Toll Group hit by ransomware a second time, deliveries affected

By Lawrence Abrams

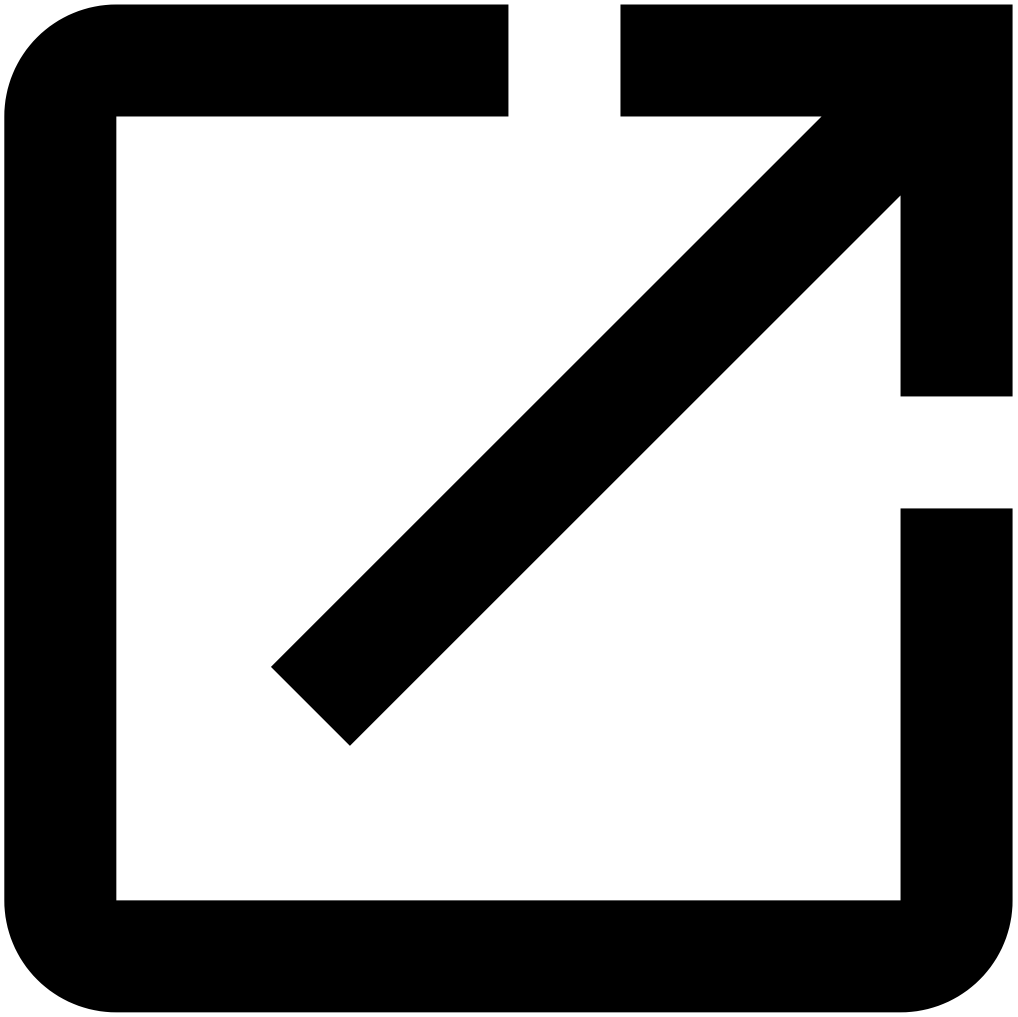
Published: 2020-05-05 · Archived: 2026-04-05 14:04:55 UTC

The Toll Group has suffered its second ransomware cyberattack in three months, with the latest one conducted by the operators of the Nefilim Ransomware.

Toll Group is Asia Pacific's leading provider of trans portion and logistics services, employing roughly 44,000 people at 1,200 locations in more than 50 countries.

On February 5th, 2020, Toll Group announced that they had suffered a cyberattack by a new ransomware variant called Mailto that required them to shut down their network to prevent more devices from being encrypted.


DIE LINKE.
0:00



Visit Advertiser websiteGO TO PAGE

This action led to some disruptions in their customer-facing applications.

A second attack by the Nefilim ransomware

In an announcement today, Toll Group states that they have suffered another attack that has caused them to shut down their systems again. This time the cyberattack was conducted by the operators of the Nefilim Ransomware.

"Toll took the precautionary step yesterday of shutting down certain IT systems after we detected unusual activity on some of our servers.

As a result of investigations undertaken so far, we can confirm that this activity is the result of a ransomware attack. Working with IT security experts, we have identified the variant to be a relatively new form of ransomware known as Nefilim. This is unrelated to the ransomware incident we experienced earlier this year. Toll has no intention of engaging with any ransom demands, and there is no evidence at this stage to suggest that any data has been extracted from our network. We are in regular contact with the Australian Cyber Security Centre (ACSC) on the progress of the incident."

The Nefilim Ransomware is a relatively new Ransomware-as-a-Service operation created by the developer of the Nemty Ransomware and a private group of malware distributors.

This group has been actively looking for threat actors experienced in spamming and gaining access to remote networked computers to launch network-wide corporate attacks.

While the Toll Group states that there is no evidence of any data being stolen, Nefilim is known for stealing unencrypted files and using it as leverage to get victims to pay the ransom.

This further extortion tactic is done through a "Leaks" site that they have created where they threaten to release stolen data if a victim does not pay.

As pointed out by security researcher Troy Mursch of Bad Packets Report, the Toll Group was utilizing a vulnerable Ctrix ADC Netscaler server in the first attack and continued to do so during the latest one.

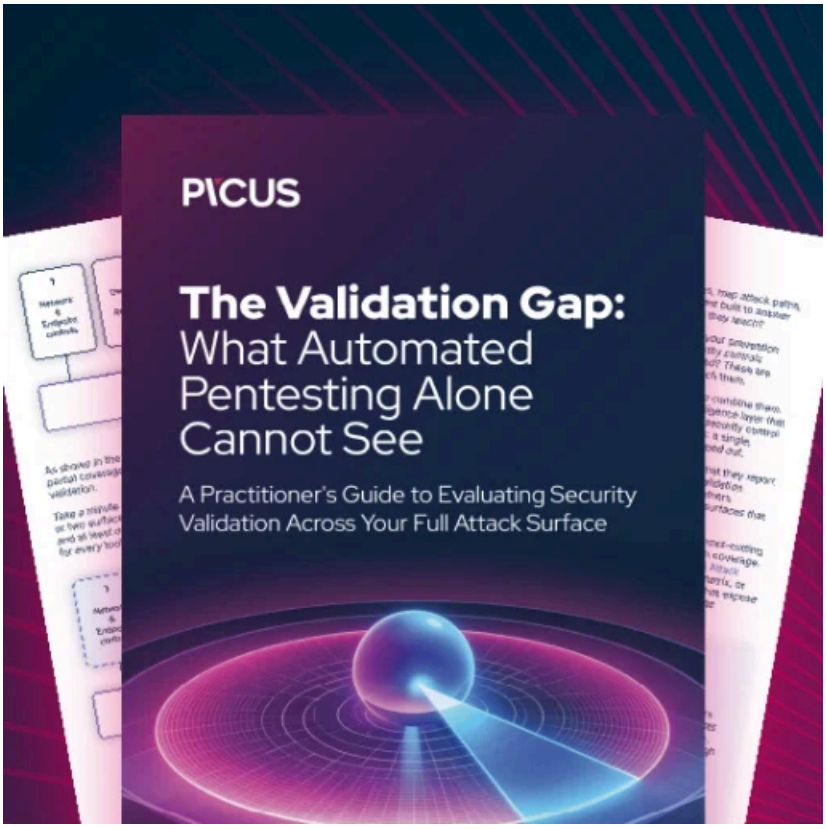
Shut down impacting deliveries

In a tweet posted by Toll Group, they state that they have had to shut down their "MyToll" shipping portal customer site as part of their defense against the ransomware attack.

In reply to the tweet, customers have stated that their deliveries have been impacted as without MyToll they are unable to redirect shipments to another collection center.

BleepingComputer has contacted the Toll Group with questions related to the attack but has not heard back as of yet.

Update 5/6/20: Included information about Citrix ADC Netscaler device



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/toll-group-hit-by-ransomware-a-second-time-deliveries-affected/