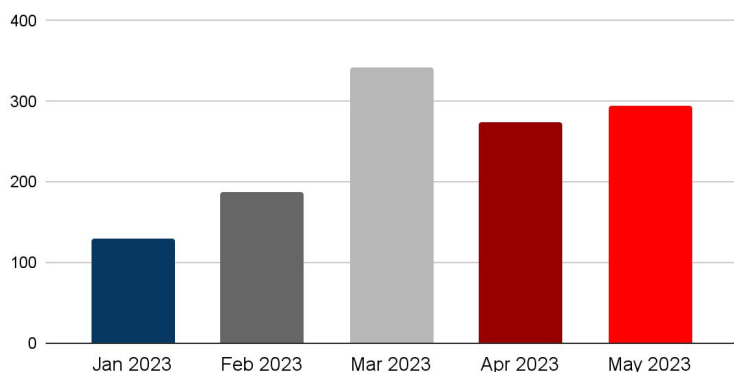


Ransomware and Digital Extortion Attacks on Upward Trajectory

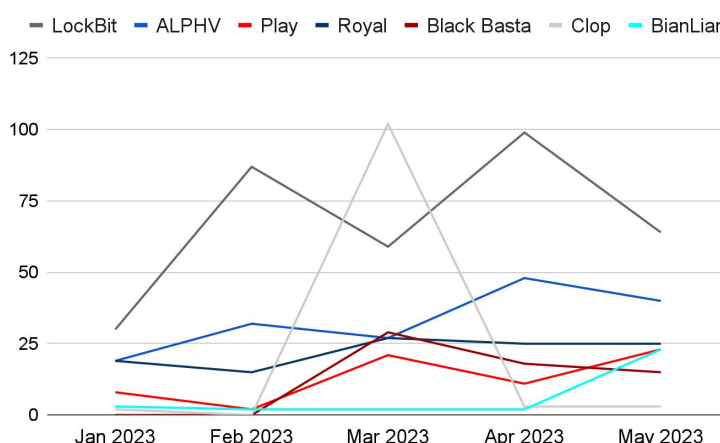
- ZeroFox Intelligence is observing an increased threat from ransomware and digital extortion. Following a significant uptick during Q1 2023, the number of monthly extortion incidents so far in Q2 2023 has increased further, with the total incidents this quarter very likely to exceed Q1 2023.
- Increased deployment of the most prolific ransomware strains has almost certainly underpinned the rising threat. Over April and May 2023, LockBit, ALPHV, BianLian, and Play each set new records for the highest number of victims in a given month.
- However, the recent emergence of new ransomware variants, such as Akira, CrossLock, and Cryptnet, is also very likely contributing to an overall increased threat. Since its inception in April 2023, Akira has claimed 27 victims, currently making it one of the top 10 most prolific strains in Q2 2023.
- Notably, the sustained rise in attacks comes despite a significant—and expected—drop in Clop activity. Following the widespread exploitation of CVE-2023-0669 in March 2023, Clop deployment has returned to typical levels, with a total of six attacks observed across April and May 2023.
- **It is a realistic possibility the increased activity is driven by a confluence of factors, including—but not limited to—increased ransomware-as-a-service proliferation, emboldened threat actors, and early indications that victims' susceptibility to paying ransoms is increasing, thereby encouraging further attacks. As a result, the ransomware and digital extortion threat will likely remain high over at least the coming three months.**

**Ransomware and Digital Extortion
Recorded Incidents in 2023**



Source: ZeroFox Intelligence

Prominent Ransomware Strains' Recorded Incidents



Source: ZeroFox Intelligence

Recommendations

- Regularly back up critical data, including password-protected copies of files kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Enable multi-factor authentication wherever possible.
- Disable PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.