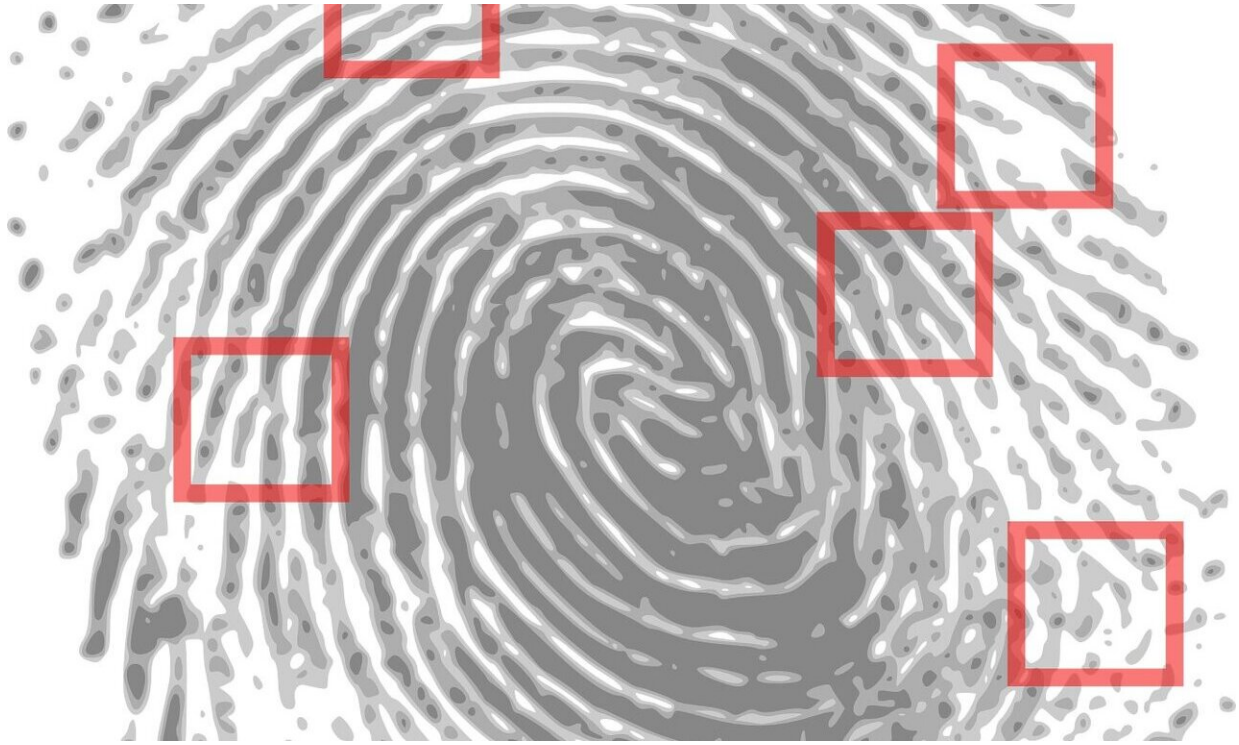
Unsecured database exposes 76,000 fingerprints

March 12 2020, by Peter Grad



Credit: CC0 Public Domain

A security firm handling employee fingerprint identification for companies worldwide has exposed more than 2 million bits of data, including 76,000 fingerprints, according to a cyberthreat research group.

Antheus Tecnologia, a Brazilian firm that develops and manages

automated fingerprint identification systems, left 16 gigabytes of highly sensitive information related to client identification and biometric details unsecured on their servers. The breach was discovered by researchers at SafetyDetectives.com, which specializes in analyzing antivirus software. Researchers say the breach has been secured.

The threat of biometric data theft is more serious than the average password breach or malware infection. Once a breach is detected, a user can change a password or apply a software patch to eliminate the threat. But fingerprint data are different: Fingerprints are for life, they can't be "upgraded" or changed. Iris scans and facial recognition data are also essentially permanent.

The Antheus server was found to employ weak measures relating to system access. It also stored actual fingerprint images and index logs that could easily be matched and utilized in criminal activity by malicious hackers.

"The unsecured method in which Antheus Tecnologia stores information is rather alarming considering its importance," said researcher Anurag Sen. "It's even more alarming that Antheus Tecnologia was built and deployed by a security company."

"Instead of saving a hash of the fingerprint (that cannot be reverse-engineered), Antheus is saving people's actual fingerprints through rudimentary encoding which can then be replicated for malicious purposes," Sen explained.

The security breach is troubling considering the increased reliance on biometric data for access to personal computers, mobile phones and banking and business institutions.

The incident is reminiscent of the 2015 cybertheft of 22 million personal

records and 1 million fingerprints used by the FBI. In an analysis of the event by one of the identity-theft victims, Janice Kephart, founder of the Secure Identity and Biometrics Association, she said that all who worked for the government since 2000 "are now not only subject to identity theft based on our biographic information, but our fingerprints are now linked to that biographic data" forever.

Sen noted the types of criminal activity the breach exposes users to include identity theft, access to classified information, financial theft, phishing attacks, blackmail, extortion and ransomware.

He listed measures, many of them long-established, common-sense solutions, to protect against identify theft. Among them:

- Check that the website you're on is secure (look for https and/or a closed lock)

- Only give out what you feel confident cannot be used against you (avoid government ID numbers, personal preferences that may cause you trouble if made public, etc.)

- Create secure passwords by combining letters, numbers, and symbols—Utilize online scanning tools to checks your devices for known vulnerabilities—Do not click links in emails unless you are sure that the sender is legitimate—Avoid using credit card information and typing out passwords over unsecured WiFi networks

More information: www.safetydetectives.com/blog/antheus-leak-report/