Sodinokibi Ransomware Data Leaks Now Sold on Hacker Forums

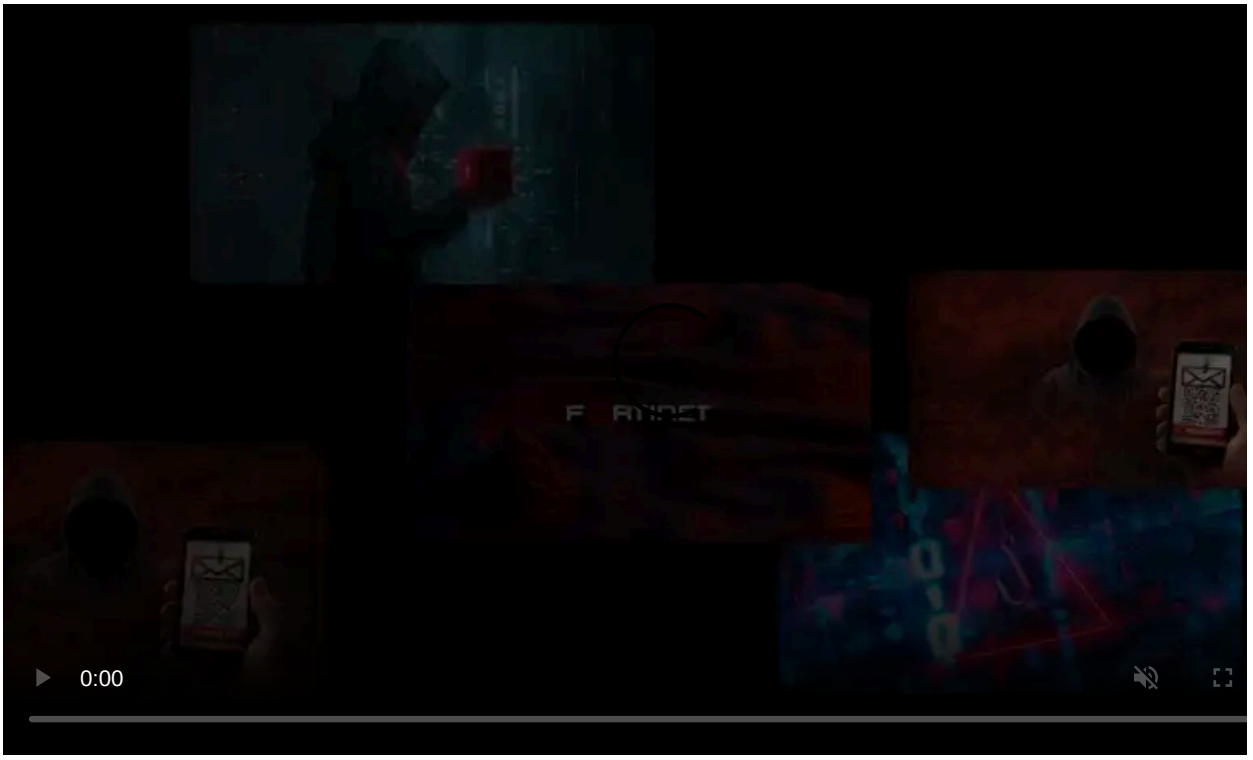
By Lawrence Abrams

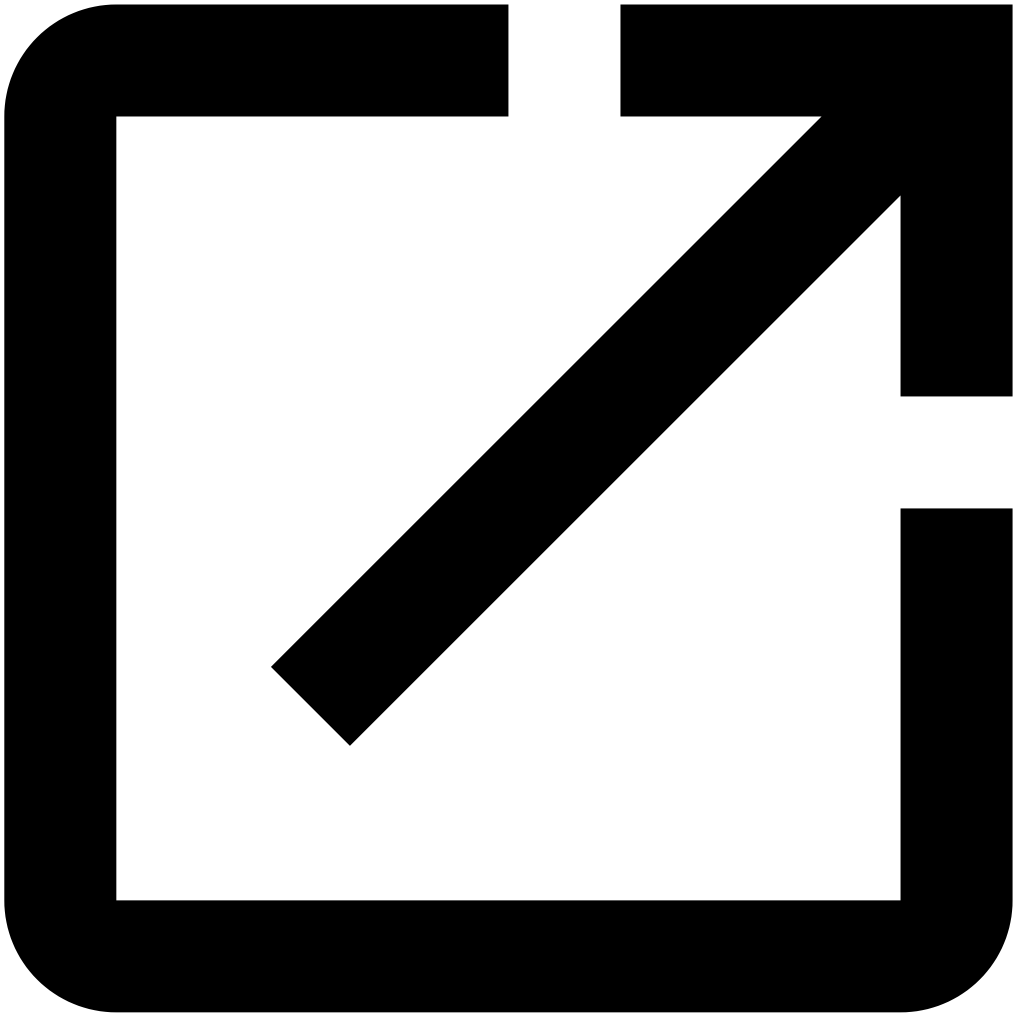
Published: 2020-03-19 · Archived: 2026-04-06 00:52:04 UTC

Ransomware victims who do not pay a ransom and have their stolen files leaked are now facing a bigger nightmare as other hackers and criminals sell and distribute the released files on hacker forums.

In 2019, the Maze Ransomware operators began stealing data from victims before encrypting devices and using the stolen files as leverage to get the victims to pay. If the victim decided not to pay, the Maze operators would then publish the files.

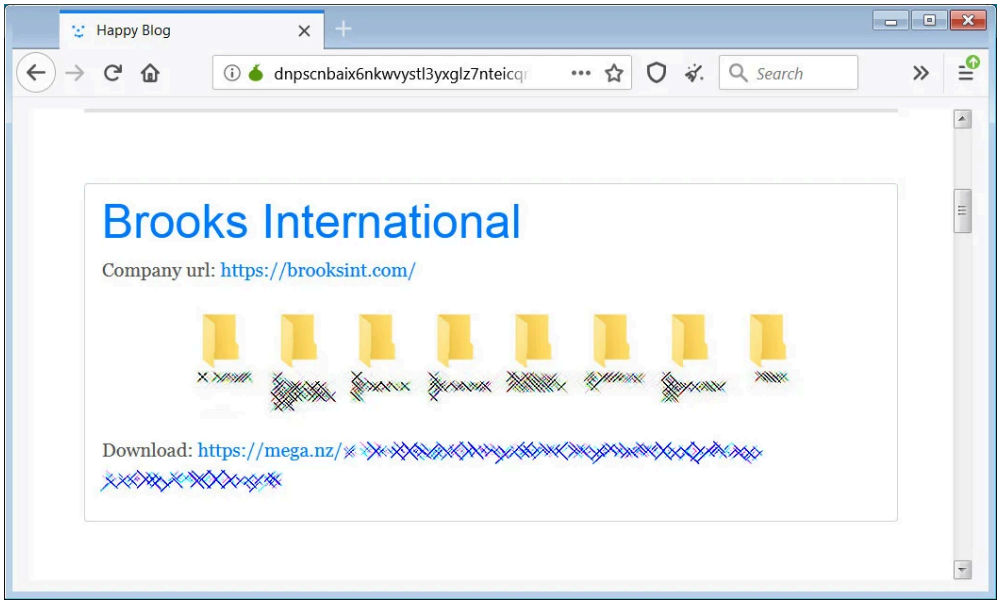
Since then, other ransomware operators such as Sodinokibi, DoppelPaymer, and Nemty have begun the same practice of using stolen files as leverage.


0:00



Visit Advertiser websiteGO TO PAGE

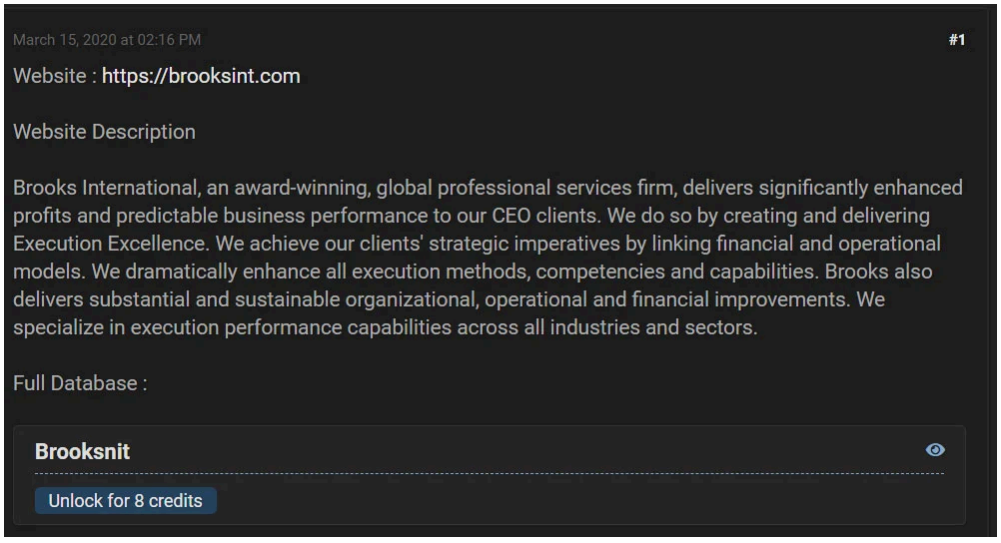
Recently, the Sodinokibi Ransomware operators published over 12 GB of stolen data allegedly belonging to a company named Brooks International for not paying the ransom.



Sodinokibi Ransomware leaking data

While making the data publicly accessible is bad enough, BleepingComputer has been told by cyber-intelligence firm Cyble that other hackers and criminals have started to distribute and sell this data on hacker forums.

For example, the following image is a hacker forum post where a member is selling a link to the stolen data for 8 credits, which is worth approximately 2 Euros.



Hacker forum post selling the data

From screenshots of the files shared with BleepingComputer, this stolen data is very valuable to hackers as it contains user names and passwords, credit card statements, alleged tax information, and much more.

Based on the comments from hackers who purchased the link to this data, they are also finding the data valuable.

"It even has credit card number & a password. lol !!"

"To bad these W2 forms weren't Donald Trump's taxes. lol !!"

"Thank you for being the hero we may not deserve, but need."

BleepingComputer reached out to Brooks International by phone to warn them about the distribution of their data and ask related questions, but after speaking to someone never received a phone call back.

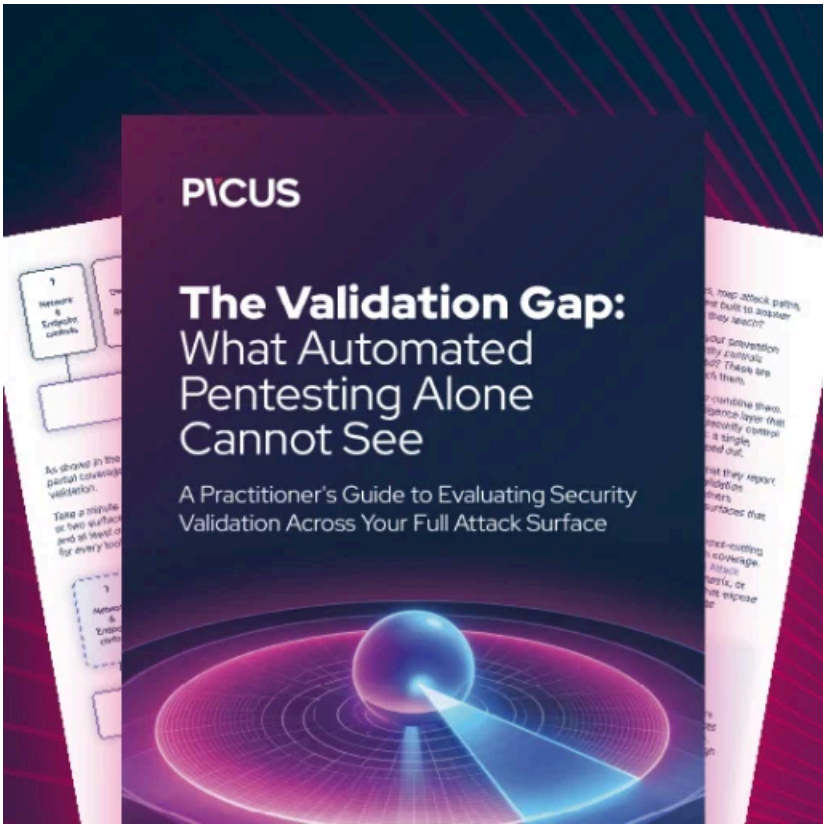
Ransomware attacks are data breaches

For a long time, BleepingComputer has been stating that Ransomware attacks are data breaches as it has been a widely known secret that attackers sifted through their victim's files before encrypting them.

Now that they are also stealing and publishing these files for non-payment, there is no longer any doubt that these attacks need to be classified as data breaches.

To make matters worse, it is not only corporate data being exposed, but also employee's personal information being stolen. These employees need to be informed of these breaches so that they can protect themselves from identity theft.

Unfortunately, too many ransomware attacks go undisclosed, even to the employees who are impacted.



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/sodinokibi-ransomware-data-leaks-now-sold-on-hacker-forums/