NTT Security Holdings

Telecommunications sector

Notable news & breaches

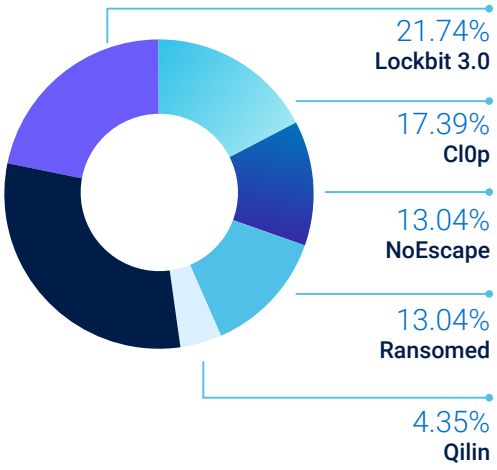
- RedEnergy, a new stealer-as-a-ransomware, targets telecom and other sectors via targeted social media lures.
- Multiple critical vulnerabilities affecting various Zyxel devices observed in the wild.
- Critical zero-day flaw impacting Ivanti Sentry actively exploited in the wild.
- Multiple zero-day vulnerabilities in Cisco ASA, Threat Defense and IOS allow initial access to corporate networks.
- ShroudedSnooper targets Middle Eastern telecommunications companies.

Noteworthy threat actor

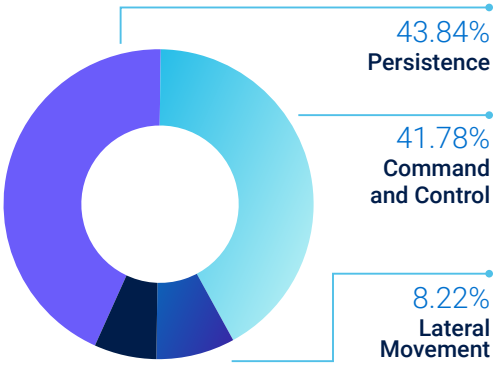
BlackTech

Chinese-linked threat actors BlackTech, have been targeting telecommunications, government and other industries in sophisiticated router attacks — pivoting from subsidiary to headquarters. CISA, NSA, FBI and Japan released a joint advisory (AA23-270A) with the threat actors TTPs.

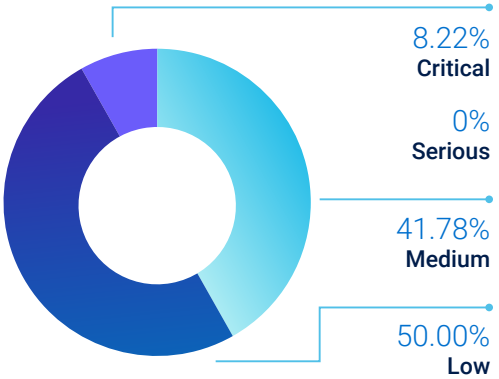
Top ransomware



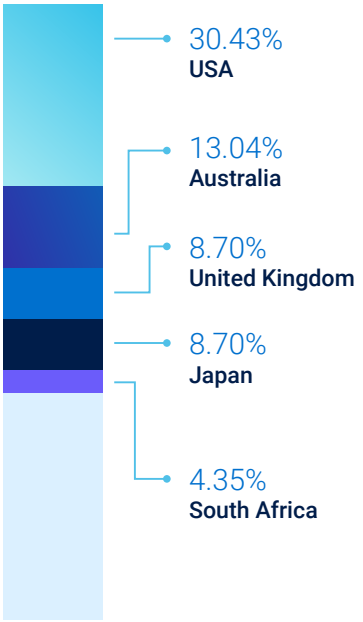
Incident MITRE tactics



Incident severity



Ransomware victim locations



Monthly victim trending

Ransomware	July	Aug	Sept
Lockbit 3.0	2	2	1
Cl0p	4	0	0
NoEscape	0	3	0
Ransomed	0	0	3
Bianlian	1	0	0

Recommendation

As noted in the 2023 Global Threat Intelligence report, attack surface awareness and monitoring is vital. The TTPs of BlackTech noted in the threat actor section highlight the shift of actors toward fringe network devices to avoid detection.