INTRINSEC

Innovative by design

Cyber Threat Intelligence

Cybercrime Threat Landscape August 2023

www.intrinsec.com

INTRINSEC
Innovative by design

Focus on ransomware compromises

Key figures

393

Decrease of 25.14 % of ransomware attacks claims between July and August 2023

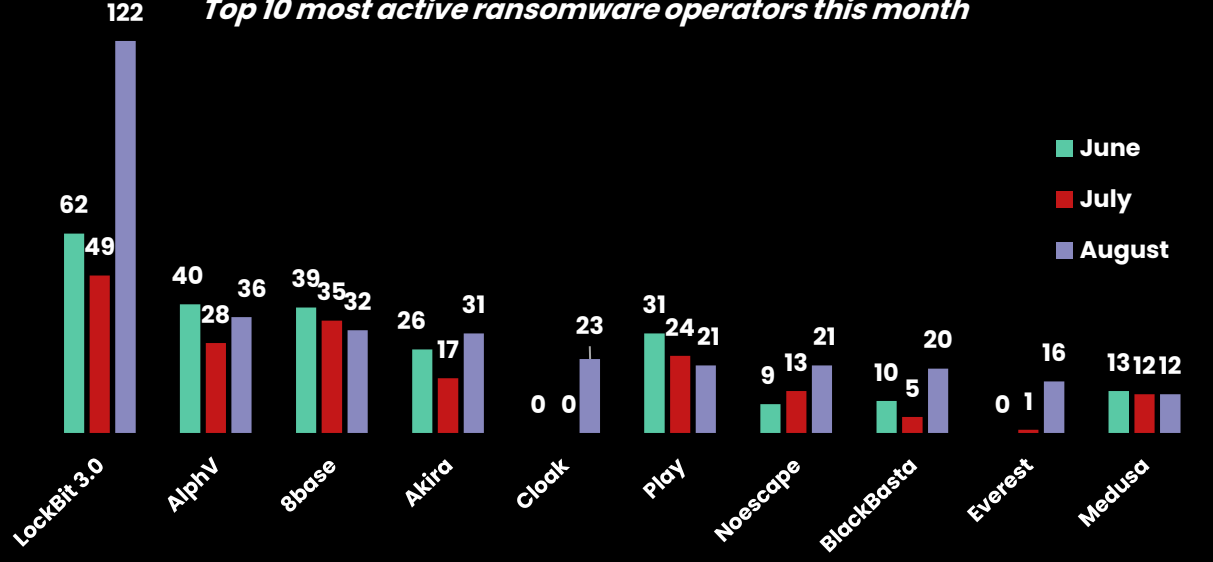
1 United States (176)
2 Germany(24)
3 United Kingdom (21)
5 France (14)

1 Manufacturing
2 Retail
3 Construction

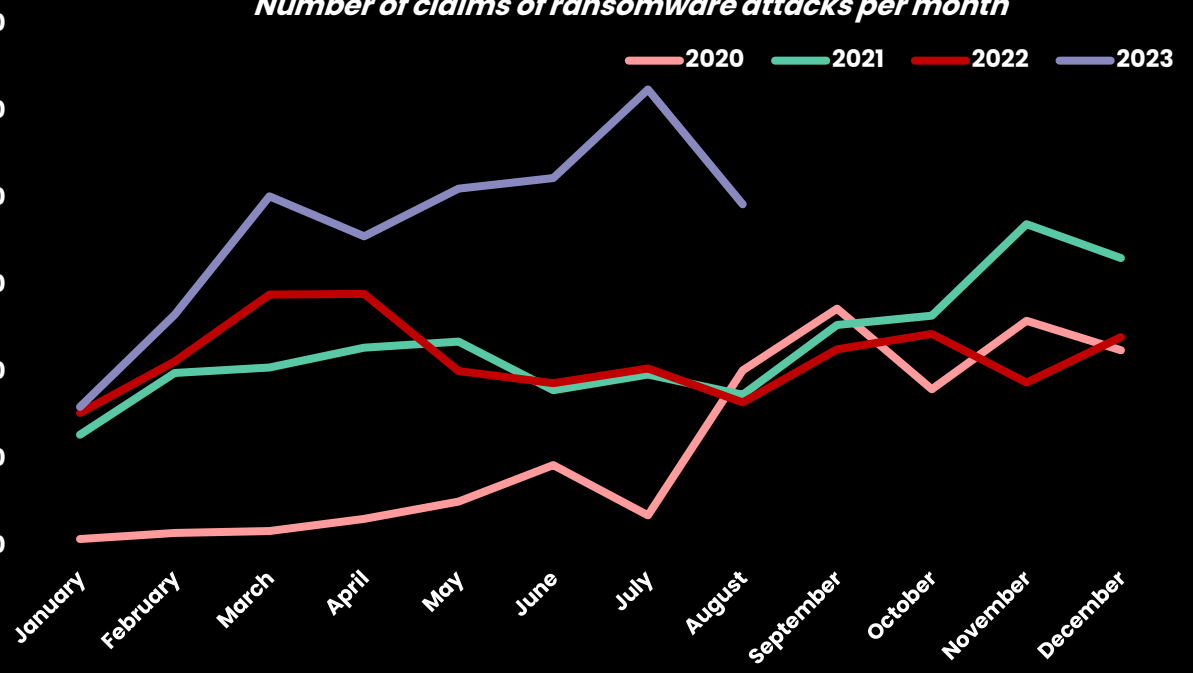
2 941

Claims since 1st January 2023.

Top 10 most active ransomware operators this month



Number of claims of ransomware attacks per month



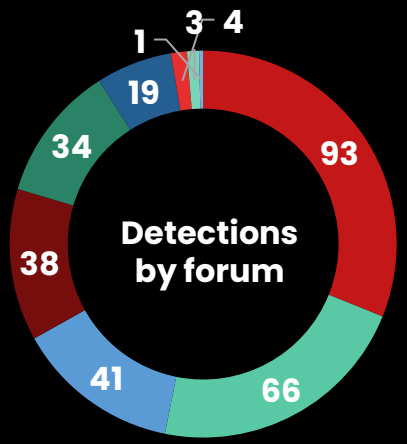
* *This data is the result of an internal methodology used by Intrinsec's CTI team, which consists of identifying public claims of attacks directly on the websites of ransomware operators.*

INTRINSEC
Innovative by design

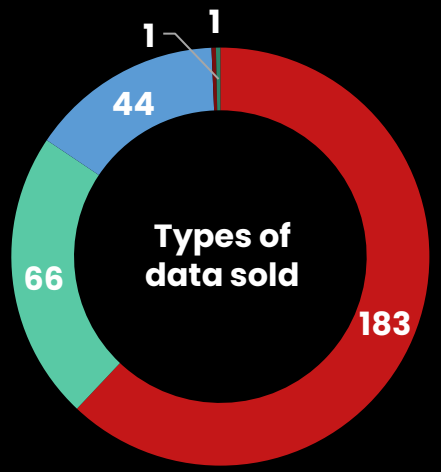
Focus on access and databases sales

299 **Initial access/database sales witnessed online in August 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.



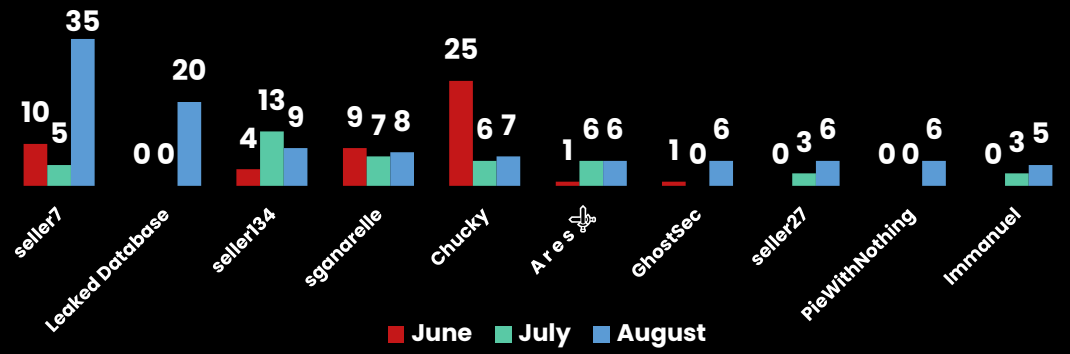
- BreachForums
- FreshTools
- Exploit
- Leakbase
- Telegram
- XSS
- LeakedDatabases
- Leakbase.org
- Nulled



- Database
- Webmail
- Access
- Documents
- Vulnerability

Food and drinks businesses	9
Banking institutions	9
Consulting	11
Telecommunications	12
Road transport	14
Government and administrations	16
Retail (distribution)	16
Citizens	20
Finance	20
Unknown	50

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 August 2023

SmokeLoader

First advertised on undeground forums like Prologic, Grabberz and DamageLab (now XSS) in 2011, Smokeloader is a malware that serves as a loader for other malicious softwares such as Ursnif, Danabot, Djvu ransomware, Rhadamanthys, Fabookie, Redline, Amadey, Aurora, Vidar, Laplas, XMrig, Dcrat, PrivateLoader and the Eternity toolkit.

GootLoader

GootLoader is the evolution of GootKit, a banking trojan that was first reported in 2014. This version had the ability to perform web injections in banking pages. By doing so, the malware could intercept the requests from the user to the bank and steal their content or modify it. The malware is now more commonly known as “GootLoader”, since the functionalities related to banking had disappeared and only the loading ones remained.

107 (-13.71 %)

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

APT15

APT15 is a sophisticated Chinese-linked intrusion set known to target public and private organisations all over the world, including in France. The present analysis focuses on two malwares, Ketrican and Graphican, used in recent APT15’s campaigns and the associated command and control infrastructure.

Recent Russian Cyber Threat Landscape

It is always interesting to dwell on what has been happening in a major cyber power’ ecosystem to better grasp the overarching evolution of cyber threats. Specifically, aims of this analysis is to delve into the Russian cyber threat ecosystem in order to pinpoint some macro tendencies of Russia’s cyber malicious activities over the past three months.

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