NTT | Security Holdings

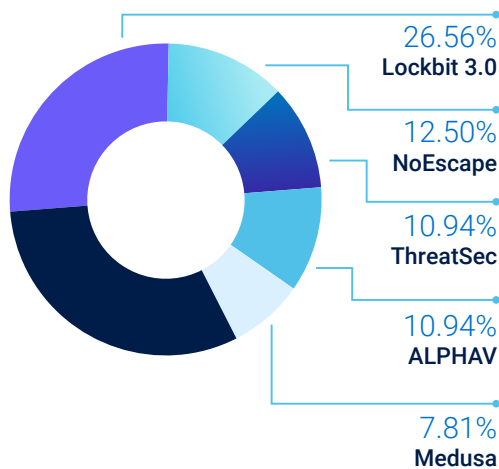# Government sector

Notable news & breaches

- Over 50% of United States ransomware incidents were municipalities with under 200 employees
- Security incident takes Kansas Court System offline for almost 2 weeks
- BlackSuit claimed the Government of Brazil on victim site
- Large Norwegian municipality, Stavanger, claimed by PLAY ransomware group
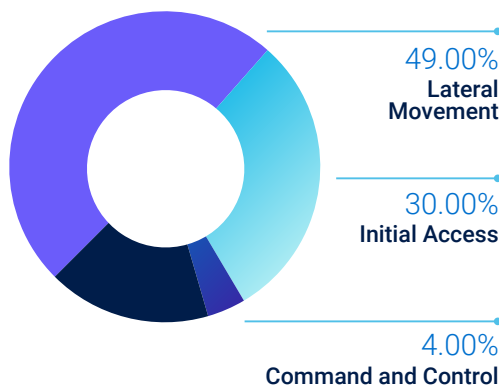
Noteworthy threat actor

ThreatSec

ThreatSec launched an extortion site in December 2023, listing data for several local governments. The group claims they are not financially motivated but aim to target governments they believe to be corrupt or oppressive.
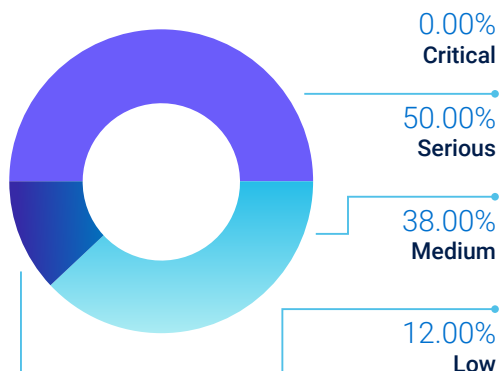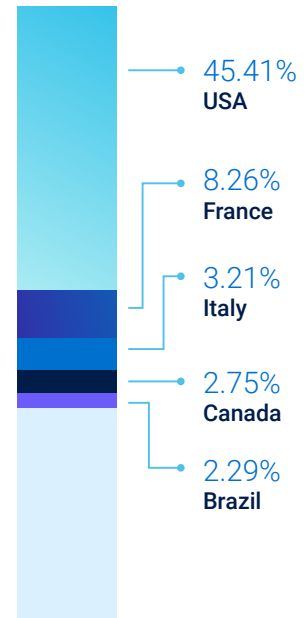
Top ransomware

26.56% Lockbit 3.0
12.50% NoEscape
10.94% ThreatSec
10.94% ALPHAV
7.81% Medusa

Incident MITRE tactics

49.00% Lateral Movement
30.00% Initial Access
4.00% Command and Control

Incident severity

0.00% Critical
50.00% Serious
38.00% Medium
12.00% Low

Ransomware victim locations

45.41% USA
8.26% France
3.21% Italy
2.75% Canada
2.29% Brazil

Monthly victim trending

Ransomware	Oct	Nov	Dec
Lockbit 3.0	2	9	6
NoEscape	6	2	0
ALPHAV	4	1	2
ThreatSec	0	0	7
Medusa	3	2	0

Recommendation

Smaller governments and municipalities should assess cybersecurity funding. In the US, the State and Local Cybersecurity Grant Program looks to aid state, local, and territorial (SLT) governments in reducing threats and cyber risk.