M20 ASSOCIATES
1100 NW Loop 410
Suite 700
San Antonio, TX 78213
M20Associates.com

Texas Driver's Licenses on the Dark Web

Earlier this year, a couple of data breaches took place in Texas law enforcement databases. A source with firsthand access to the information discovered Texas Drivers' Licenses, along with associated dates of birth, on the Dark Web.

In June 2020, hundreds of thousands of potentially sensitive files (270 Gigabytes) from multiple police departments (to include intelligence and fusion centers) across the United States were leaked on-line. The searchable collection, known as "Blue Leaks," was from Netsential, a Houston, Texas web design and hosting company who maintained a number of state law enforcement data-sharing portals. The collection was released by Distributed Denial of Secrets (DDoSecrets), which is an alternative to Wikileaks.

The National Fusion Center Association (NFCA) confirmed the leaks, which included data that spanned 24 years (from 1996 to 2020). The documents included names, email addresses, and phone numbers, at a minimum.

The NFCA assessed in June that cyber threat actors and criminals might seek to exploit the data centers and associated agencies and their personnel in various cyber-attacks and campaigns. It is expected that with many breaches, notification to the victim will be delayed.

There is a high likelihood that license information, even from simple traffic stops where no citations were issued, was compromised. In some instances, a picture is taken, and these were also likely compromised. In addition, it is unknown what the police departments' retention policies are, so it is uncertain how far back their data repositories go.

In May, a new ransomware known as Ransom X successfully targeted the Texas Courts and Texas Department of Transportation. It is likely that the ransomware laterally moved across multiple state networks, to include the Texas Department of Public Safety (In 2019, approximately 23 Texas towns were targeted with ransomware (assessed as REvil/Sodinokibi)).

Sources

https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

https://www.bleepingcomputer.com/news/security/blueleaks-data-dump-exposes-over-24-years-of-police-records/

https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/

https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations