Bridgestone Americas confirms ransomware attack, LockBit leaks data

bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-attack-on-bridgestone-americas/

Ionut Ilascu

By
Ionut Ilascu

- March 11, 2022
- 04:28 PM
- 0

A cyberattack on Bridgestone Americas, one of the largest manufacturers of tires in the world, has been claimed by the LockBit ransomware gang.

The threat actor announced that they will leak all data stolen from the company and launched a countdown timer, which is currently at less than three hours.

Timer activated

Bridgestone has tens of production units across the world and over 130,000 employees (regular and contractual), as per the company's data at the end of 2020.

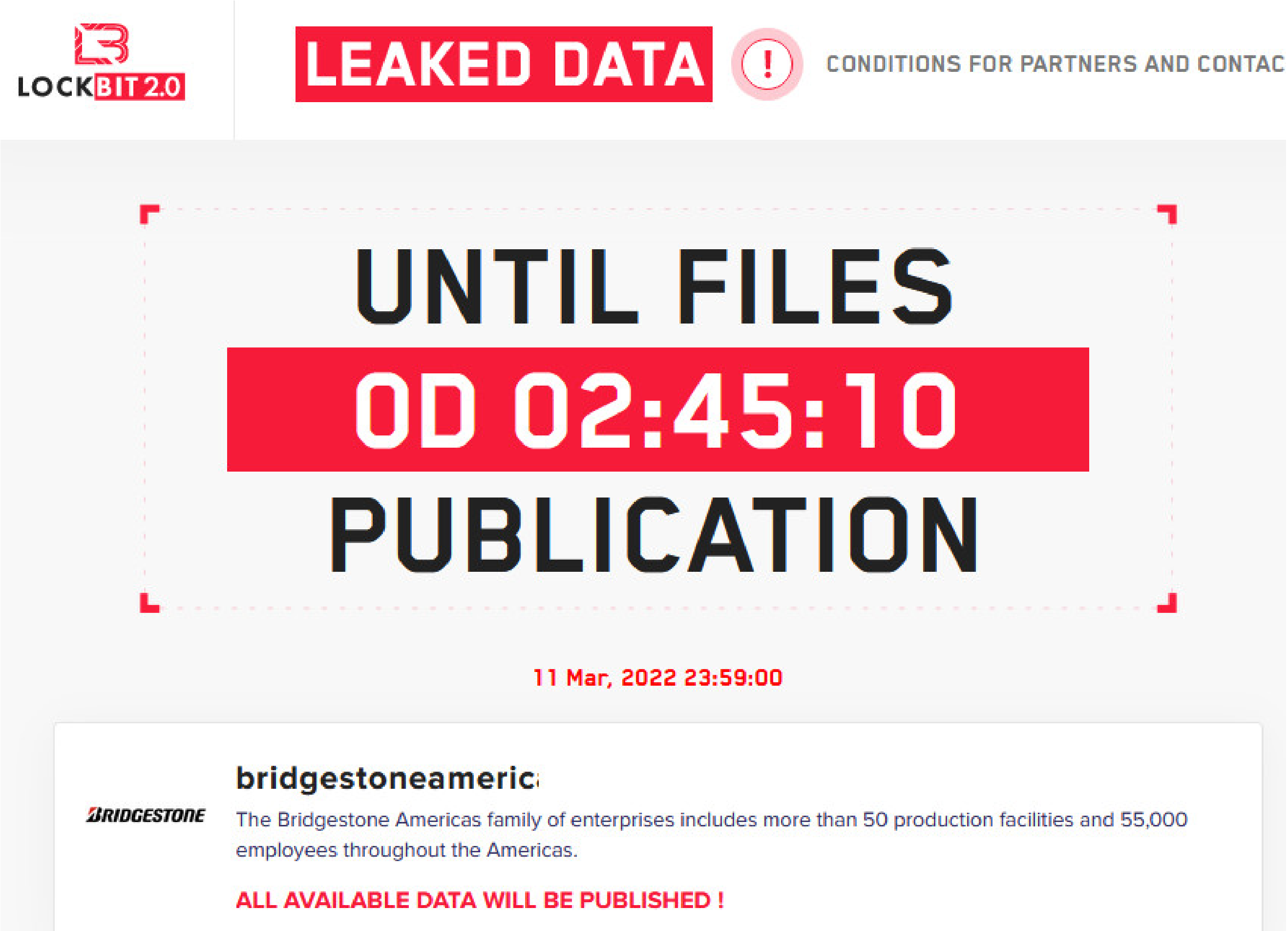
On February 27, Bridgestone started to investigate "a potential information security incident" detected in the morning hours of the same day.

"Out of an abundance of caution, we disconnected many of our manufacturing and retreading facilities in Latin America and North America from our network to contain and prevent any potential impact," Bridgestone said in a statement to media.

No details about the incident emerged until today when the LockBit ransomware gang claimed the attack by adding Bridgestone Americas to the list of their victims.

LockBit is one of the most active ransomware gangs today, targeting large corporations, sometimes asking for ransoms of tens of millions of U.S. dollars, as was the case with Accenture.

It is unclear what data LockBit stole from Bridgestone or how detrimental leaking it would be to the company. At the time of writing, the countdown from the actor for publishing the files expires in about three hours and a half.



UNTIL FILES
0D 02:45:10
PUBLICATION

11 Mar, 2022 23:59:00

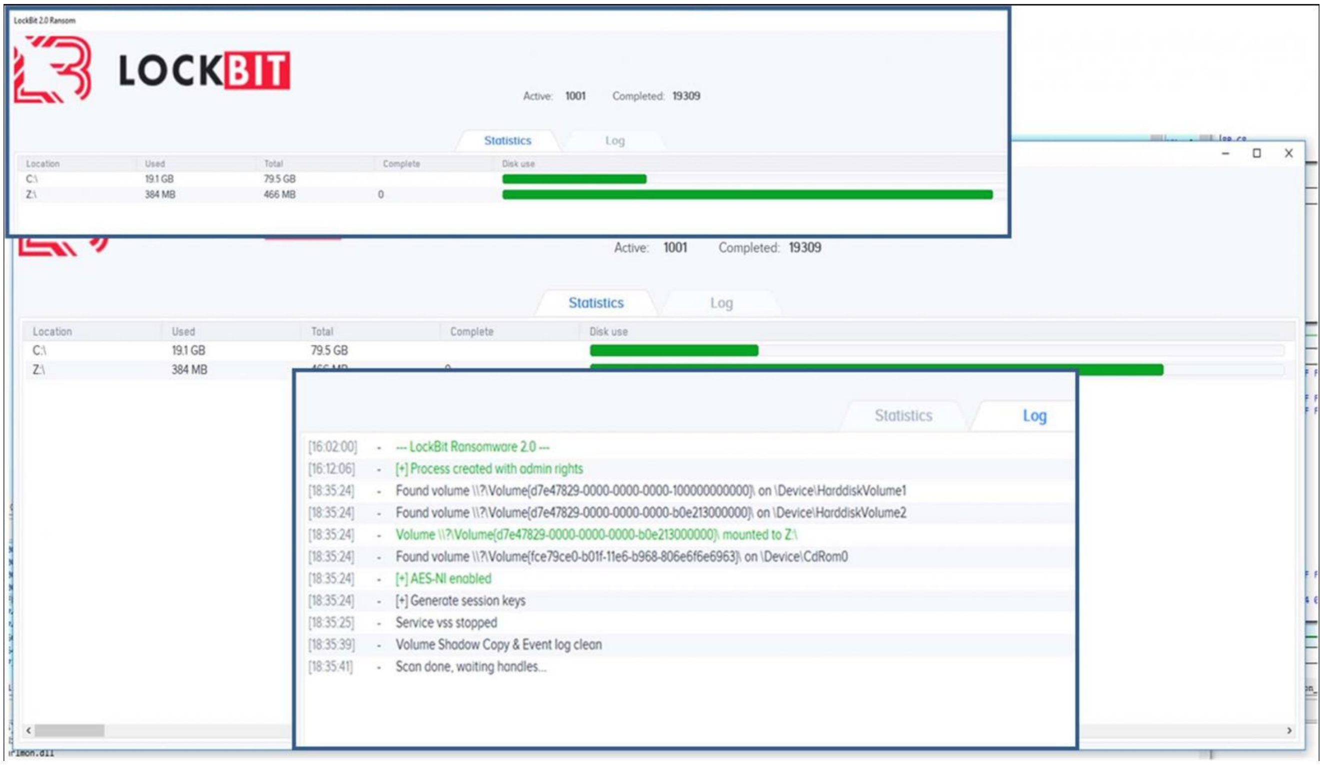
bridgestoneameric

The Bridgestone Americas family of enterprises includes more than 50 production facilities and 55,000 employees throughout the Americas.

ALL AVAILABLE DATA WILL BE PUBLISHED !

In a report last month, industrial cybersecurity company Dragos notes that LockBit was the most active ransomware actor targeting the industrial sector last year, with 103 attacks, followed by the Conti gang with 63.

The FBI in early February shared technical details and defense tips for LockBit ransomware attacks, noting that a bug in the malware allows showing a hidden debug window to view in real-time the state of data destruction.



Active: 1001 Completed: 19309

Location	Used	Total	Complete	Disk use
C:\	19.1 GB	79.5 GB		🟩
Z:\	384 MB	466 MB	0	🟩

```
[16:02:00]  -  --- LockBit Ransomware 2.0 ---
[16:12:06]  -  [+] Process created with admin rights
[18:35:24]  -  Found volume \\?\Volume{d7e47829-0000-0000-0000-100000000000}\ on \Device\HarddiskVolume1
[18:35:24]  -  Found volume \\?\Volume{d7e47829-0000-0000-0000-b0e213000000}\ on \Device\HarddiskVolume2
[18:35:24]  -  Volume \\?\Volume{d7e47829-0000-0000-0000-b0e213000000}\ mounted to Z:\
[18:35:24]  -  Found volume \\?\Volume{fce79ce0-b01f-11e6-b968-806e6f6e6963}\ on \Device\CdRom0
[18:35:24]  -  [+] AES-NI enabled
[18:35:24]  -  [+] Generate session keys
[18:35:25]  -  Service vss stopped
[18:35:39]  -  Volume Shadow Copy & Event log clean
[18:35:41]  -  Scan done, waiting handles...
```

BleepingComputer has reached out to Bridgestone Americas for a statement on the recent incident but did not hear back by publishing time.

Update [March 11, 16:36 EST]: Bridgestone Americas replied to BleepingComputer's request for comments saying that it is working with *Accenture Security* "to investigate and understand the full scope and nature of the incident" and that they are analyzing to determine what data was stolen.

The full statement below:

On February 27, 2022, Bridgestone Americas detected an IT security incident. Since then, we have proactively notified federal law enforcement and are staying in communication with them. We are also working around the clock with external security advisors, Accenture Security, to investigate and understand the full scope and nature of the incident. We have determined this incident to be the result of a ransomware attack. We have no evidence this was a targeted attack. Unfortunately, ransomware attacks similar to this one are increasing in sophistication and affecting thousands of organizations of all sizes.

As part of our investigation, we have learned that the threat actor has followed a pattern of behavior common to attacks of this type by removing information from a limited number of Bridgestone systems and threatening to make this information public.

We are committed to conducting a swift and decisive investigation to determine as quickly as possible what specific data was taken from our environment. Bridgestone treats the security of our teammates, customers, and partners' information with the utmost importance. We will continue to communicate with them often, working together to mitigate potential harm from these types of incidents and to further enhance our cybersecurity measures as recommended by our internal and external security advisors.

Related Articles:

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

The Week in Ransomware - April 15th 2022 - Encrypting Russia

LockBit ransomware gang lurked in a U.S. gov network for months

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.