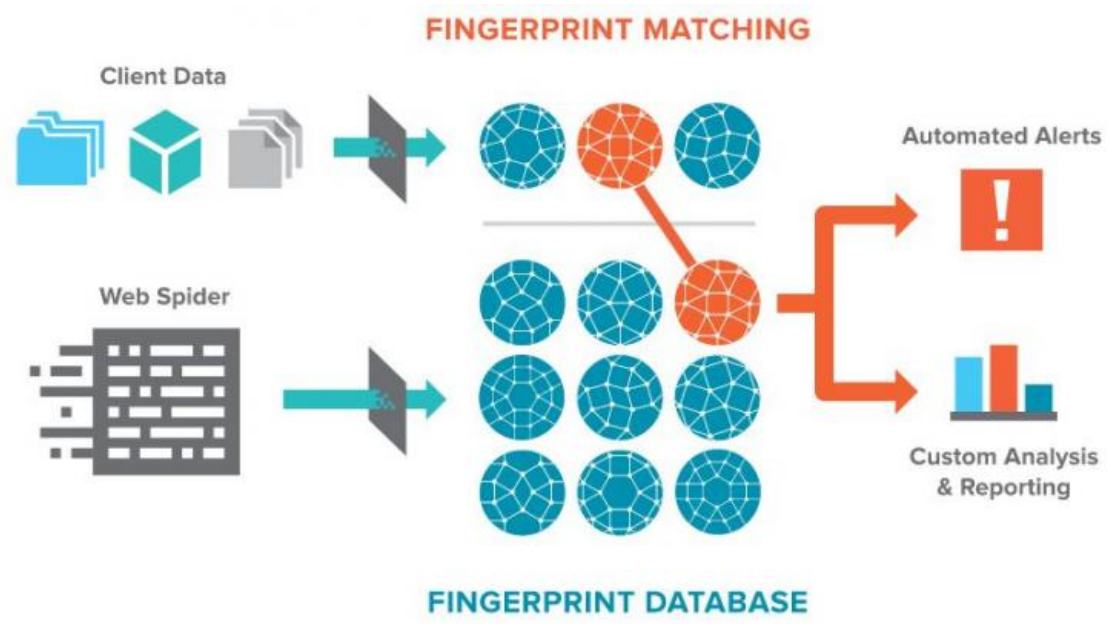
Stolen data finder could reduce harm for companies

June 8 2015, by Nancy Owano



Business owners don't need IT skills to understand that data breaches are serious. Certainly big names in retail and health care know by experience that such breaches have serious after-effects. Breaches have an impact on customer trust and in turn threaten profits.

Sponsored by IBM, the Ponemon Institute's "2015 Cost of Data Breach Study: Global Analysis," reported that the average total cost of a data

breach for the 350 companies participating in the research increased from 3.52 to $3.79 million.

"In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches and cyber attacks. However, there is a growing concern about the potential damage to reputation, class action lawsuits and costly downtime that is motivating executives to pay greater attention to the security practices of their organizations."

One company with a solution has a distinct point of view. Terbium Labs said, "We are a different sort of information security company." Consider this: Critical data and intellectual property are always at risk, they said. Data security does not exist. Maryland-based Terbium Labs said at least it can give you the power to immediately counter data theft. They cannot promise you will never lose data, but they can tell you that they will help to find data that is lost, and quickly.

"We started Terbium with the thesis that defense, while still necessary, is no longer sufficient. In today's insecure digital world, your organization's critical data will always be at risk, whether from a sophisticated outside actor or inside threat. That's why modern organizations are shifting their information security focus from prevention to risk management," said the team.

Terbium Labs' Matchlight system enables breach discovery to be immediate and automatic. The company's "immediate" is a key point, indicating breach discovery within seconds or minutes instead of months. (The average data breach traditionally has taken over 200 days to discover, and 85 percent of those breaches are discovered by external third parties.) The speed-up may enable an organization to start remediation plans before real damage occurs.

"Overall, the system allows companies, such as retailers and financial institutions, to detect whether a criminal has published some of their data on the Dark Web without revealing to anyone the exact nature of the sensitive data," said *MIT Technology Review*.

A patent-pending, one-way digital fingerprinting technique is put to work. Matchlight collects fingerprints from across all places on the Internet where stolen information is traded, including Dark Web markets and forums. They monitor for matches. If a match is found you get an alert.

Matchlight could be used by health care providers, banks, payment card providers, payment processors and other financial services and by engineering and manufacturing companies, among other sectors. "Organized crime and foreign nation-states make up a majority of industrial-espionage attacks, and their frequency continues to rise," said the company.

(The data fingerprinting technique uses "cryptographic hashing." It makes sure no one including Terbium Labs can decipher the originating data. A cryptographic hash function is described as a hash function which takes an input or message and returns a fixed-size alphanumeric string.)

So what actually happens after a breach is found? With Matchlight, organizations are alerted when elements of their data as short as fourteen bytes appear on the Internet. The alerts are sent immediately. Organizations can begin their remediation plans before any further damage can occur.

A number of companies have been testing Matchlight and now Terbium is inviting further signs of interest. "We have been testing Matchlight with a select number of alpha and beta clients. If your organization

would like access to Matchlight, contact us today!" said the company.

What good does it do to help find data that has already been stolen? For companies, it could mean reducing damages. "Already the system has helped companies testing the system find thousands of credit-card numbers that had been put up for sale on the Internet. While the Matchlight system catches attackers only after they post data following a breach and does not prevent the original compromise, it does reduce the time between compromise and discovery," said *MIT Technology Review*.

Referring to a major retailer breach incident which cost the company millions, the article said, "Catching the attack as soon as the thieves attempted to sell the data could have given the attackers less time inside the company's network and the buyers of the data less time to rack up fraudulent charges."

Jeremy Kirk, IDG News Service, talked about the finding-out process."Where we're looking at are places where people are leaking or are trying to monetize data," CEO Danny Rogers said. Companies using Matchlight can get alerts when a piece of data is found. A fingerprint ID number can be looked up to see what original data it corresponds to. Companies can then potentially start the breach mediation process, Rogers said in the article by Kirk. Signs of success so far? According to Kirk: "Rogers said the first day Terbium turned Matchlight on, it found in a single 24-hour period 20,000 to 30,000 credit card numbers and 600 leaked email addresses and passwords. Both sets of data were detected minutes after being posted, Rogers said."

More information: Terbium Labs: terbiumlabs.com/