INTRINSEC
Innovative by design

Cyber Threat Intelligence

Cybercrime Threat Landscape
July 2023

www.intrinsec.com

INTRINSEC
Innovative by design

Focus on ransomware compromises

Key figures

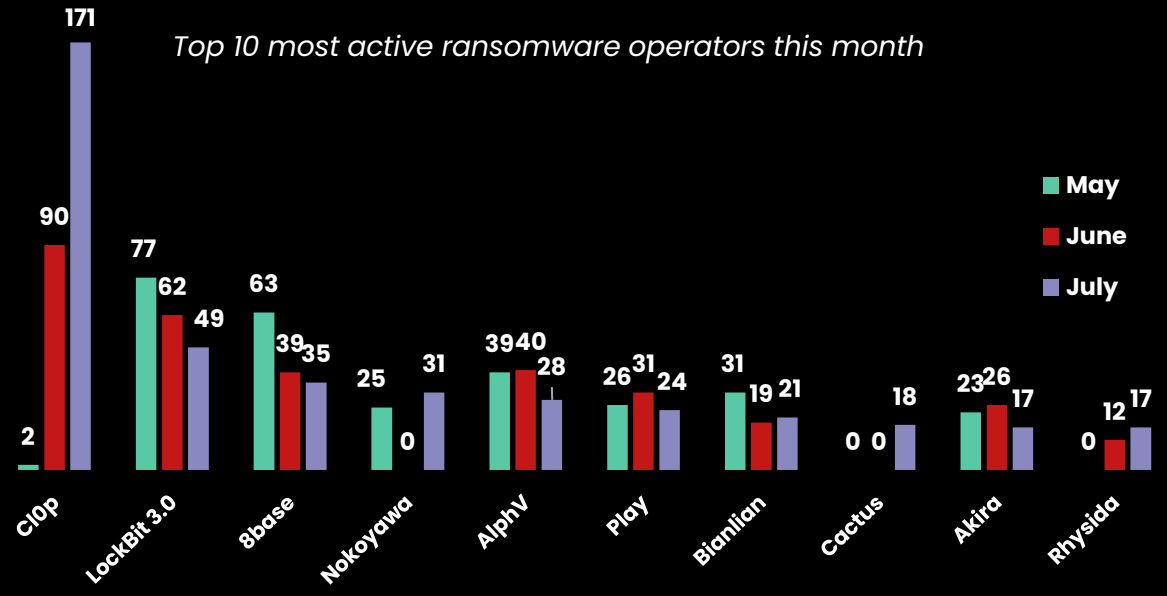
525 **Increase of 24.11 %** of ransomware attacks claims between June and July 2023

1 **United States (260)**
2 **United Kingdom (44)**
3 **Italy (20)**
7 **France (12)**

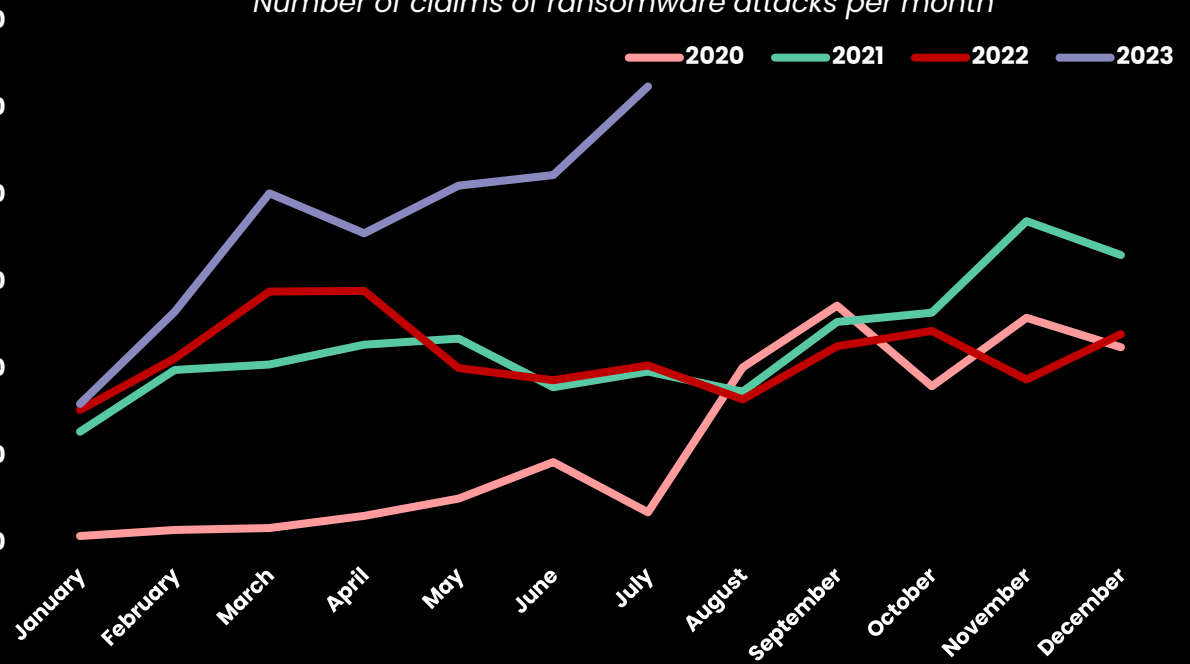
1 **Manufacturing**
2 **Consulting**
3 **Education**

2 548 **Claims** since 1st January 2023.

Top 10 most active ransomware operators this month



Number of claims of ransomware attacks per month



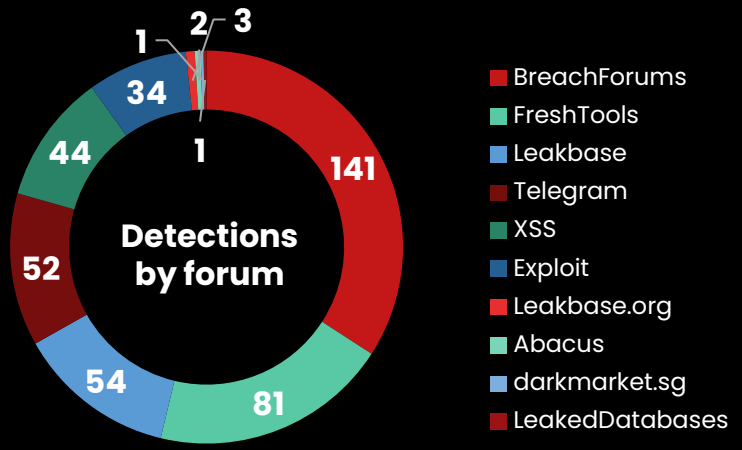
* *This data is the result of an internal methodology used by Intrinsec's CTI team, which consists of identifying public claims of attacks directly on the websites of ransomware operators.*

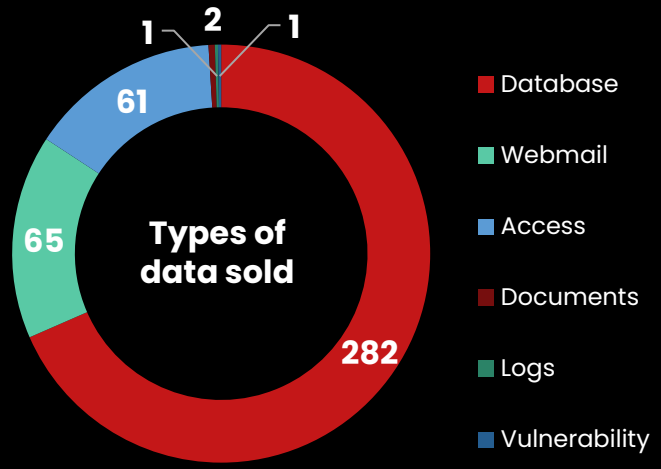
INTRINSEC
Innovative by design

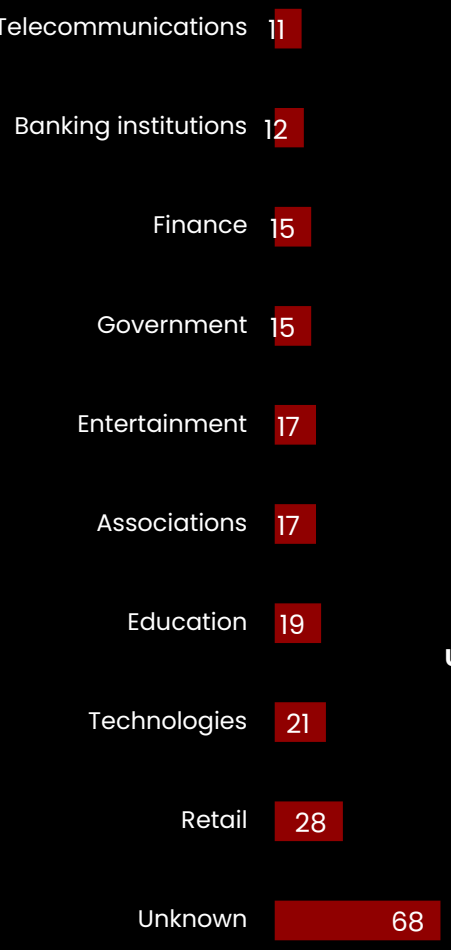
Focus on access and databases sales

413 Initial access/database sales witnessed online in July 2023

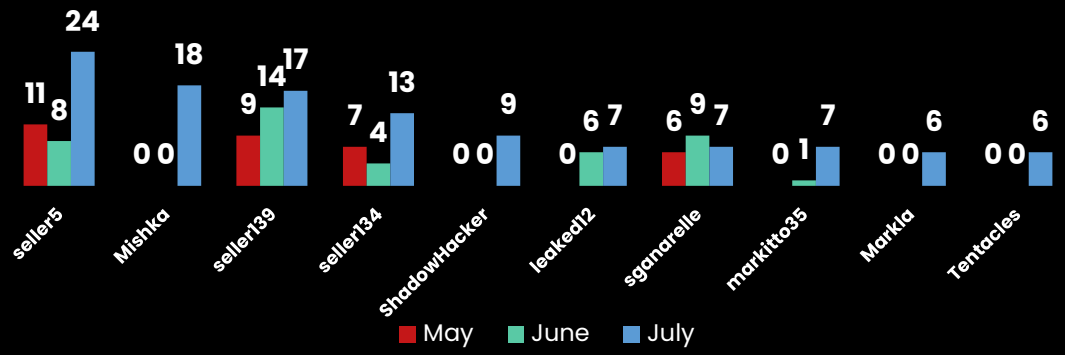
Every day, dozens of accesses and databases are sold on forums and malicious marketplaces. Obtaining them could lead to attackers gaining initial footholds and compromising more entities.







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.*

INTRINSEC
Innovative by design

Global threat trends for July 2023

BlackGuard

BlackGuard is an info stealer discovered in 2021 and sold as a malware-as-a-service on Russian-speaking underground forums and Telegram Channel. BlackGuard remains active in 2023, despite its disappearance from underground forums. Blackteam007, a top tier underground XSS forum member, is behind the development of Blackguard. This threat actor has a medium level of credibility.

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. The actor that bought GuLoader must provide to the building program the URL hosting the software that it wants to protect and load on the system. It must be encrypted and can be hosted on legitimate services like Google Drive or any other domain. GuLoader can come in different files format like VBS scripts or NSIS installers.

124 (+5.98 %)

Vulnerabilities processed in our Information Reports (VMware, Cisco, Fortinet, Apple, Microsoft, etc.).

Imperial Kitten

Imperial Kitten, an intrusion set associated to Iran, has set up watering holes onof legitimate Israeli websites operating mainly in the shipping industry, to deliver malicious JavaScript to these websites' visitors.

The JavaScript was used to collect information about the victims' systems. We identified several variants of this JavaScript, indicating different development stages of Imperial Kitten's campaign.

UAC - 0006

The threat actor known as UAC-0006 has recently conducted a large phishing campaign against several Ukrainian entities to deploy a loader called SmokeLoader. This malware is used to drop other payloads and is broadly associated with criminal activities.

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