CRYTICA SECURITY

If you can't detect, you can't protect.™

CYBER BREACH ANALYSIS
CASE STUDY

cloudnordic
The Nordic Cloud Experts

Date of Attack: August 19, 2023

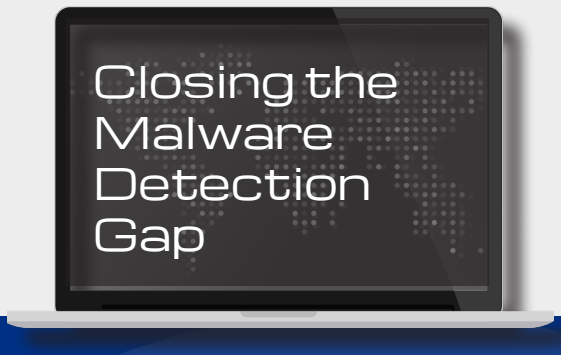
Malware Type: Ransomware

Attack Mechanism/Name: Malware was injected into "dormant servers" which, when reconnected to the network contained the malware, which then launched, spread throughout the network, and encrypted all of the data.

Damage Caused: Malware encrypted both the primary and backup systems. "the majority of our customers have thus lost all data" CloudNordic must start from scratch in rebuilding the company's IT systems.

Defenses Defeated: Not Known - but obviously not any systems that could detect new malware at the time of injection.

Defenses Defeated By: Malware that was not detected upon injection. The malware was resident in servers for a long time before it launched.



HOW CRYTICA WOULD HAVE HELPED

Crytica would have detected the malware IMMEDIATELY upon injection. The malware would not have been permitted to remain "dormant" in "dormant" servers. Upon detection, steps could have been taken to remove the malware before it launched.

info@cryticasecurity.com | 877-614-9300