March 2023 broke ransomware attack records with 459 incidents

bleepingcomputer.com/news/security/march-2023-broke-ransomware-attack-records-with-459-incidents/

Bill Toulas

By
Bill Toulas

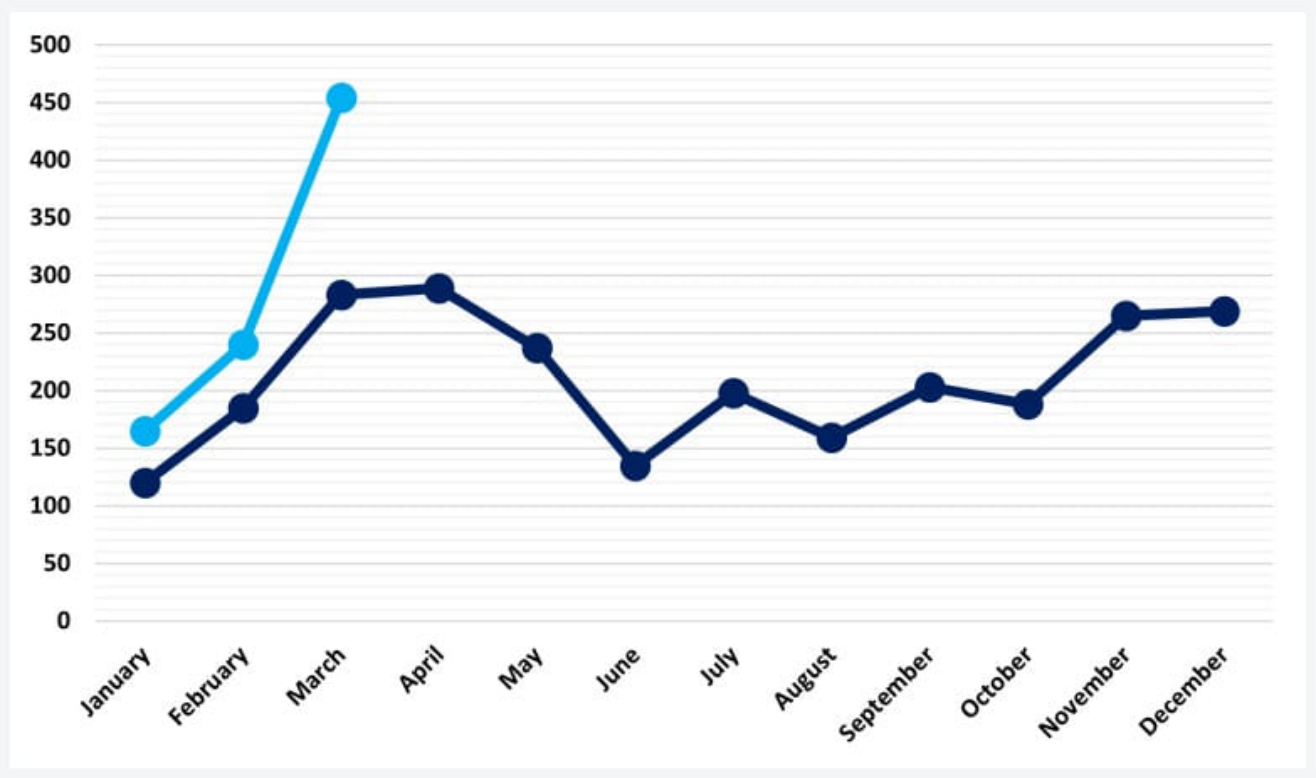
- April 19, 2023
- 03:00 AM
- 0

March 2023 was the most prolific month recorded by cybersecurity analysts in recent years, measuring 459 attacks, an increase of 91% from the previous month and 62% compared to March 2022.

According to NCC Group, which compiled a report based on statistics derived from its observations, the reason last month broke all ransomware attack records was CVE-2023-0669.

This is a vulnerability in Fortra's GoAnywhere MFT secure file transfer tool that the Clop ransomware gang exploited as a zero-day to steal data from 130 companies within ten days.

March 2023 activity continues the upward trend observed by NCC Group since the start of the year (January and February), with the highest number of hack and data leak incidents recorded in the past three years.



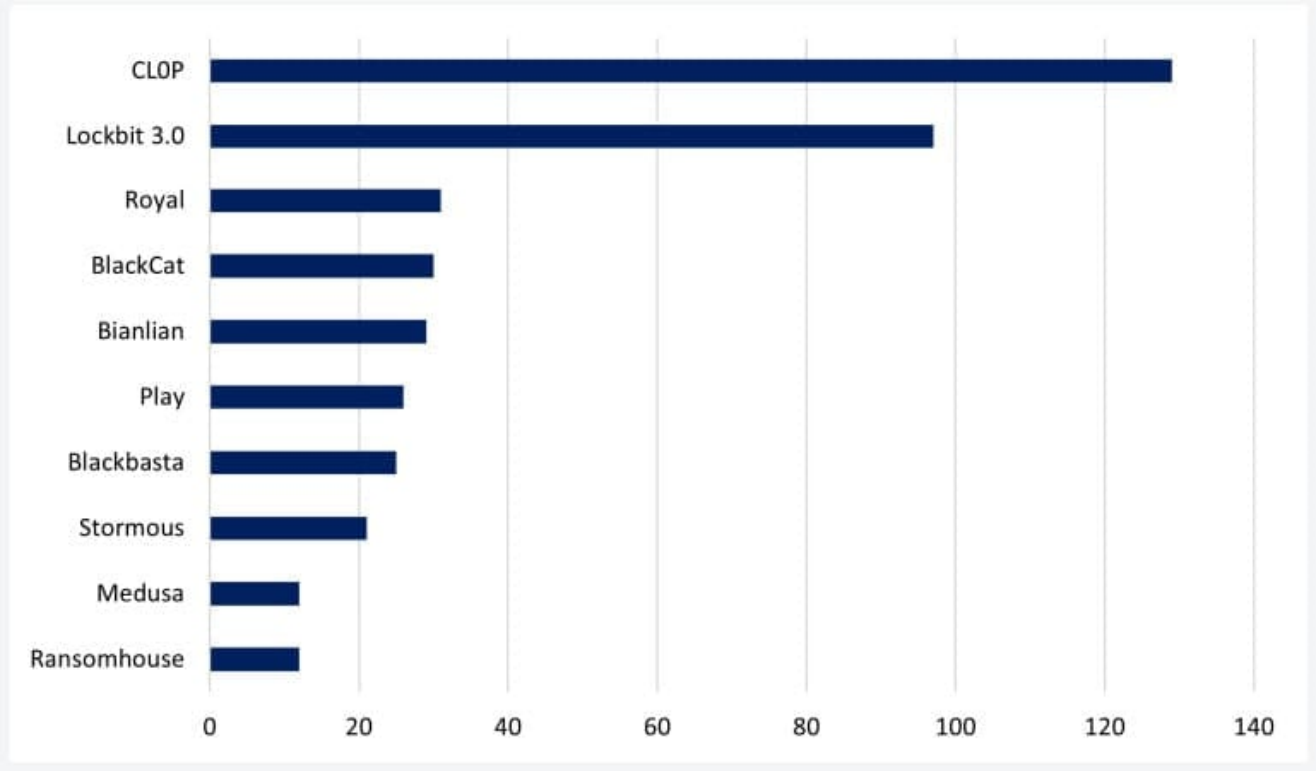
Monthly ransomware attack graph, dark blue: 2022, light blue: 2023 *(NCC Group)*

Activity spikes

Clop performed 129 recorded attacks last month, topping NCC Group's graph with the most active ransomware gangs for the first time in its operational history.

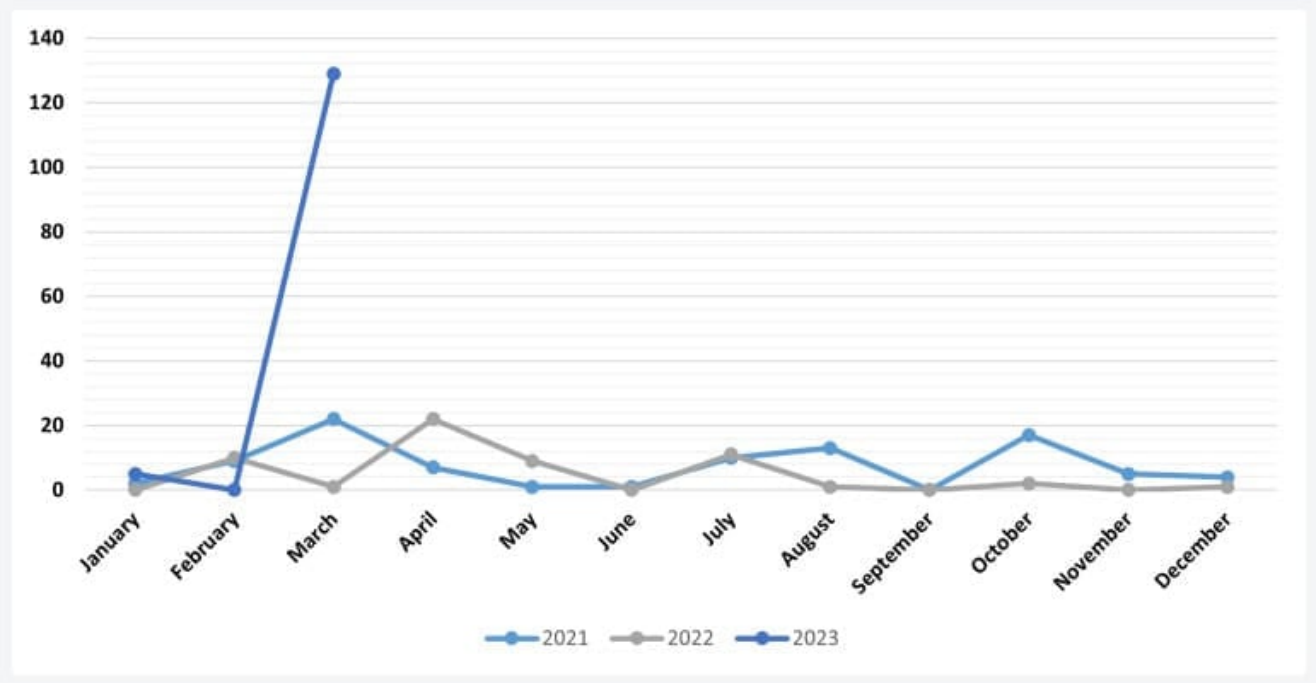
Clop's CVE-2023-0669 exploitation spree displaced LockBit 3.0, which had 97 recorded attacks, to second place for the second time since September 2021.

Other ransomware groups that had relatively significant activity during March 2023 are Royal ransomware, BlackCat (ALPHV), Bianlian, Play, Blackbasta, Stormous, Medusa, and Ransomhouse.



Threat actors with the most attacks last month *(NCC Group)*

This is not the first time Clop has performed a mass hack that propelled it to the top, as in early 2021, the ransomware group quickly amassed over 100 victims leveraging a zero-day vulnerability in Accellion's legacy File Transfer Appliance (FTA).

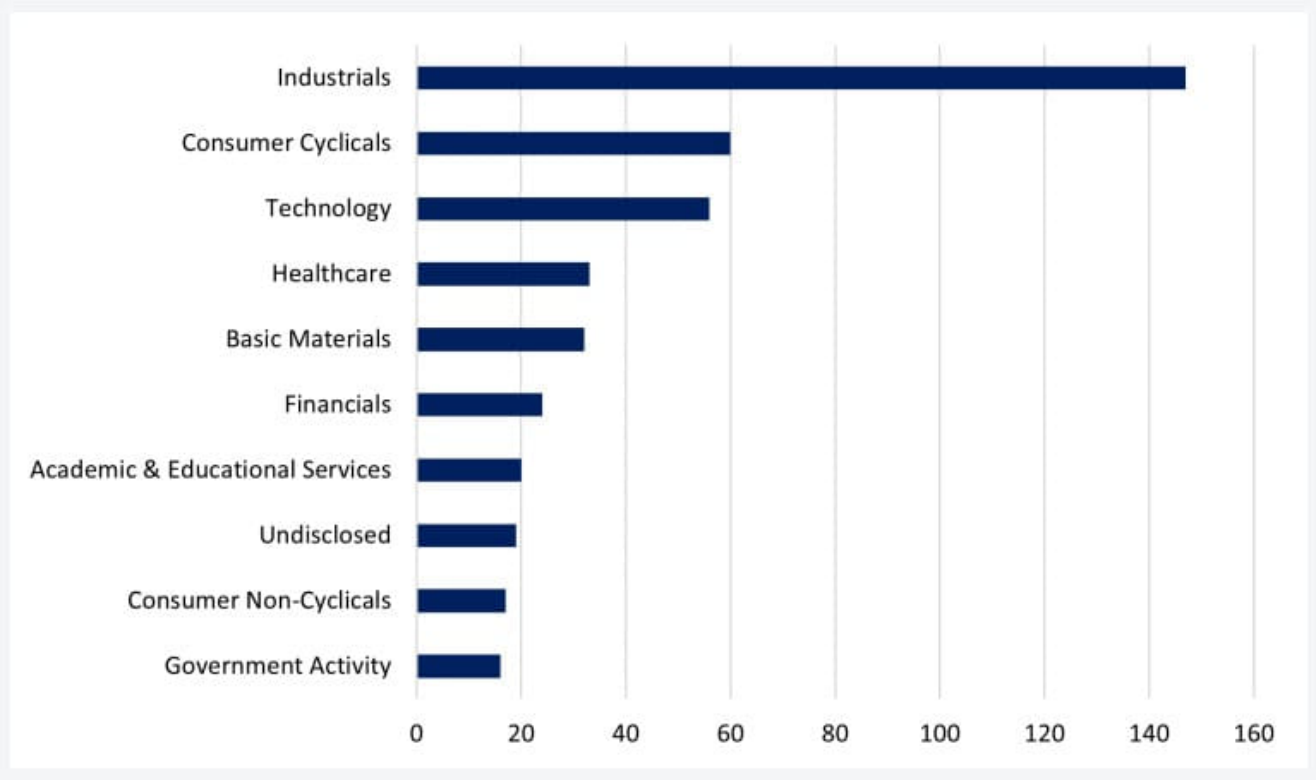


Clop ransomware activity spike *(NCC Group)*

Targeted sectors

The most targeted sector in March 2023 was "Industrials," receiving 147 ransomware attacks, accounting for 32% of the recorded attacks.

This sector includes professional and commercial services, machinery, tools, construction, engineering, aerospace & defense, logistics, transport services, and more.



Most targeted sectors by ransomware actors *(NCC Group)*

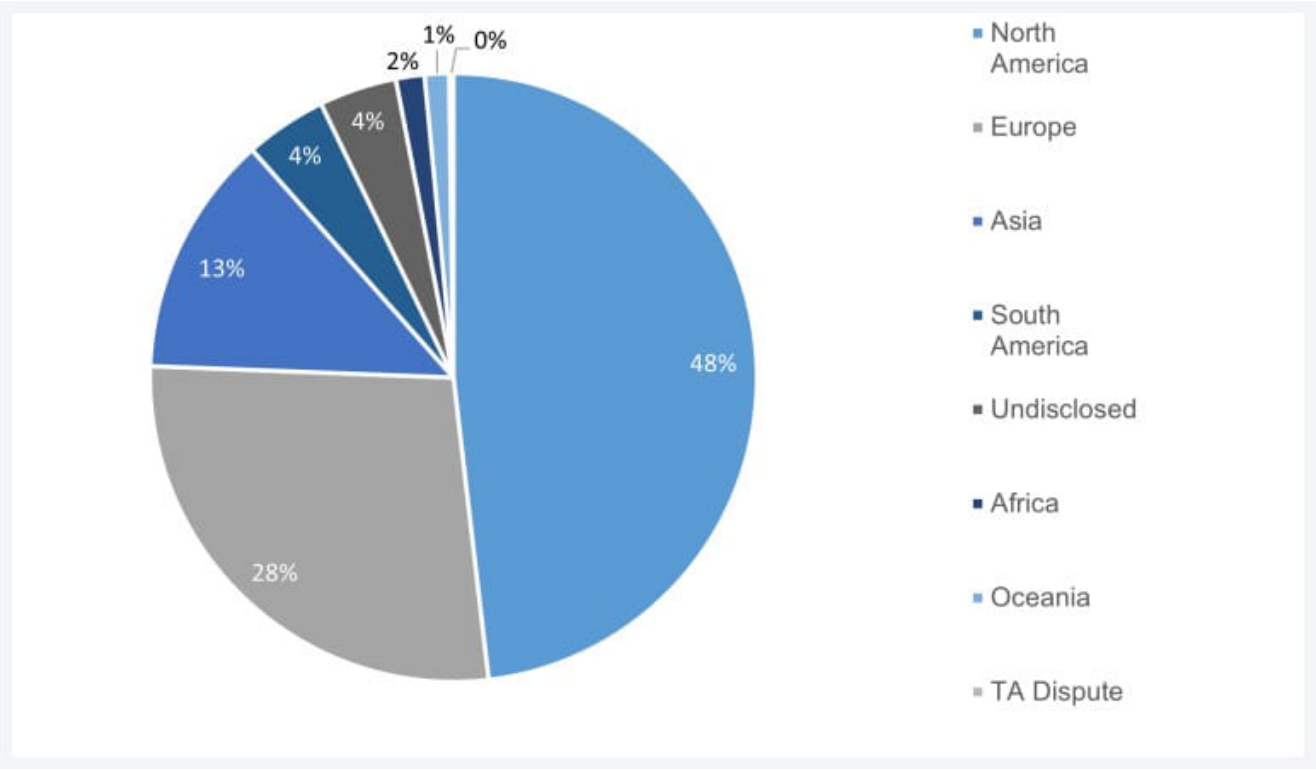
In second place are "Consumer Cyclicals," encompassing construction supplies, specialty retailers, hotels, automobiles, media & publishing, household goods, etc.

Other sectors that received significant attention from ransomware gangs are "Technology," "Healthcare," "Basic Materials," "Financials," and "Educational Services."

This month's three most active ransomware groups, namely Clop, LockBit, and Royal, primarily targeted companies within the "Industrials" sector. Clop and LockBit also directed a considerable amount of their efforts toward the "Technology" sector.

While these may be the most targeted sectors, it is important to note that ransomware attacks are usually not targeted but rather opportunistic.

Regarding the location of last month's victims, almost half of all attacks (221) breached entities in North America, Europe followed with 126 episodes, and Asia came third with 59 ransomware attacks.



Location of ransomware victims *(NCC Group)*

The recorded activity spike in March 2023 highlights the importance of applying security updates as soon as possible, mitigating potentially unknown security gaps like zero days by implementing additional measures and monitoring network traffic and logs for suspicious activity.

Related Articles:

City of Dallas hit by Royal ransomware attack impacting IT services

Brightline data breach impacts 783K pediatric mental health patients

The Week in Ransomware - April 28th 2023 - Clop at it again

Microsoft: Clop and LockBit ransomware behind PaperCut server hacks

Fortra shares findings on GoAnywhere MFT zero-day attacks

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.