Australian cybersecurity agency warns of spike in LockBit ransomware attacks

By Catalin Cimpanu

Published: 2023-01-18 · Archived: 2026-04-10 03:09:04 UTC

Australia's cybersecurity agency has issued a security advisory on Friday warning about a sudden spike in LockBit ransomware attacks across the country.

The Australian Cyber Security Centre (ACSC) said that while the LockBit ransomware gang has attacked Australian companies since 2020, the agency has seen "a sharp and significant increase in domestic victims in comparison to other tracked ransomware variants" since July 2021.

"The ACSC has observed LockBit affiliates successfully deploying ransomware on corporate systems in a variety of sectors including professional services, construction, manufacturing, retail and food," the agency said today.

LockBit 2.0 — a perfect storm

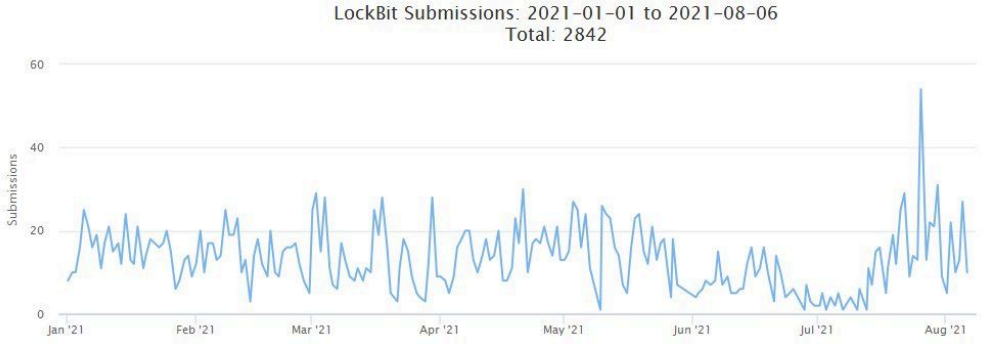
The ACSC warning comes after the LockBit operation has seen what can be described as an influx of "affiliates."

Operating on a *Ransomware-as-a-Service* model, the LockBit gang rents access to their ransomware to other threat actors (commonly referred to as *affiliates*), who are then responsible for breaching enterprise networks to steal data, and then deploy the ransomware payload to encrypt local copies.

While the LockBit gang has been operating since September 2019 with a modicum of success, they launched a new version of their RaaS platform in June 2021.

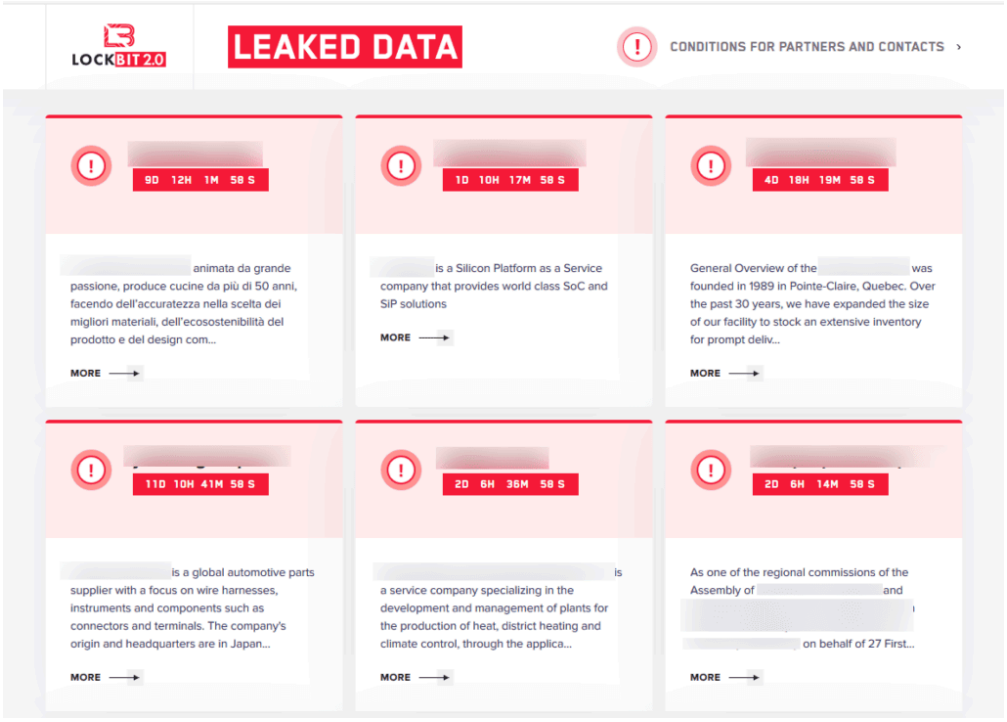
This launch coincided with the shutdowns of the Darkside, REvil, and Avaddon ransomware operations, which had the side effect of drawing many of those gang's affiliates to its platform, as Brett Callow, a malware analyst for security firm Emsisoft pointed out last month.

This resulted in a general spike of LockBit attacks, which can be easily seen in the chart below, showing submissions to ID-Ransomware, a web-based tool for identifying what type of ransomware has infected a victim.



The ACSC is now warning Australian companies to take note of this rise in LockBit affiliate activity and prepare for attacks. The agency particularly warns companies to patch their Fortinet networking devices for CVE-2018-13379, a vulnerability that has been identified as the entry point for many LockBit 2.0 attacks.

Furthermore, the agency also warns companies that once their files are encrypted, if they choose not to pay the threat actor and recover from backups, the LockBit gang is one of the ransomware cartels that operates a site on the dark web where they leak data from companies that refused to pay, so victims should be prepared to deal with a public data leak once they got hit.



No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
