INTRINSEC

Innovative by design

Cyber Threat Intelligence

Cybercrime Threat Landscape June 2023

www.intrinsec.com

INTRINSEC
Innovative by design

Focus on ransomware compromises

Key figures

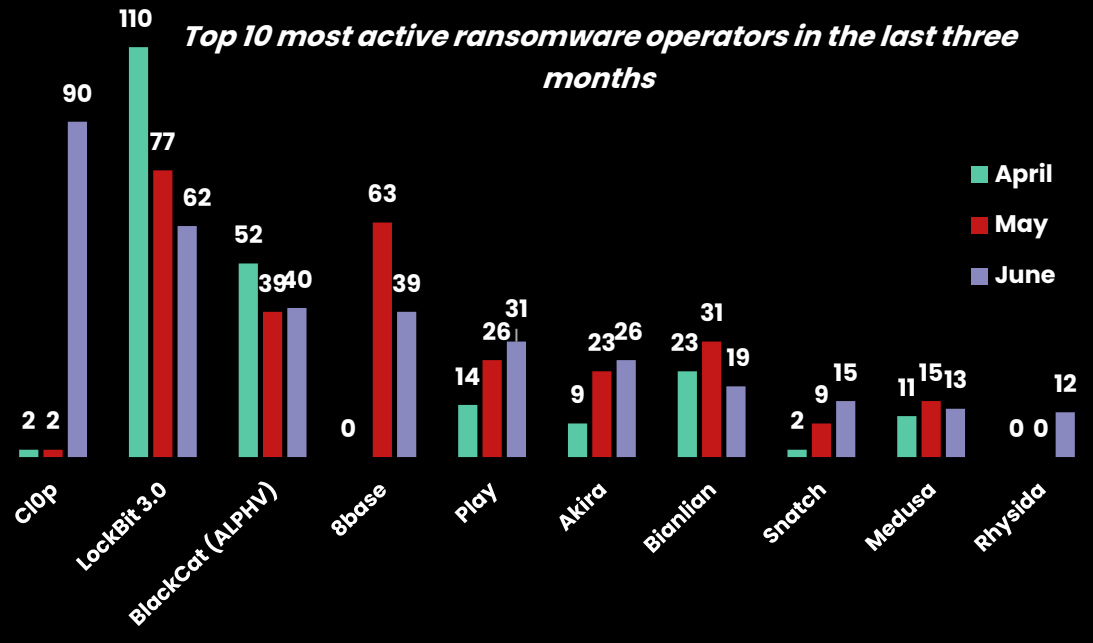
423 Increase of 2,92 % of ransomware attacks claims between May and June 2023

1 United States (210)
2 United Kingdom (26)
3 France (18)

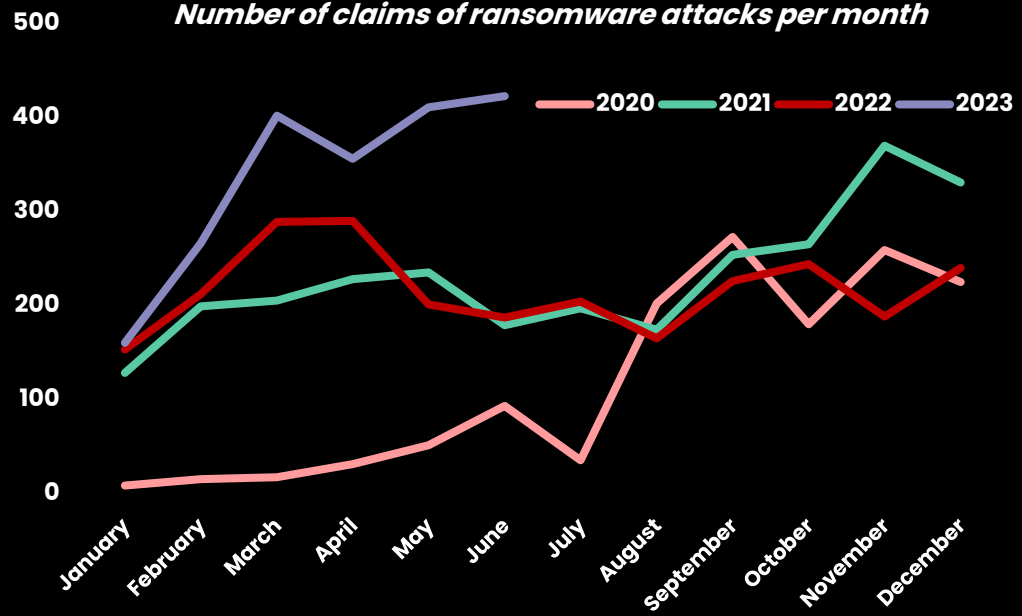
1 Manufacturing
2 Health services
3 Education

1990 Claims since 1st January 2023.

Top 10 most active ransomware operators in the last three months



Number of claims of ransomware attacks per month



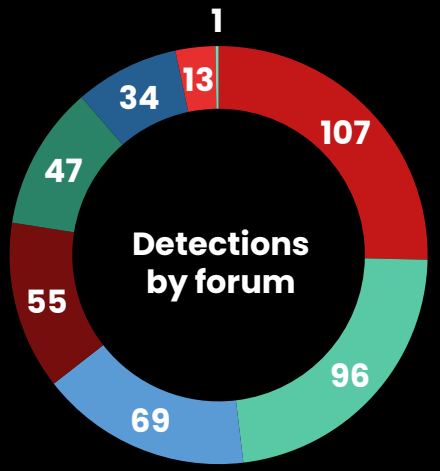
* *This data is the result of an internal methodology used by Intrinsec's CTI team, which consists of identifying public claims of attacks directly on the websites of ransomware operators.*

INTRINSEC
Innovative by design

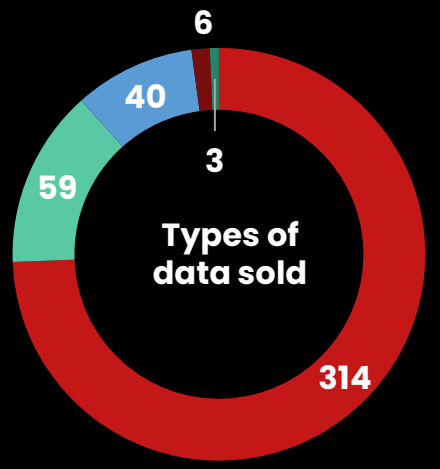
Focus on access and databases sales

422 **Initial access/database sales witnessed online in June 2023**

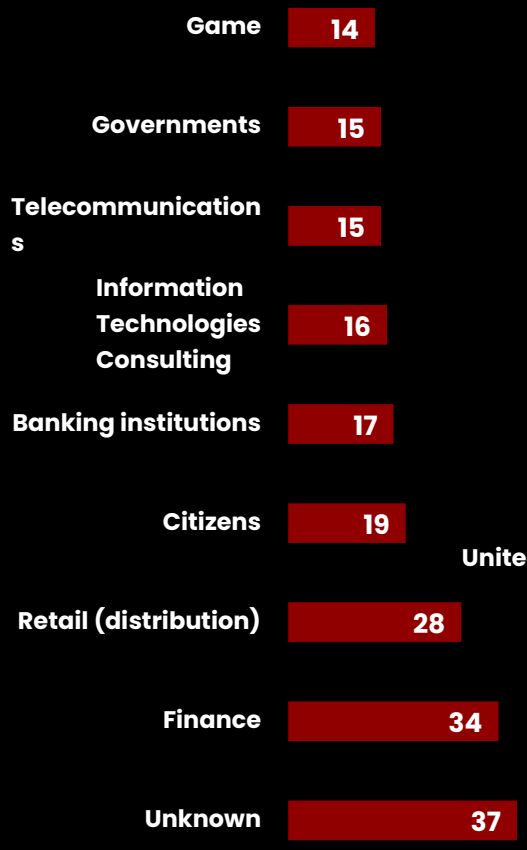
Every day, dozens of accesses and databases are sold on forums and malicious marketplaces. Obtaining them could lead to attackers gaining initial footholds and compromising more entities.



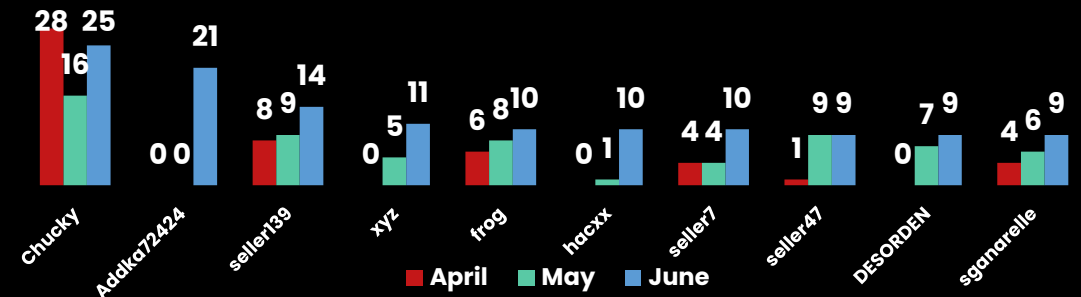
- Exposed
- LeakBase
- BreachForums
- Freshtools
- XSS
- Exploit
- Leakbase.org
- Telegram



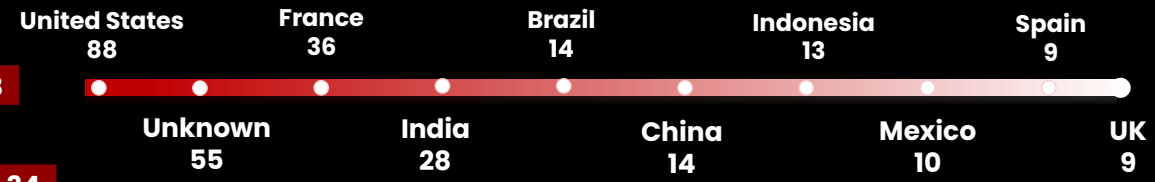
- Database
- Webmail
- Access
- Documents
- Vulnerabilities



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.*

INTRINSEC
Innovative by design

Some of our analysis from June 2023

Gamaredon

The Gamaredon intrusion set continues its campaign of attacks against NATO allies in Europe, and particularly in Ukraine.

SHARP PANDA

Active since at least 2021, Sharp Panda is a fairly sophisticated intrusion set associated, in open sources, with China. While Sharp Panda's campaigns appear to have historically focused on Southeast Asia, a recent major shift in victimology suggests that it may now also be targeting G20 countries, including 11 high-ranking French officials.

GuLoader

GuLoader is a loader used to evade detection and analysis by leveraging a variety of techniques like checking for its environment of execution and encrypting the payload it is trying to inject on the infected system. GuLoader is known to drop malware like Lokibot, AzorUlt, Remcos, Nanocore, WarzoneRAT, AgentTesla, FormBook and Hakbit ransomware.

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

PASSI
LPM | RGS | PRIS

Order PoC Now