NTT Security Holdings

Healthcare sector

Notable news & breaches

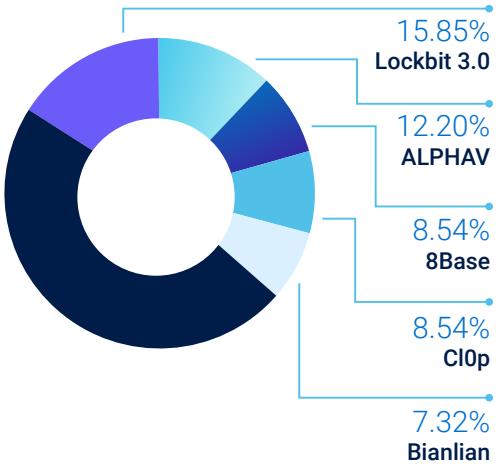
- Targeted phishing campaign attempts to steal patient information of dozens of prominent healthcare providers and associates in the United States.
- Johnson & Johnson Health Care Systems informed CarePath customers that their sensitive information has been compromised in a third-party data breach.
- Colorado Department of Health Care Policy & Financing (HCPF) fell victim to a supply chain attack, resulting in the breach of medical and health information.
- Health Sector Cybersecurity Coordination Center (HC3) warns healthcare organizations of Akira, a newer ransomware group that has been targeting healthcare organizations.
- Personal information linked to the Academy of Medicine in Singapore, including senior figures in the medical fraternity, has been put up on the Dark Web by Lockbit.

Noteworthy threat actor

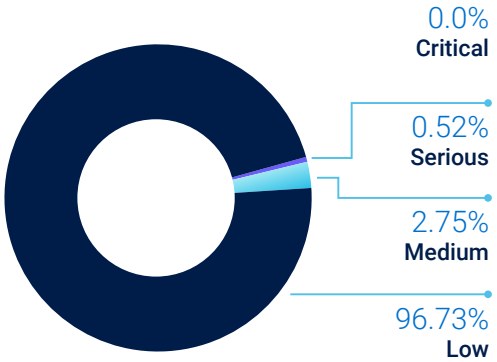
AtlasCross

A relatively new advanced persistent threat actor, AtlasCross, has been impersonating the American Red Cross. The actor delivers two Trojans, DangerAds and AtlasAgent.

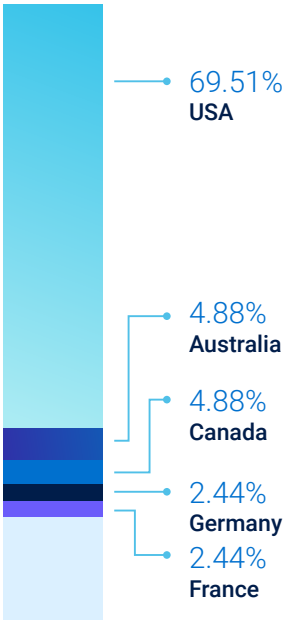
Top ransomware



Incident severity



Ransomware victim locations



Monthly victim trending

Ransomware	July	Aug	Sept
Lockbit 3.0	3	5	5
ALPHAV	1	1	8
8Base	3	3	1
Cl0p	7	0	0
Bianlian	3	2	1

Noteworthy Malware Muldrop

In Q3, GTIC observed a unique uptick in Muldrop variants and similar Trojan droppers for our healthcare customers. Below are the top TTPs for the most prevalent and recent samples.

ID	Technique	Variant Usage
T1027	Obfuscated Files or Information	80%
T1082	System Information Discovery	80%
T1083	File and Directory Discovery	60%
T1129	Shared Modules	45%
T1027.002	Software Packing	40%

Recommendation

As noted in the 2023 Global Threat Intelligence report, assessing third party vendor security is critical. The healthcare sector saw several high profile breaches as a result of poor or careless vendors.