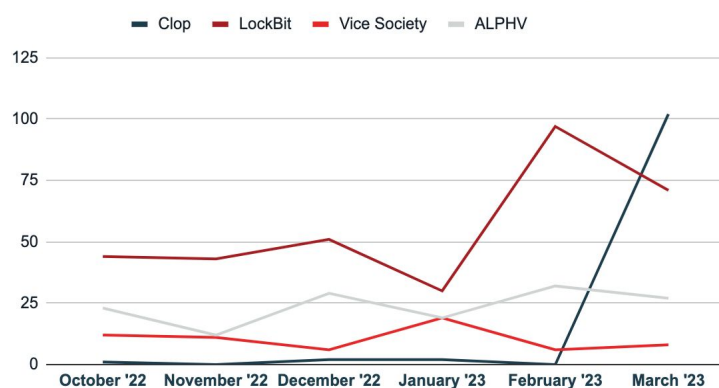


Clop Sets Record for Ransomware and Digital Extortion Incidents

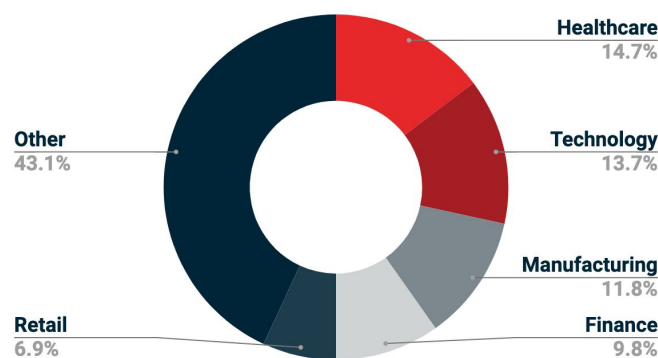
- In March 2023, the Clop digital extortion collective added 102 victims to its leak site. This is the highest number of digital extortion victims listed in a single month in ZeroFox Intelligence's records, as well as the first month in over a year that LockBit has not been the most prolific digital extortion operation.
- Clop's success is very likely due to its operators' successful January 2023 exploitation of CVE-2023-0669, a zero-day exploit in GoAnywhere MFT file transfer software.
- In February 2023, Clop claimed to have compromised over 130 organizations in this campaign, indicating that some victims may have chosen to pay ransom demands.
- While not on such a vast scale, Clop operators had widespread success in the exploitation of Accellion FTA file transfer service in 2020 and 2021, highlighting the multiplier effect that successful exploitation of vulnerabilities in these services can have.
- ZeroFox Intelligence anticipates that Clop's campaign will finish in April 2023, resulting in a significant drop in activity in coming months. As of this writing, ZeroFox Intelligence has identified no further digital extortion victims listed by Clop in April 2023.

Prominent Ransomware Strains Monthly Recorded Incidents



Source: ZeroFox Intelligence

Clop Targets by Industry: March 2023



Source: ZeroFox Intelligence

Recommendations

- Implement mitigations as outlined by the GoAnywhere software vendor, including:
 - Rotate organization Master Encryption Keys and review audit logs.
 - Revoke xposed GoAnywhere MFT instances with hosted credentials of users of other systems.
 - Update to GoAnywhere MFT version 7.1.2 as soon as possible.
- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new ransomware targets.
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise and metadata related to Ransomware.