INSIGHTS

Cyber made simple.

one brightly cyber

YOUR DATA HAS BEEN LEAKED – OR HAS IT?

BY JAY BORDEN

Cybercriminals stealing data is nothing new. It began years ago. Ransomware for a while existed alongside data stealing as an attack.

Then as people and companies chose to not pay the ransom, the cybercriminals began to steal the data before encrypting it. The stolen data was the leverage to convince you to pay. If you didn't pay, your private information and that of your customers would be released publicly. That convinced many to pay the ransom.

Now a new tactic has emerged. Fake data leaks. Why do cybercriminals fake data leaks?

Cybercrime is a business and cybercriminals promote their businesses like any other business. Their channels are articles in the media and publicity on the Dark Web in order to garner respect, and attention. The goal of course is money as other cybercriminals purchase their data or stolen credentials or Ransomware as a Service.

As in any industry there are bigger players and smaller ones. The bigger ones have the money and skills to do the most damage and offer the most attractive data and credentials for sale. The smaller ones have to do something to compete. Faking data leaks is a current tactic.

Why a fake data leak? Because it is easy, doesn't require deep skills but still intimidates targeted companies and gives cybercriminals credibility on the Dark Web.

The data from the fake leak can be sold to others on the Dark Web.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

YOUR DATA HAS BEEN LEAKED – OR HAS IT?

Continued

Where does the data from a fake leak originate? Any public information is the source of the fake data leak. It can be information found in public databases then reorganized to mask the source, anything available on the internet, information scraped from the company website and other websites containing any information about the target company in any format such as graphs, tables, texts, links, social media platforms, really anything. Even old leaks may become part of it.

If the information is restructured and reorganized the source is harder to recognize as is the fact that it really isn't leaked but is publicly available.

Experienced cybercriminals won't fall for this, but new ones may.

Why is it valuable? The targeted company may still be damaged by bad publicity even if the leak is fake. We all know that initial stories garner the most attention. Follow-ups not as much.

The company may be asked to pay to not have all the data released publicly.

What to do when confronted with this type of situation? Stop and examine what really happened. Do not contact the cybercriminals. Look at the data provided as evidence of the leak. Is it already publicly available or is it really private information that was stolen?

This is a very important point. If the former then use your Communications Plan to communicate, not with the cybercriminals but with necessary parties that the report was fake. There has been no breach of private data at the company.

If it is private data, then activate your Incident Response plan.

Remember to communicate with clients, suppliers, regulators, law enforcement, employees, reporters, anyone who may have picked up on the news of the leak or be affected by a real data breach.

Incident Response and Communication plans need to be created before an event happens.

Need help or guidance? Learn how we can help you in so many ways.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.