Ransomware Threat Landscape Quarterly

Trends and Insights in January-March 2024

25 April 2024

TLP: CLEAR
Disclosure is not limited

Clipeus Intelligence OU
Estonian Business Registration: 16862531
Harju maakond, Tallinn, Kesklinna linnaosa, Ahtri tn 12, 15551

Scope and Methodology

OSINT Monitoring

Data collection via monitoring of leak sites without actor engagement

Curated

We collect with automation but validate and enrich data with human intelligence

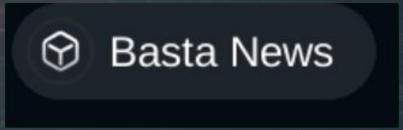
Time Scope

Our scope goes from January 1 to March 31, 2024, with references to developments occurring in early April 2024

We developed RansOmnia, a brand new web application for ransomware monitoring and intelligence gathering. We used RansOmnia to create this report. Specifically, RansOmnia helped us extract intelligence on ransomware trends and TTPs of various operations. If you want to know more, check out this webpage!

Ransomware Actors

Most Active Ransomware Operations By Volume Of Attacks



LOCKBIT
Claimed Victims: 199

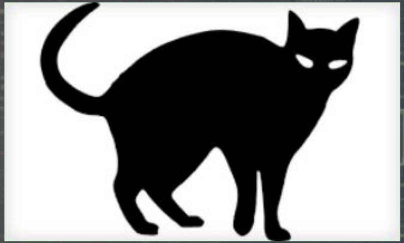
BLACKBASTA
Claimed Victims: 75

PLAY
Claimed Victims: 74

Around the end of 1Q2024, in the aftermath of the Cronos operation, LockBit has been declining and potentially rebranding. Yet, in 1Q2024, the group's activity reached new heights.

Evolution Of The Landscape

Rebranding Of Major Actors



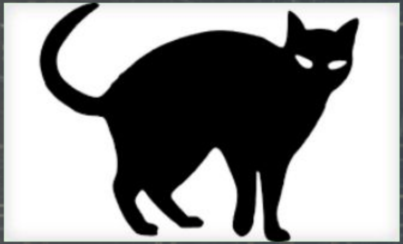
In early March, BlackCat/Alphv shutdown its operation with an exit scam reportedly worth USD 22 million towards its affiliate network. Reports suggests the proceeds may have come from the hack of an US-based business management company.

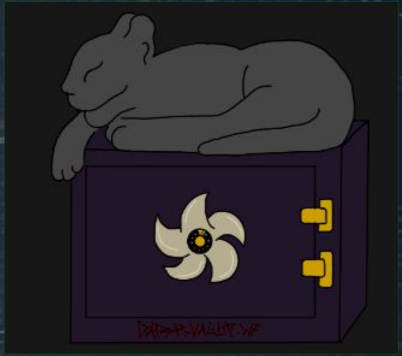
In April, RansomHub, an operation which appeared in February 2024, claimed to have access to the data of the same provider BlackCat/Alphv hacked. Data released on the RansomHub DLS on April 15 may corroborate such claims and, subsequently, suggest RansomHub may be a BlackCat/Alphv rebrand.

ransomhub :~#

Evolution Of The Landscape

Rebranding Of Major Actors





At the very beginning of 2Q2024, a new actor by the name DarkVault emerged on the scene. Based on commonalities between the two DLS, it has been speculated to DarkVault may be a rebrand of LockBit. However, the same rationale may suggest also a correlation with actors previously linked to BlackCat; DarkVault's logo is composed of a black cat lying over a vault - which may recall the notion of a lock.

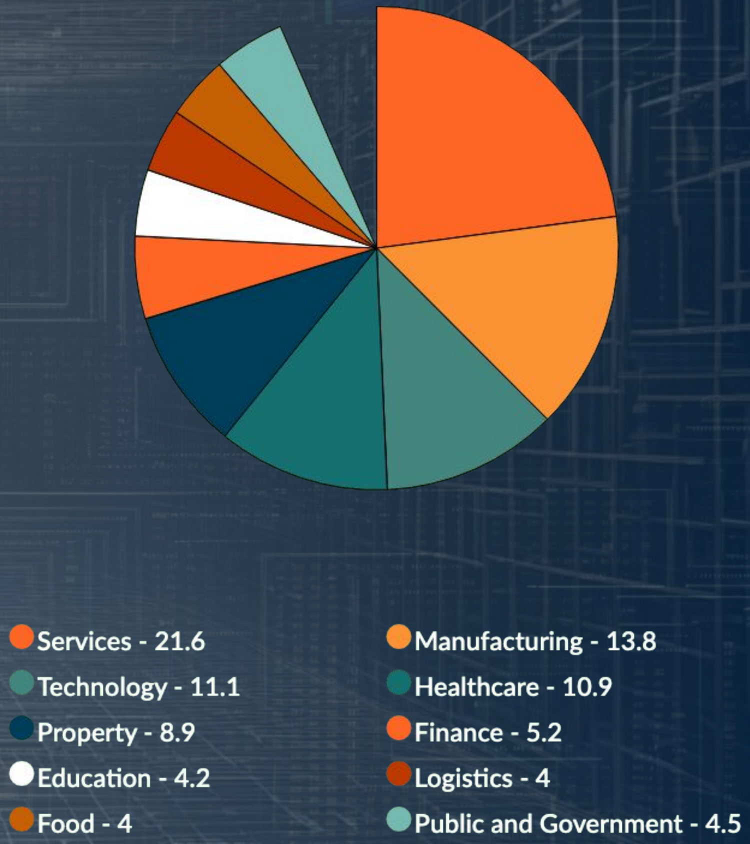
Victimology

Top Ten Impacted Sectors By Attack Volume

SMEs have been under increasing threat, particularly those that are likely to hold clients' PII. These include law firms, accounting, investment brokers, insurance firms, realtors, and medical professionals.

Technology and electronics are particularly targeted in the cloud infrastructure and web hosting segments. A number of semiconductor companies were also targeted. Such compromises may have relevant ramifications in light of the "chip war" between China, on the one side, and the United States and the EU, on the other side.

Local government organizations have been growingly a target of a variety of ransomware operations.



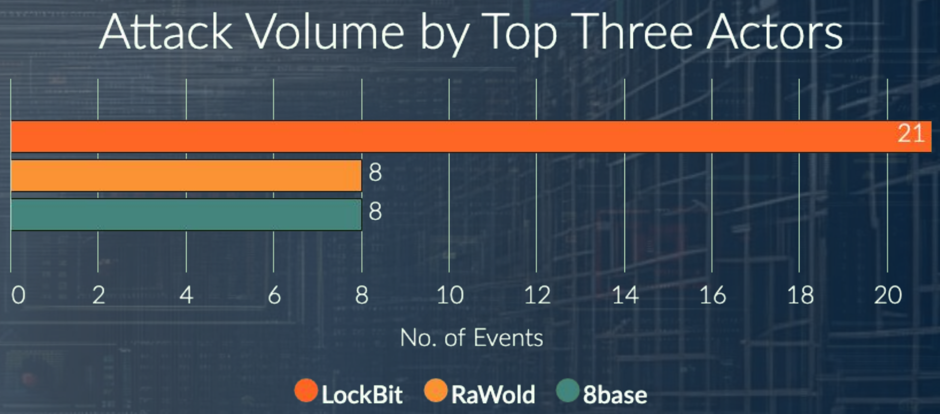
Regional View

Asia-Pacific

While LockBit has been consistently the most active actor in the region, RaWorld emerged as the second most active threat in the last part of 1Q2024.

Australia has been the most targeted country in the region. India and China were targets of a slightly lower number of events.

Attacks against Taiwan-based semiconductor companies were claimed in January and February by LockBit and MyData respectively. This sector is particularly critical in the current geopolitical context.



Regional View

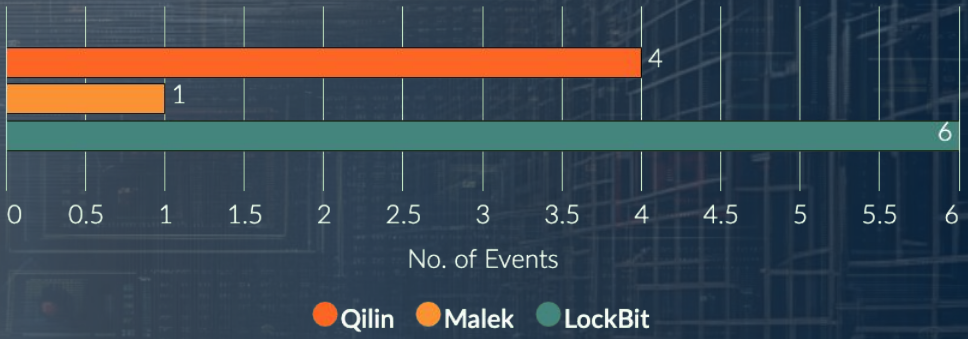
Middle East

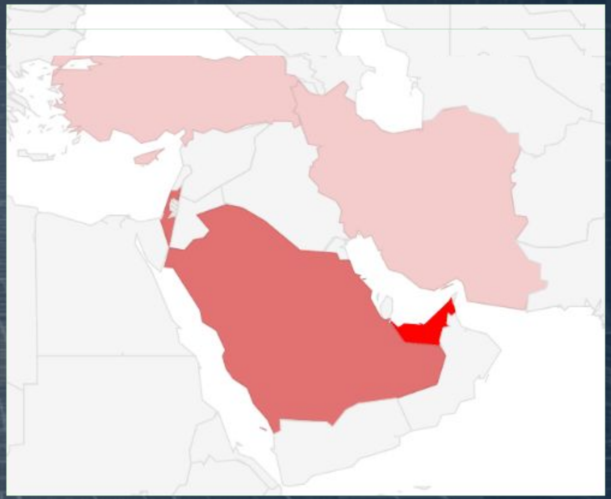
The UAE has been the most targeted country in the region with a volume of events amounting to three times that of KSA and Israel that share the second spot in the event count.

In the UAE property managers and construction contractors are the primary targets of ransomware actors. Technology companies, particularly cloud and hosting service providers have been also frequently targeted.

Geopolitics has a major impact on ransomware in the region. Malek, potentially linked to Iran, has targeted Israel in politically-motivated attacks.

Attack Volume by Top Three Actors





Regional View

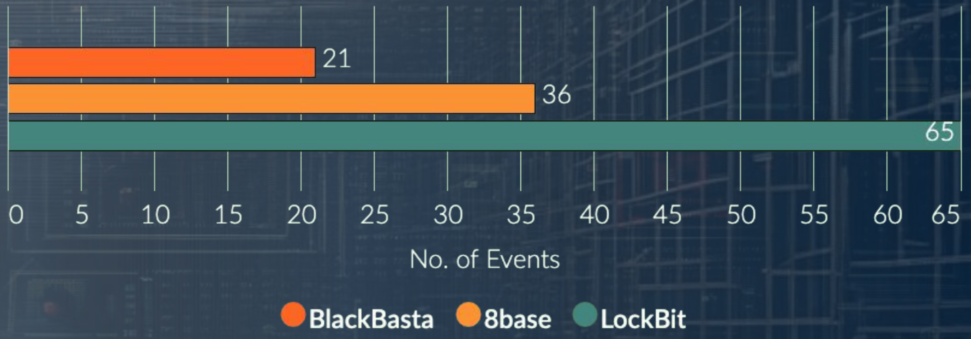
Europe

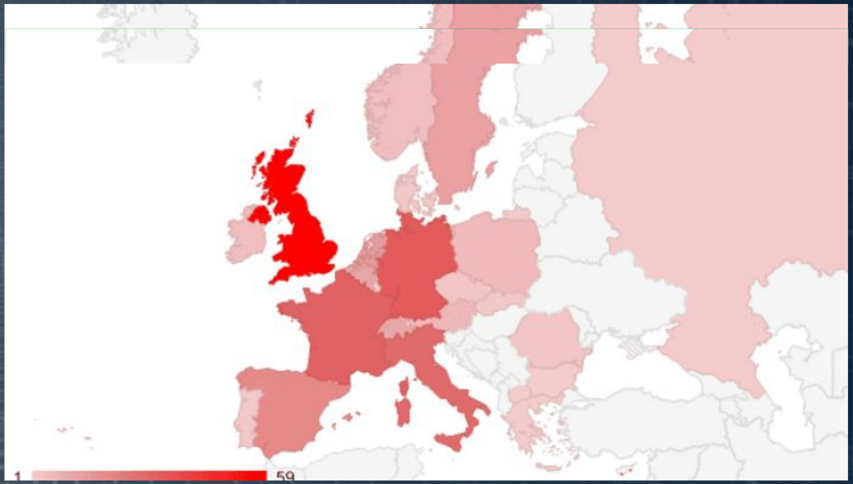
In Western Europe, ransomware has been a major threat to SMEs, particularly construction contractors, accounting firms, and law firms that have often targeted by LockBit, 8base and BlackBasta, the most active actors in the region. The UK, Germany, France and Italy have been the most impacted countries.

State administration and state-owned hospitals were also under attack. Rhysida listed hospitals in Italy and France.

Russia was the target of a single event claimed by Werewolves on March 13, on the eve of the Russian general election.

Attack Volume by Top Three Actors





Regional View

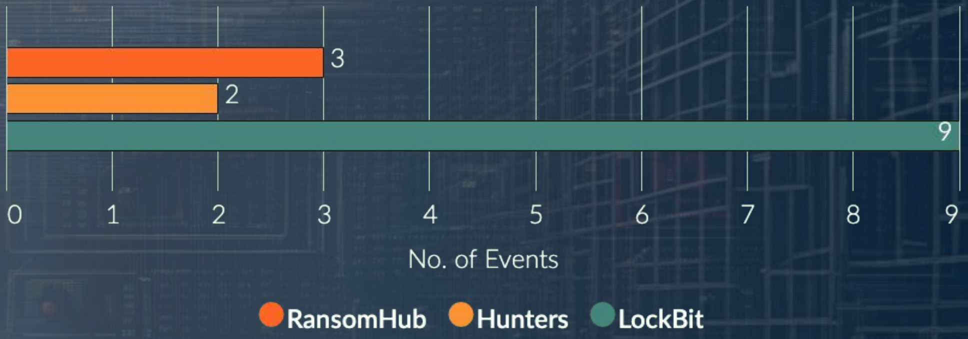
Africa

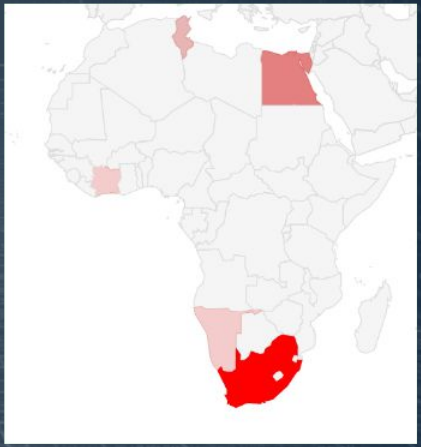
In Africa, various ransomware events impacted high profile organizations and a number of government administration entities.
LockBit was behind the attack on a bank in Namibia and a water management corporation and a government pension fund in South Africa.

Electric power operators were targeted in Egypt by DragonForce.

A number of automotive retailers in South Africa were targets of LockBit's attacks.

Attack Volume by Top Three Actors





Regional View

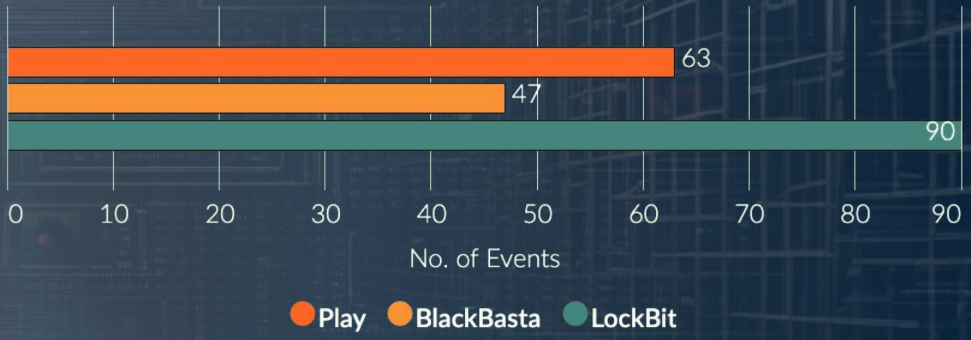
North and Central America and Caribbeans

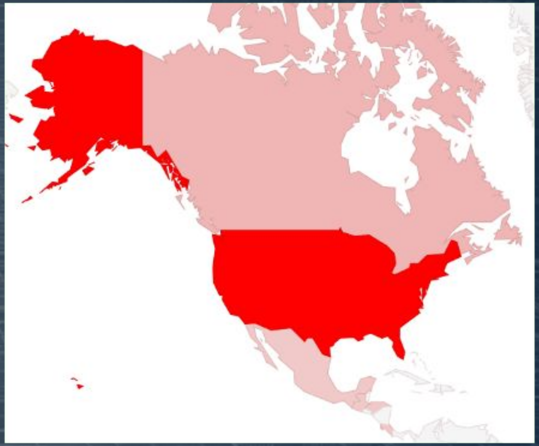
The United States and Canada are primary targets of cybercriminals, likely due to their large economies.

While LockBit has been the most active actor (at least until the Cronos operation), groups such as Akira and DragonForce claimed compromise of private companies engaged in sensitive sectors, including critical services, energy infrastructure, oil and gas.

In Central America, notable compromises impacted a Mexican telecommunication provider, meanwhile, in the Caribbeans, professional service providers, particularly law firms, were impacted.

Attack Volume by Top Three Actors





Regional View

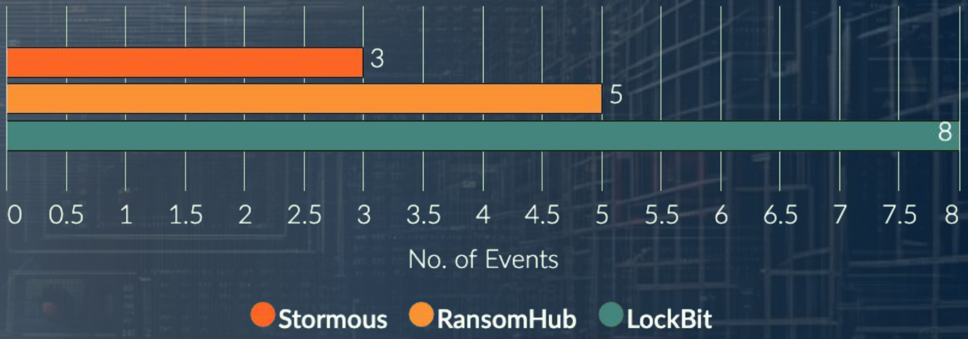
South America

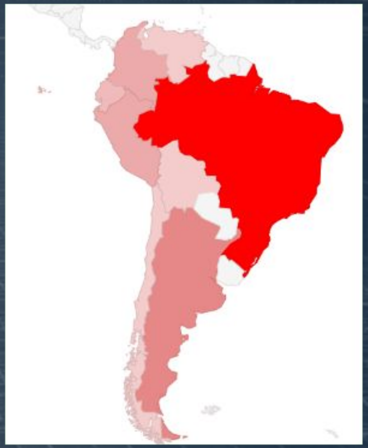
While nearly all countries in the region were targets of at least one attack, the Brazil was recipient of the majority of the attacks, with Argentina, Colombia and Peru following at distance.

Rhysida and IncRansom claimed compromise of a Peruvian government organization and a major oil and gas company with international interests.

A number of attacks targeted the telecommunication sector in Venezuela, Bolivia and Argentina.

Attack Volume by Top Three Actors





Access Brokers

Recent Trends In The Ransomware Landscape

LockBit, BlackCat/Alphv and BlackBasta affiliates were observed leveraging RustDoor, a Rust-based backdoor, as access broker for ransomware deployment. The malware was first observed disguised as a Visual Studio installer

With Qbot being targeted by law enforcement, PikaBot loader growingly grew in importance in the ransomware landscape

Beginning in January 2024, a malversating campaign was employed to spread DanaBot, a banking trojan linked to Cactus ransomware infection

The Defense Side

Attack Surface Management

Corporate VPNs are a frequent intrusion point for ransomware actors; in February 2024, Akira started targeting Cisco appliances via exploitation of CVE-2020-3259

BlackBasta has been linked to exploitation in the wild of ConnectWise ScreenConnect vulnerabilities (CVE-2024-1708 and CVE-2024-1709)

JetBrains TeamCity vulnerabilities (CVE-2024-27198 and CVE-2024-27199) have been reportedly exploited to deploy the Jasmin ransomware

Discover RansOmnia

Clipeus Intelligence Ransomware Intelligence Web Application

CLIPEUS INTELLIGENCE

A tool developed by intelligence analysts for intelligence analysts. We aim to facilitate collection and analysis of ransomware intelligence

We enable executives and CISOs to visualize strategic intelligence and convey it effectively to C-level decision-makers

Our objective is to support CTI, threat hunting and SOC teams with actionable tactical and operational intelligence

Check it out here: Clipeus Intelligence | RansOmnia

This document is intellectual property of Clipeus Intelligence OÜ (thereafter only “Clipeus Intelligence” or "Clipeus"), an Estonia-registered limited liability company.

The document has been prepared by Clipeus Intelligence based on collection and analysis of open source intelligence and publicly available information. The document has been prepared respecting the criteria of legality and privacy policies presented on the company's website. Unless agreed with the client, no active collection technique has been employed. No engagement with any threat actor was conducted.

Clipeus Intelligence is committed to the betterment of communities and of the security ecosystem. In this spirit, intelligence is always shared with jurisdictionally-competent law enforcement whenever the company encounters information of potential illicit or criminal relevance.

Ransomware victim names were not reported, even if they were already disclosed via press or other online sources.

For questions, reach out to info@clipeusintelligence.com, or visit our website.

Clipeus Intelligence OU (registration: 16862531)

Harju maakond, Tallinn, Kesklinna linnaosa, Ahtri tn 12, 15551