Data leak marketplaces aim to take over the extortion economy

bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/

Lawrence Abrams

By
Lawrence Abrams

- May 7, 2021
- 08:16 AM
- 0

Cybercriminals are embracing data-theft extortion by creating dark web marketplaces that exist solely to sell stolen data.

Long before ransomware gangs started extorting victims through the use of stolen data, other threat actors had already been using this practice.

One well-known and highly publicized hacker who performed this practice was The Dark Overlord, who stole data and demanded ransoms from Disney, Netflix, and insurance companies.

The Maze Ransomware group revolutionized ransomware operations in 2019 by adopting a double-extortion strategy. Using ransomware data leak sites, Maze warned victims that they would publicly leak stolen data if victims did not pay a ransom.

Other gangs quickly adopted this extortion tactic.

Some threat actors have told BleepingComputer that the practice of stealing data and threatening to release it often generates more ransom payments than the loss of encrypted files.

You can see this shift in tactics with Babuk ransomware's recent announcement that they would no longer encrypt devices and are moving solely to data-theft extortion.

The rise of stolen data marketplaces

With breaches happening almost every day, and governments issuing heavy fines for the exposure of personal information, threat actors are now capitalizing on these fears by using dedicated marketplaces that sell stolen data.

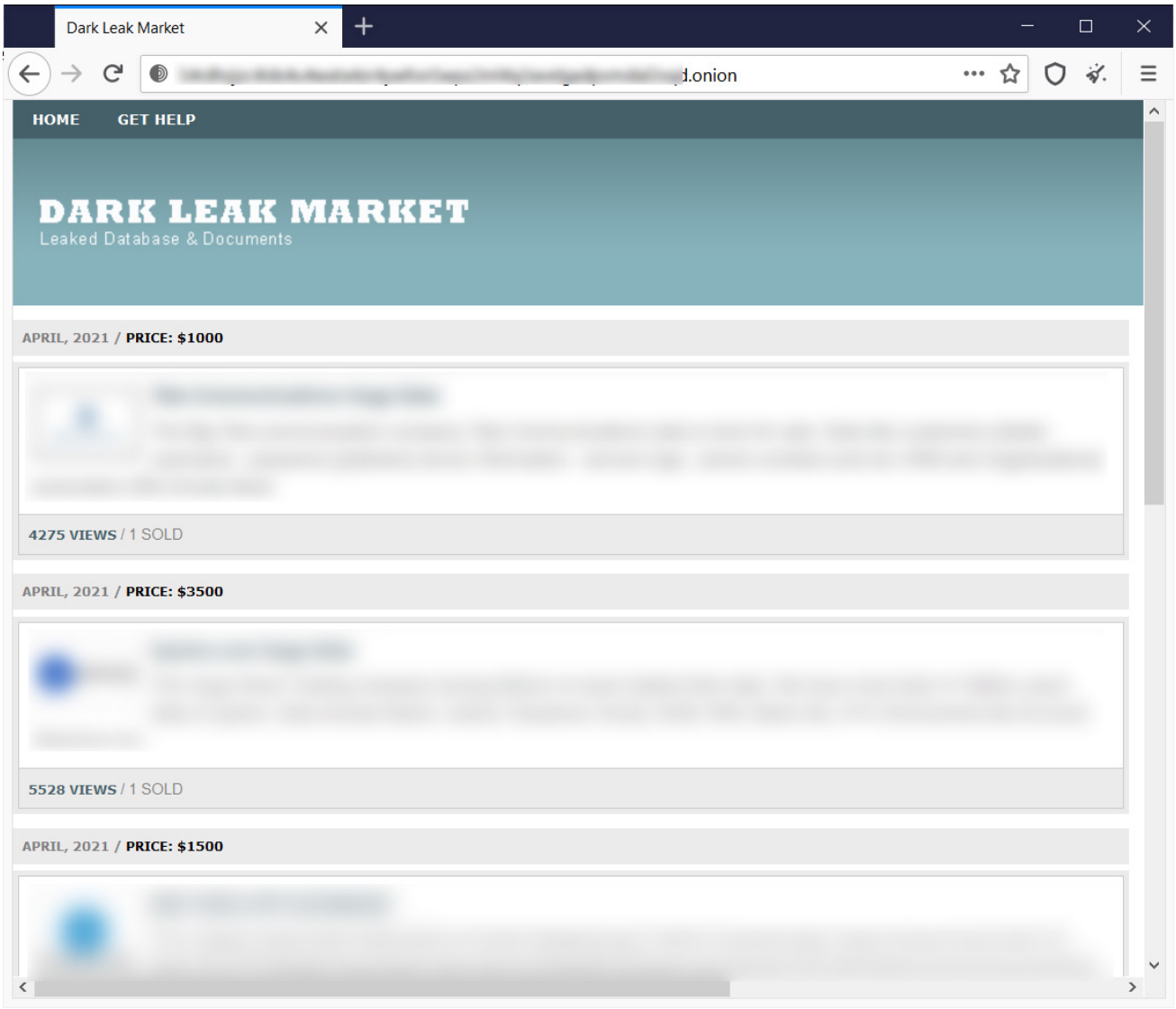
While dark web marketplaces for illicit goods are not new and have been used to sell stolen data in the past, they were not designed solely for data-theft extortion.

Recently, BleepingComputer has identified two new marketplaces called Marketo and File Leaks created to sell data to other threat actors or back to the victim themselves. In addition, there is one marketplace called 'Dark Leak Market' that appears to have been created in 2019.

Dark Leak Market

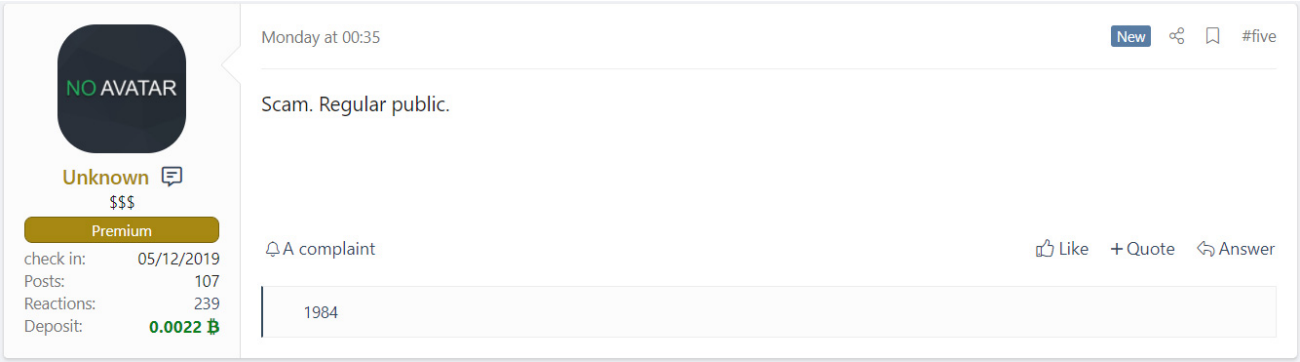
The oldest of these marketplaces is Dark Leak Market who has been selling stolen data since 2019.

The data sold at this site ranges from $100 to $9,000 and has been gathered from ransomware gang's data leak sites and hacking forums, such as RaidForums.



Dark Leak Market

Using KELA's DarkBeast intelligence platform, BleepingComputer found a post by REvil Ransomware's Unknown confirming that the data is being resold from other data leaks.

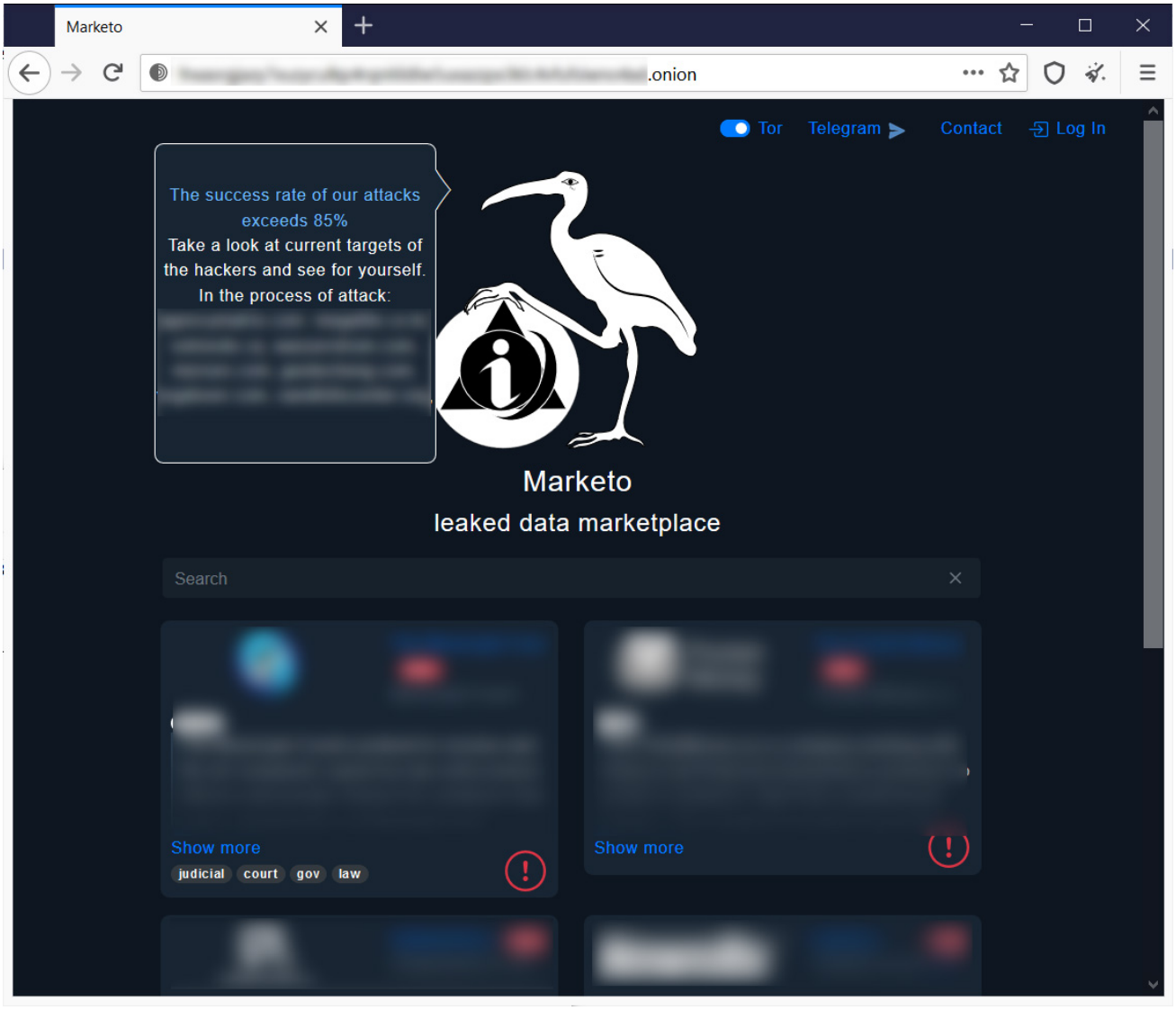


Post by REvil Ransomware's Unknown calling the site a scam

Marketo marketplace

Last month, threat actors launched a new marketplace called Marketo, with the owner contacting journalists and security researchers to promote the site.

"We would like to present the new marketplace Marketo, soon to be the best place to find, buy and sell any information about any company," a threat actor behind Marketo emailed BleepingComputer.



Marketo leaked data marketplace

When we asked if this data was stolen as part of their own attacks or others, they stated, "It is a marketplace for people who have information for sale, we don't hack companies."

They also claimed to be against ransomware and are not affiliated with "those who block networks and extort funds."

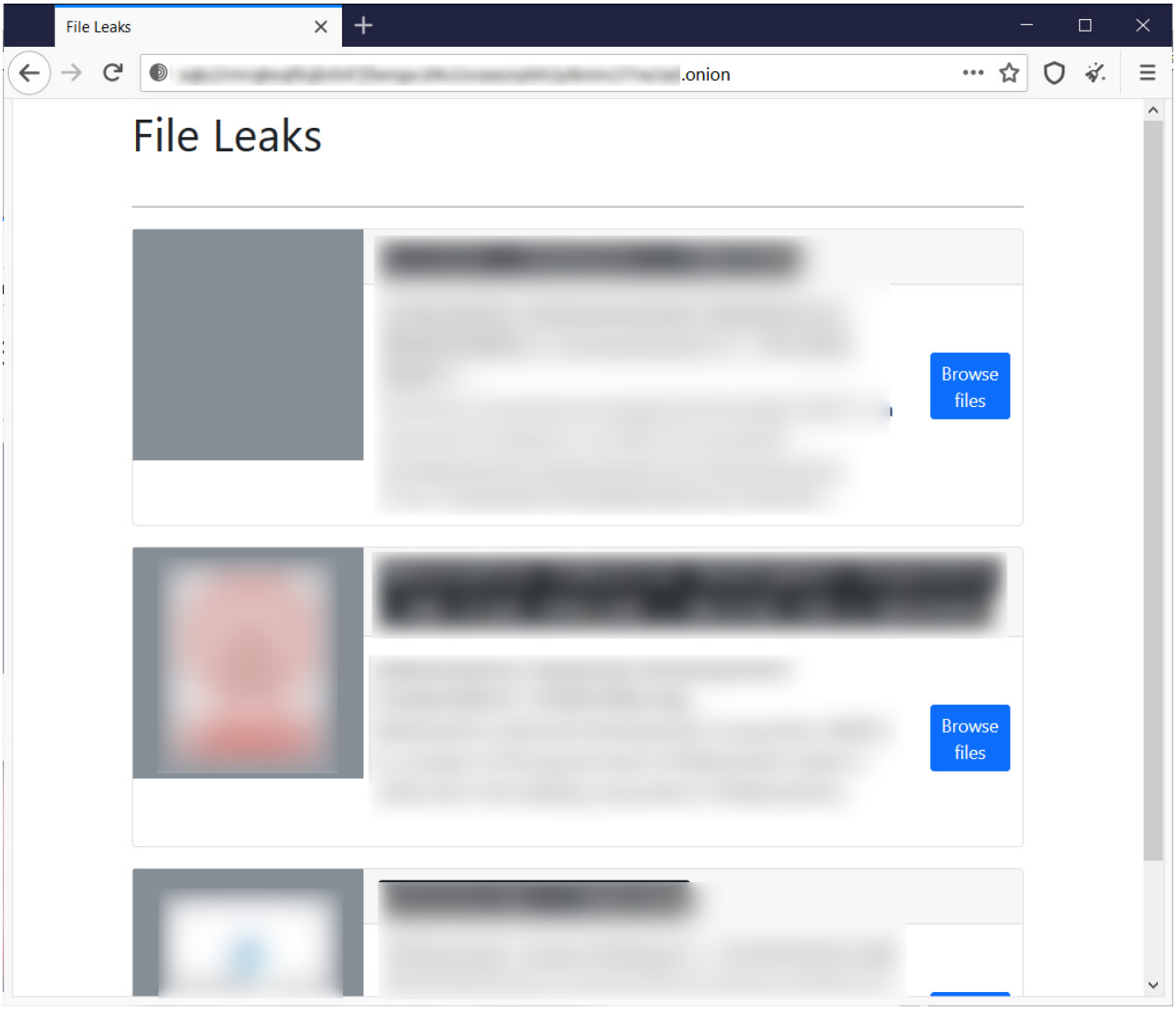
While most of the data found on the site does not appear to be associated with known ransomware attacks, that does not mean they are not hosting data from those types of attacks.

BleepingComputer was recently alerted by someone in the automotive cybersecurity industry who saw data on Marketo for a dealership known to have recently suffered from a ransomware attack.

File Leaks marketplace

The File Leaks marketplace was launched in April 2021 and dumps all of the stolen data at once, telling victims to contact them to pay to remove it.

The File leaks marketplace is the smallest of the sites, with two victims from Italy and one from India.



File Leaks marketplace

Paying the ransom is throwing money away

As we reported in November, victims should never pay a ransom for stolen data as there is no guarantee that their data will be deleted and not sold to other threat actors.

Ransomware negotiation firm Coveware told BleepingComputer that cybercriminals are increasingly failing to keep their promises after a ransom was paid.

In some cases, victims who paid were later extorted again using the same data, or the threat actors leaked the data anyway.

Furthermore, as shown by the Dark Leak Market, once data is leaked, there is no way to contain it as it spreads between different hacking forums and sites frequented by threat actors.

With this in mind, Coveware tells victims always to expect the following if they decide to pay a ransomware gang not to leak data:

> The data will not be credibly deleted. Victims should assume it will be traded to other threat actors, sold, or held for a second/future extortion attempt

- Stolen data custody was held by multiple parties and not secured. Even if the threat actor deletes a volume of data following a payment, other parties that had access to it may have made copies so that they can extort the victim in the future
- The data may get posted by mistake or on purpose before a victim can even respond to an extortion attempt

Instead, data theft victims should always treat an attack as a data breach and properly disclose the breach to all customers, employees, and business partners to prevent them from being harmed by the stolen data.

Update 5/7/21 11:14 AM EST: *We incorrectly stated Lorenz is a data leak marketplace, when in fact it is a ransomware group's data leak site. Thx to Andre Gironda for the correction.*

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Darknet market Versus shuts down after hacker leaks security flaw

New RansomHouse group sets up extortion market, adds first victims

Quantum ransomware seen deployed in rapid network attacks

New Industrial Spy stolen data market promoted through cracks, adware

- Dark Web
- Data Exfiltration
- Data Leak
- Marketplace
- Ransomware
- Tor

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: