Nefilim Hackers Publish Oil Firm Data Online and Continue Campaign

By CBR Staff Writer

Published: 2020-06-09 · Archived: 2026-04-05 12:45:41 UTC

“Nefilim’s code shares many notable similarities with Nemty 2.5 ransomware"

A cyber criminal group known for its Nefilim (Netfilim) ransomware is continuing to target energy companies and has published an array of sensitive data belonging to India’s largest offshore drilling company Aban Offshore this week.

Cybersecurity firm Cyble has confirmed the data breach, which contains business sensitive information relating to the firm and its contractors, as well as more than 250 employee passport details.

Aban Offshore is India’s largest offshore drilling company and has done extensive work with Iranian firms in operating five offshore rigs. The latest information dump comes as a growing number of firms have been targeted and held to ransom by the hackers in recent months.

Trend Micro noted in a security blog: “Nefilim’s code shares many notable similarities with Nemty 2.5 ransomware; the main difference is the fact that Nefilim has done away with the Ransomware-as-a-Service (RaaS) component. It also manages payments via email communication rather than through a Tor payment site.”

The ransomware uses AES-128 encryption to lock a victim's files. All files are also marked with a 'Nefilim' string to the files so if a file is oil.doc it would be marked as oil.doc.nefilim. In order to decrypt these files the victim requires the RSA private key held by the hackers.

Nefilim Operator's Campaign in Full Swing

The Nefilim ransomware hackers are proving to be a significant threat for companies as they have breached a number of systems and are not hesitant to publish sensitive data online.

Yet it's not just energy firms that are being targeted as Australian-based logistics behemoth Toll Group was also a victim of the campaign in May which successfully breached a Toll Group server. The logistic firm turned down any attempt to engage with the hackers and pay a fee to restore their system.

Toll Group stated in May that: "After detecting this attack, we shut down our IT systems to mitigate the risk of further infection. Toll has refused from the outset to engage with the attacker's ransom demands, which is consistent with the advice of cyber security experts and government authorities."

"Our ongoing investigations have established that the attacker has accessed at least one specific corporate server. This server contains information relating to some past and present Toll employees, and details of commercial agreements with some of our current and former enterprise customers. The server in question is not designed as a repository for customer operational data."

The hackers subsequently published a cache of the data on the dark web. Toll Groups last public update on the incident was at the end of May in which they noted that they were still in the process of restoring 'key online systems.'

Ransomware is a serious issue for firms and is getting more sophisticated as just last February the UK's cyber agency NCSC updated its guidance as it had seen "numerous incidents where ransomware has not only encrypted the original data on-disk, but also connected USB and network storage drives holding data backups."

So all precautions should be taken to ensure that threat actors don't get access to networks as the damage could be permanent.

See Also: DWP Wraps Up Mammoth "Job Seeker's" Mainframe to X86 Migration

More Relevant

from future marketing communications. Our services are intended for corporate subscribers and you warrant that the email address submitted is your corporate email address.
