NTT Security Holdings

Insurance sector

Notable news & breaches

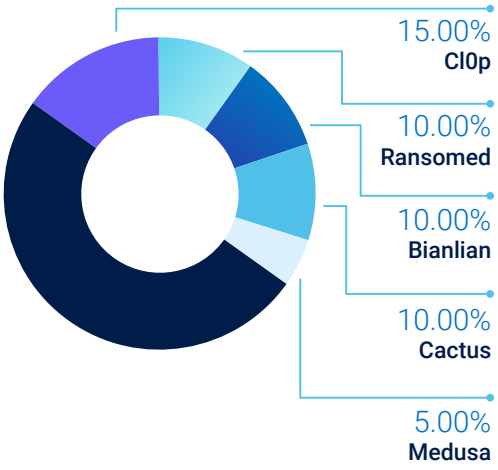
- A reflected cross-site scripting vulnerability targeting Japanese insurance companies for sale on dark web.
- Third party vendor exposes confidential customer data of Progressive Casualty Insurance Company.
- Multiple insurance and financial services organizations claimed by Cl0p as part of prior MOVEit exploitation.
- Nippon Life Insurance impersonated by a threat actor to steal customer PII via fake website redirection.
- Argentine National Institute of Social Services for Retirees and Pensioners disabled access to site and systems due to ransomware attack.

Noteworthy threat actor

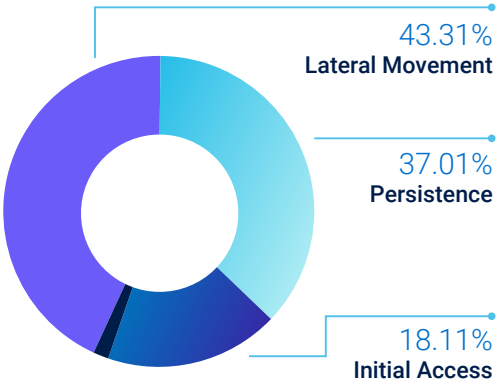
CL0P Ransomware Gang

Cl0p has continued surging in Q3 after exploiting the CVE-2023-34362 MOVEit vulnerability. Cl0p posted over 30 insurance and financial services victims on their leak site this past quarter.

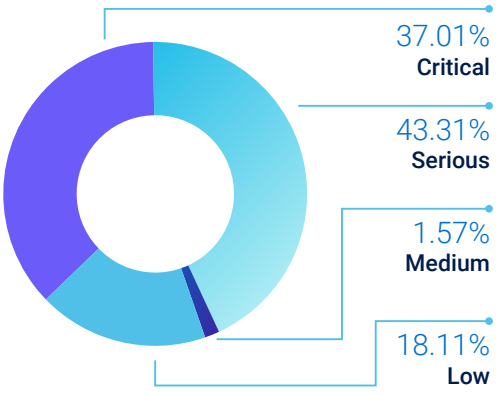
Top ransomware



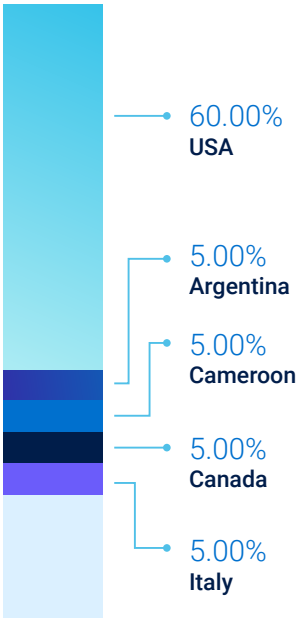
Incident MITRE tactics



Incident severity



Ransomware victim locations



Monthly victim trending

Ransomware	July	Aug	Sept
Cl0p	3	0	0
Bianlian	1	1	0
Ransomed	0	0	2
Cactus	0	0	2
Medusa	1	0	0

Recommendation

Ensure your organization has security training and user awareness around phishing and impersonation threats. GTIC has observed multiple campaigns targeting non-technical employees of insurance and financial service organizations.