

Finance sector

Notable news & breaches

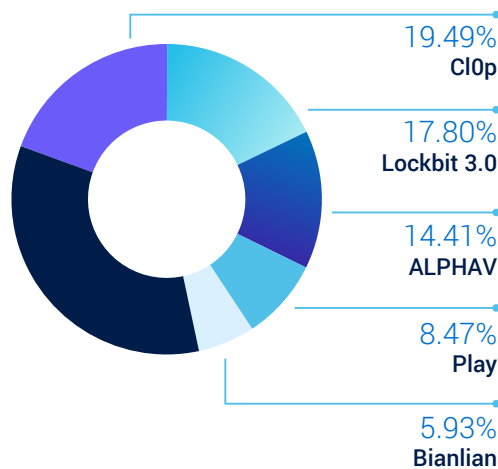
- 4.8 million impacted by data breach at TMX Finance.
- Financial fraud-focused cybercrime marketplace 'Styx' emerges.
- 3CX supply chain attack tied to financial trading app breach.
- Financial services company OneMain fined \$4.25 million for security lapses.
- Genworth Financial reports data breach leaking SSNs belonging to 2.7 million policyholders and customers.

Noteworthy threat actor

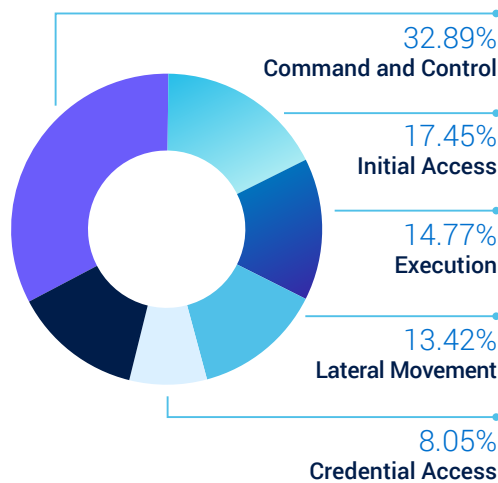
CL0P Ransomware Gang

After a quiet April and May, Cl0p surged back in June after exploiting the CVE-2023-34362 MOVEit vulnerability. Cl0p posted nearly 100 victims on their leak site, with around 1/3 falling within Financial Services or Insurance.

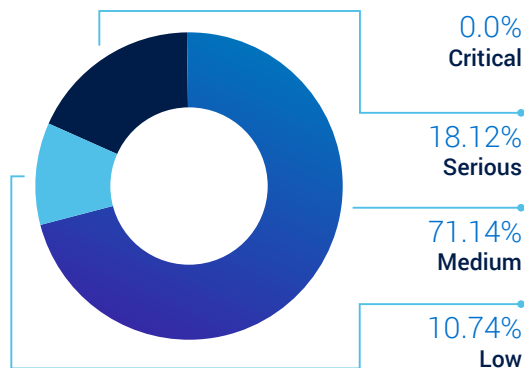
Top ransomware



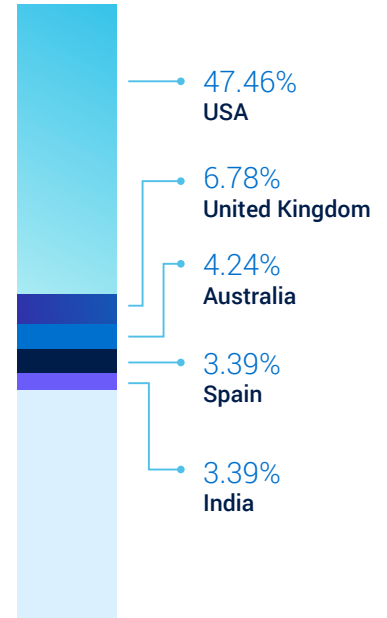
Incident MITRE tactics



Incident severity



Ransomware victim locations



Monthly victim trending

Ransomware	April	May	June
Cl0p	0	0	23
Lockbit 3.0	12	6	3
ALPHAV	8	4	5
Play	3	4	3
Bianlian	2	1	4

Recommendation

Q2 trends reiterate the need to assess vendor and supply chain security, and continuously review attack surface and vulnerability management approaches. We continue to observe that small gaps in these area lead to major breaches.