NTT Security Holdings

Education sector

Notable news & breaches

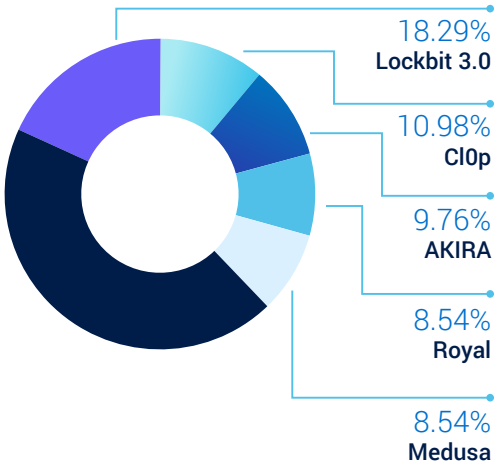
- Faculty databases from over 100 US school districts and universities for sale on BreachedForums 2.
- Cl0p claims major US universities such as UCLA, University of Georgia and Johns Hopkins.
- Greek Education Ministry online exam platform targeted by DDoS attack.
- Bl00dy Ransomware Gang exploits PaperCut vulnerabilities targeting Education sector.
- AvosLocker claimed responsibility for attack on Bluefield University, stealing over 1 TB of data.

Noteworthy threat actor

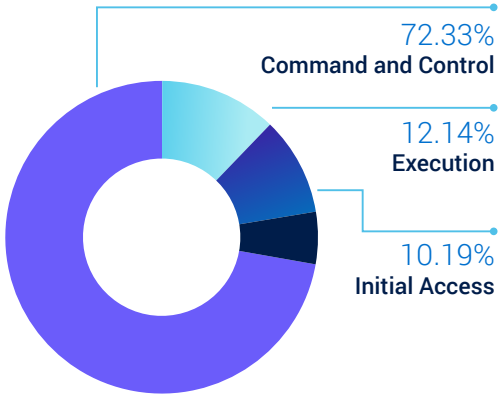
Bl00dy Ransomware Gang

Beginning in May 2023, Bl00dy Ransomware Gang was observed attempting to exploit newly discovered vulnerable PaperCut servers against the education facilities sector. Bl00dy specifically targeted CVE-2023-27350, a high severity vulnerability announced in Q1 of 2023 but still unpatched in many environments.

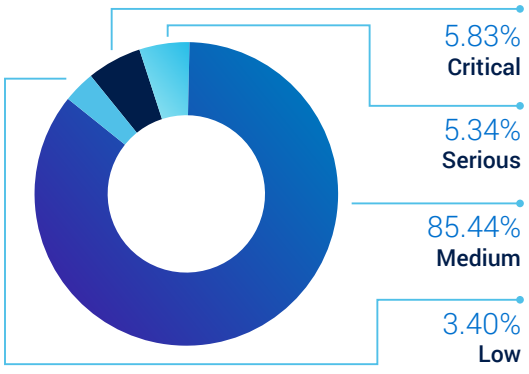
Top ransomware



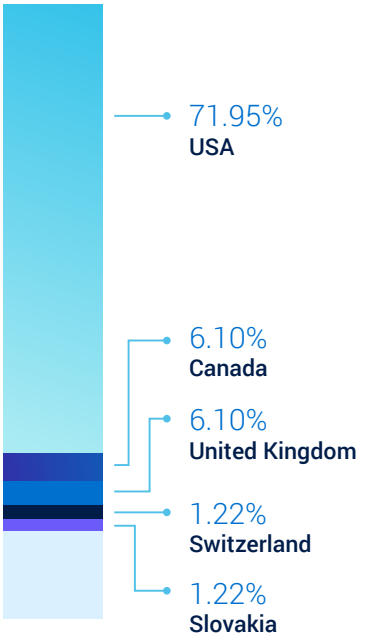
Incident MITRE tactics



Incident severity



Ransomware victim locations



Monthly victim trending

Ransomware	April	May	June
Lockbit 3.0	3	6	6
Cl0p	0	0	9
AKIRA	1	4	3
Royal	1	5	1
Medusa	3	1	3

Recommendation

Where feasible, some form of dark web monitoring should be leveraged by educational institutions to monitor for leaked credentials and compromised accounts. Using valid accounts is one key avenue for ransomware delivery, and in some cases the leaked data has led to secondary incidents.