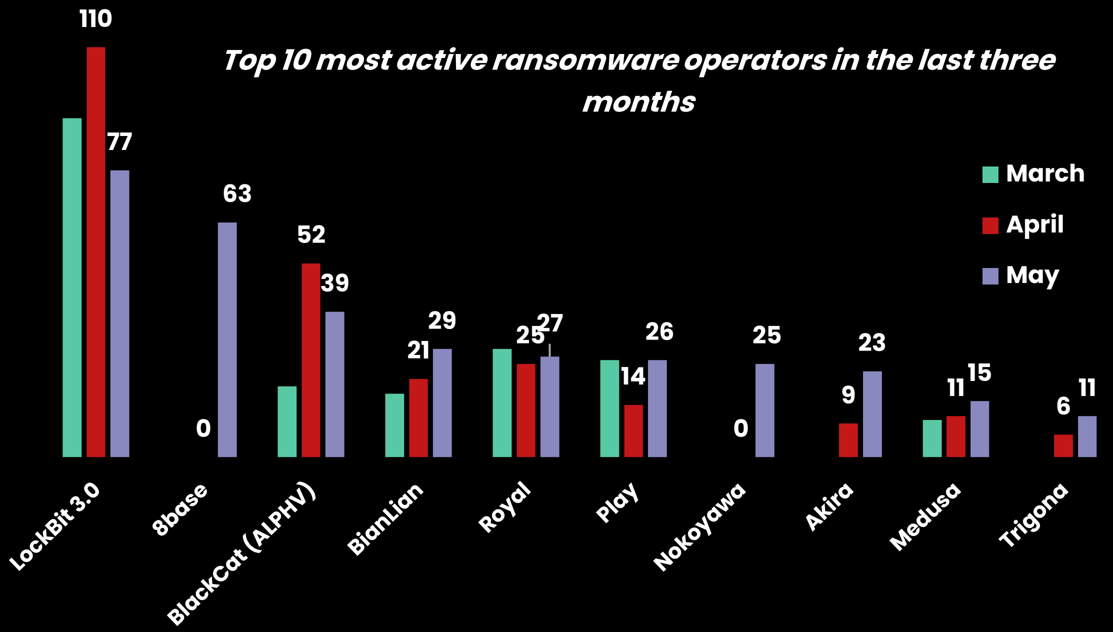
Key figures

411 Increase of 15,45 % of ransomware attacks claims between April and May 2023

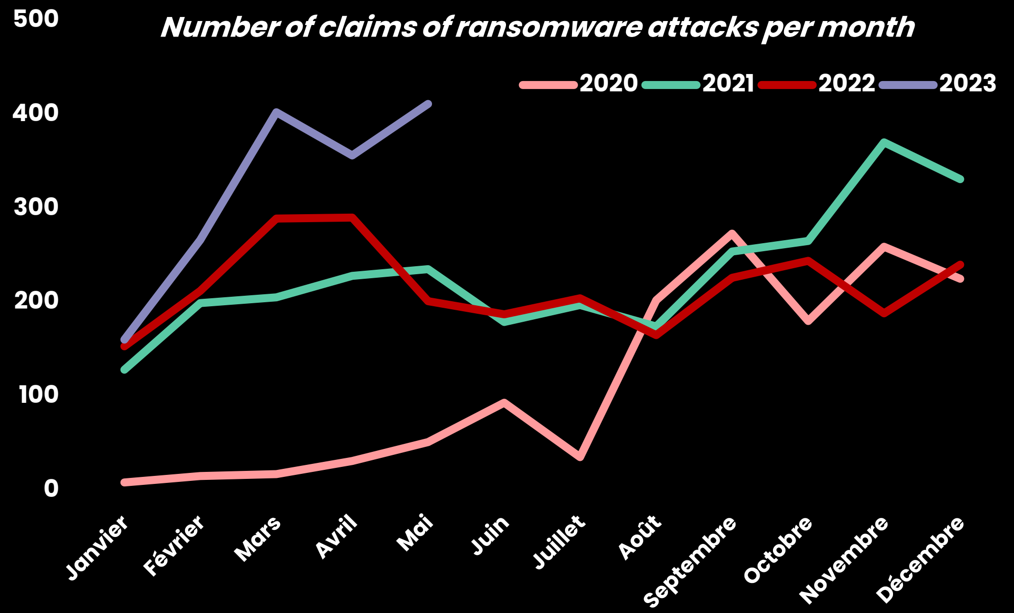
1 United States (186)
2 United Kingdom (32)
3 Canada (22)

1 Manufacturing
2 Finance
3 Health services

1 595 Claims since 1st January 2023.



Top 10 most active ransomware operators in the last three months



Number of claims of ransomware attacks per month

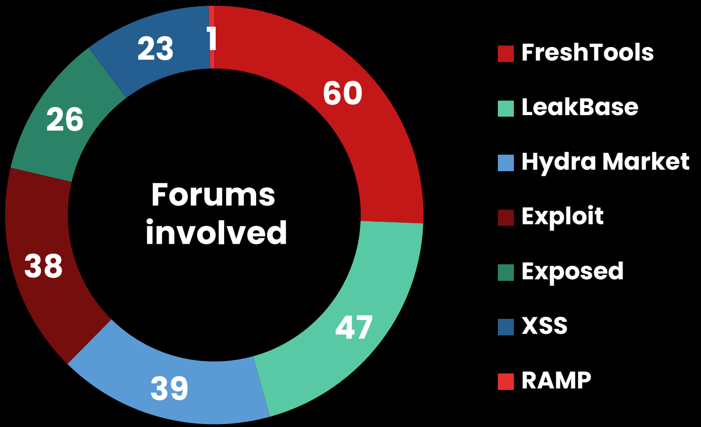
* *This data is the result of an internal methodology used by Intrinsec's CTI team, which consists of identifying public claims of attacks directly on the websites of ransomware operators.*

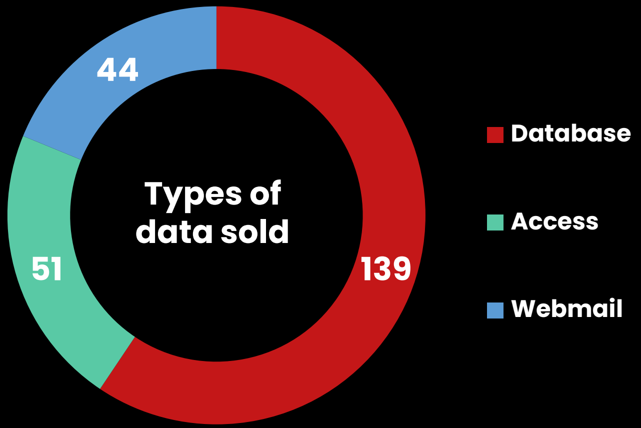
INTRINSEC
Innovative by design

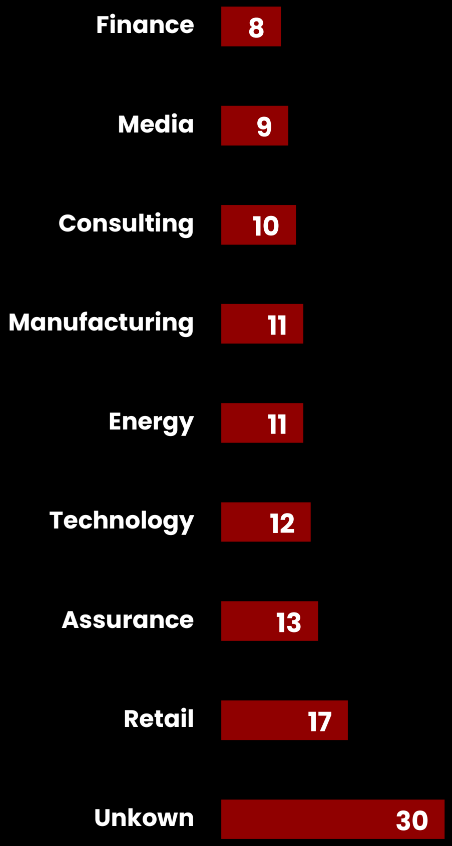
Focus on access and databases sales

234 Initial access/database sales witnessed online in May 2023

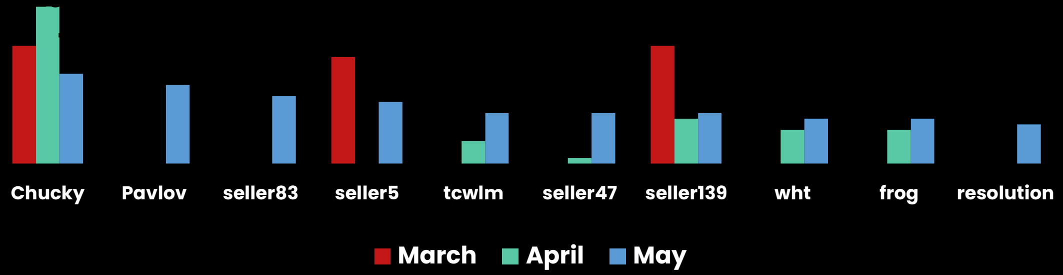
Every day, dozens of accesses and databases are sold on forums and malicious marketplaces. Obtaining them could lead to attackers gaining initial footholds and compromising more entities.



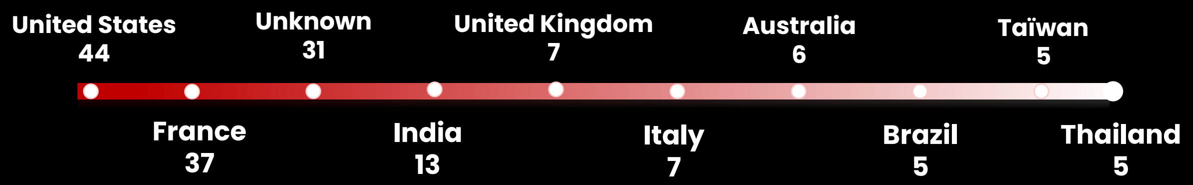




Most active threat actors this month



Targeted countries during sales *



* *The research methodology of the CTI team induces a bias on the indicators for France, a country for which the indicators are more exhaustive than for other countries, due to the origin and activities of the CTI service's clients.*

Some of our analysis from May 2023

GALLIUM

GALLIUM, also known as Alloy Taurus (Unit42) and Red Dev 4 (PwC), is a suspected Chinese state-sponsored intrusion set active since at least 2018 and possibly from 2012 onwards.

DanaBot

DanaBot is a RAT discovered in 2018 being sold as a malware-as-a-service on Russian speaking underground forums, which remain active and impactful. Due to its modular nature, threat actors leveraging DanaBot span a wide variety of malicious actions from ecrime to cyberespionage, which include disruption operations.

PikaBot

In February 2023 emerged a new malware family, very evasive and distributed by the same botnet than QakBot banking trojan; fuelling the Big-Game-hunting ransomware ecosystem. Because of some technical artefacts “PikaBot” or “Beep” retrieved upon malware analysis, this emerging malware was dubbed PikaBot.

Cyber Threat Landscape 2022

Our 2022 Cyber Threat Overview takes a look at the threat trends observed over the past year in terms of cybercrime and state threats, with a focus on the Russian, Iranian, Chinese and North Korean threats.

RISK ANTICIPATION

CUSTOMIZED CYBER INTELLIGENCE FOR EFFECTIVE DECISION-MAKING

☞ **Keep up to date with cyber news & enrich your security tools with our Information Reports**

☞ **Manage your security action plans via actionable tactical, operational & strategic intelligence on cyber threats targeting your sector : Sectoral Intelligence Note**

☞ **Put IOCs under surveillance in your security tools to protect your information system : IOC Feed by Intrinsec**

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI

PASSI
LPM | RGS | PRIS

Order PoC Now