Nefilim and Hive ransomware affiliate sentenced to 70 months in prison



A Ukrainian national has been sentenced to 70 months in prison for ransomware attacks between 2018 and 2021 that targeted hospitals, government entities and high-revenue businesses worldwide.

- The defendant is a Ukrainian national and was sentenced to 70 months in prison.
- He acted as an affiliate of the Nefilim and Hive ransomware operations.
- The attacks took place between 2018 and 2021.
- Targets included hospitals, government entities and high-revenue businesses worldwide.

What happened

A Ukrainian national has been sentenced to 70 months in prison for his part in ransomware attacks carried out between 2018 and 2021. According to the report, he took part as an affiliate of the Nefilim and Hive ransomware operations.

Who was targeted

The attacks hit hospitals, government entities and high-revenue businesses around the world. That mix of targets is a reminder that ransomware affiliates have gone after organisations where disruption is costly, including healthcare, the public sector and large commercial firms.

What it means for regulated institutions

The source reports the sentencing and does not describe new vulnerabilities or new attack activity, so no urgent technical response is implied. The case does show that affiliate-based ransomware activity can lead to prosecution, even years after the attacks. It is still a useful moment to confirm that ransomware readiness is in good order, especially in sectors resembling those named: health, government and large enterprises.

The source excerpt gives no further detail, such as the court, the amounts involved or specific victims, so we do not speculate on them.

What to do now

1. Confirm that offline or immutable backups exist for critical systems and that restoration has been tested recently.
2. Review the ransomware scenario in your incident response plan and confirm contacts and decision roles are current.
3. Check that privileged access and remote access paths are protected with multi-factor authentication.
4. Share the case with leadership as context for continued investment in ransomware resilience.