INTRINSEC

Innovative by design

Cyber Threat Intelligence

Cybercrime Threat Landscape September 2023

www.intrinsec.com

INTRINSEC
Innovative by design

Focus on ransomware compromises

Key figures

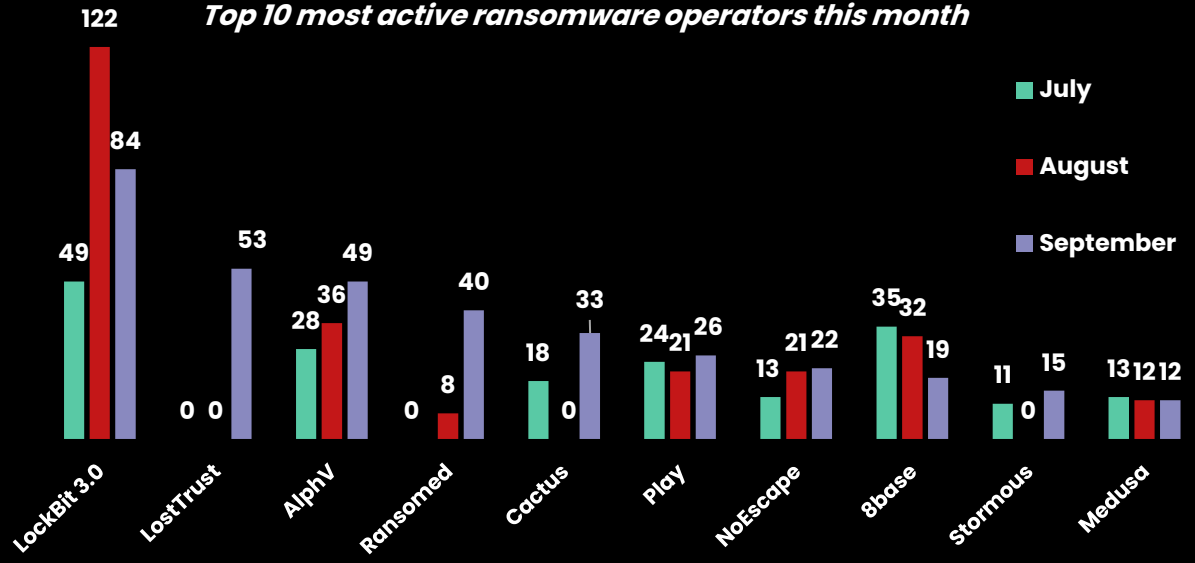
490 Increase of 24.68 % of ransomware attacks claims between August and September 2023

1 United States (230)
2 United Kingdom (27)
3 Canada (23)
4 France (22)

1 Retail
2 Construction
3 Manufacturing

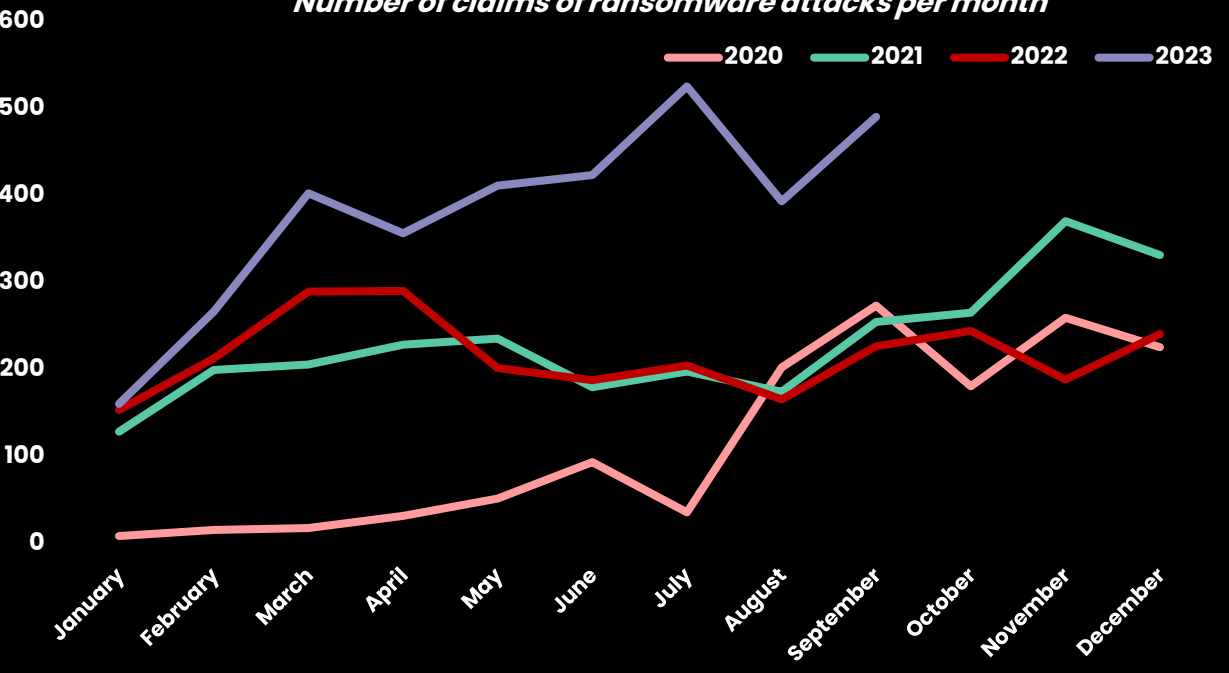
3 429 Claims since 1st January 2023.

Top 10 most active ransomware operators this 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.*

Number of claims of ransomware attacks per month

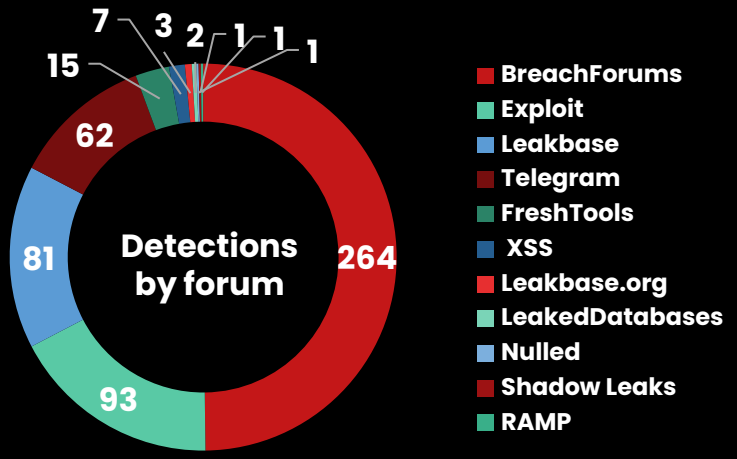


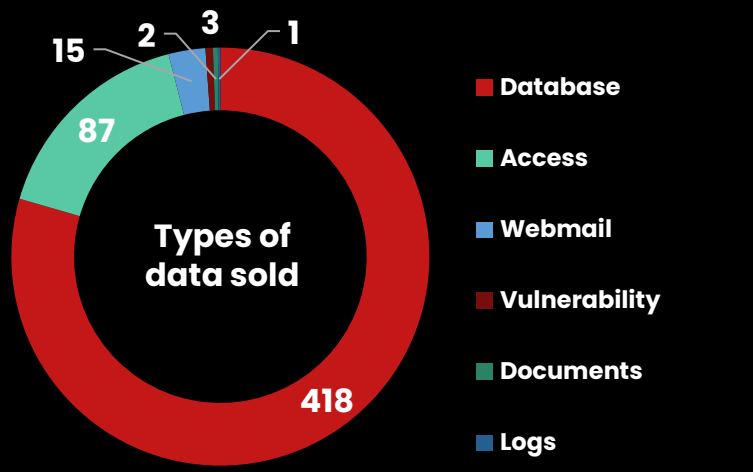
INTRINSEC
Innovative by design

Focus on access and databases sales

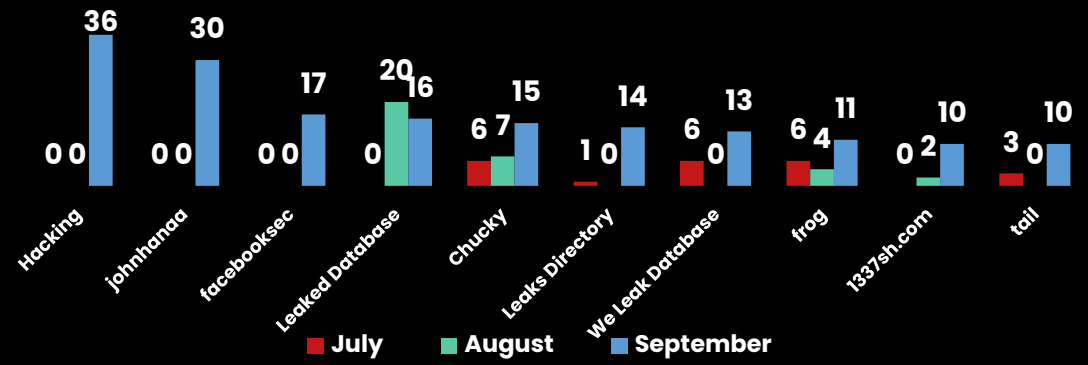
530 **Initial access/database sales witnessed online in September 2023**

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.

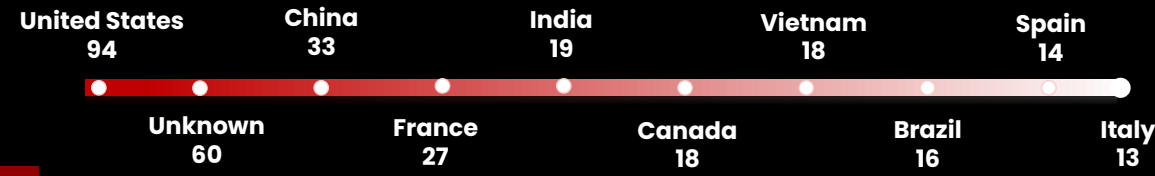




Most active threat actors this month



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

Our analysis

Mallox

Mallox is the last variant of TargetCompany ransomware that evolved rapidly to become a genuine threat from which organizations should be prepared. The latter could adopt a Ransomware-as-a-Service model to expand its operations seeking more profits. We anticipate a rise in its adoption and thus in impact. The initial accesses leveraged remain successful over time.

Cloud Babylon

During the month of July 2023, we collected several malicious emails that were used to deploy the last version of CloudEye. The latter is a malware sold by an Italian company that aims to encrypt and load an additional payload on the target's system, which we analysed in a previous report. After comparing and analysing the full infection chain that those emails deployed, we were able to attribute those campaigns to a specific intrusion set. Based on its use of the CloudEye loader, and the Babylon Bank of Iraq's website to host its encrypted payloads we dubbed the latter "Cloud Babylon".

175 (+63.55 %)

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

Evasive Panda

Evasive Panda, also known as Daggerfly or Bronze Highland, is a China-based cyberespionage group that has been active since at least 2014 according to Symantec and 2012 according to ESET.

The intrusion set is known to target individuals and public institutions across countries mainly in Asia but also in Africa using its signature backdoor named MgBot. Considering that cyberattacks on telecommunications companies in the Middle East have also been observed, it cannot be ruled out that European companies could be targeted by Evasive Panda.

Gamaredon

While reviewing a list of known Gamaredon IoCs, a subdomain resolving to a different IP than the usual REG-RU parking IP drawn our attention. We found a Portable Executable (PE) file that was undetected by antiviruses engines on VirusTotal (at that moment) and not mentioned in previous reports or sandboxes analysis was discovered by Intrinsec's CTI team. Upon analysis it was observed that the file would drop and execute multiple Visual Basic scripts, one of them communicating with unflagged infrastructure. Static analysis revealed that this script was a visual basic loader that would retrieve malware from C2 infrastructure.

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