Data Breach Today
Prevention. Response. Notification. TODAY
https://www.databreachtoday.com/

3rd Party Risk Management , Biometrics , Breach Notification

US Border License Plate and Traveler Photos Exposed

Hack Attack Victim May Be Contractor Perceptics; Stolen Data Spotted on Dark Web

Jeremy Kirk (jeremy_kirk) • June 11, 2019

Photo: U.S. Customs and Border Protection

License plate images and photos of travelers collected at the U.S. border have been compromised after a federal government subcontractor was hacked, U.S. Customs and Border Protection said on Monday. Security researchers say the data has already turned up for download via a darknet site.

See Also: Webinar | Passwords: Here Today, Gone Tomorrow? Be Careful What You Wish For.

CPB alleges that the subcontractor, which it did not name, "violated mandatory security and privacy protocols outlined in their contract." In an update late Monday, CPB says images of up to 100,000 individuals were exposed.

Those photos were taken of individuals who entered and exited the U.S. using a few lanes at an unspecified land border crossing over a six-week period. No identification information, such as passport numbers or other travel documents, appear to have been exposed.

The subcontractor copied the material to its own network, which was hacked, CPB says, noting that its own systems were unaffected, and that the breach did not compromise any airport operations.

"CBP has removed from service all equipment related to the breach and is closely monitoring all CBP work by the subcontractor," the agency says. "CBP requires that all contractors and service providers maintain appropriate data integrity and cybersecurity controls and follow all incident response notification and remediation procedures."

Congressional Inquiries

The breach comes as CPB has been increasingly using new tools and gathering more biometric information when people enter the United States. President Donald Trump has made border security and immigration key themes of his tenure, and these themes look to figure prominently in the 2020 presidential election.

CPB says it has notified Congress and is working with law enforcement and cybersecurity experts. The agency's own Office of Professional Responsibility, which investigates corruption and mismanagement, has also begun an inquiry.

The breach alert has already drawn scrutiny from lawmakers. Democratic Rep. Bennie G. Thompson of Mississippi says he plans to convene hearings next month covering the Department of Homeland Security's use of biometric data.

"Government use of biometric and personal identifiable information can be valuable tools only if utilized properly," Thompson says. "We must ensure we are not expanding the use of biometrics at the expense of the privacy of the American public."

Potential Breach Source: Perceptics

Although CPB didn't identify the contractor that suffered the breach, evidence suggests that it may be Perceptics, an imaging company based in Farragut, Tennessee. Perceptics, which has worked with CPB since 1982 and was once a subsidiary of defense contractor Northrop Grumman, did not immediately respond to an email seeking comment.

Perceptics specializes in optical character recognition, including license plate readers and cameras that can identify U.S. Department of Transportation numbers and container codes visible on the sides of commercial freight haulers.

Perceptics' headquarters in Farragut, Tennessee

The Washington Post reports that CPB sent it a statement about the breach via a Microsoft Word file titled "CBP Perceptics Public Statement." Also, the Register reports that on May 23 that it was tipped off by a source of a breach at Perceptics, which at that time confirmed its network had been compromised.

The Register writes that it was contacted by someone going by the nickname "Boris Bullet-Dodger." Files from the Perceptics breach are listed on a ".onion" website run by a group calling itself Team Snatch.

The .onion domain means the site is only available via the anonymizing Tor network, which can make it difficult to identify where data is being hosted. Such sites are sometimes referred to as darknet sites or as being on the dark web.

Who Is Team Snatch?

According to the Baltimore-based cybersecurity firm ZeroFOX, Team Snatch is a cybercrime group that was "first associated with ransomware operations who now partake in more general data theft."

Team Snatch's website contains data for other companies the group claims to have compromised, including the German IT services company CityComp, public relations agency KCSA Strategic Communications of New York and accounting firm Myatt Blume & Osburn of Levelland, Texas.

An index of files purportedly belonging to Perceptics on Team Snatch's hidden Tor service.

CPB contends that "none of the image data has been identified on the dark web or internet."

But ZeroFOX says it reviewed the leaked files on Team Snatch's website and "concluded with high confidence that the files are confidential and authentic." Twitter has suspended Team Snatch's account.

"We are unsure how they were obtained, but based on the previous CityComp breach and its associated actors, it's likely that the affected companies declined or did not respond to blackmail or extortion demands," ZeroFOX writes in a blog post.

Third-Party Risks

Data protection lapses by subcontractors or partners continue to be a long-term source of cybersecurity concern.

Third parties are a growing source of risk, says Terence Jackson, CISO with Washington-based Thycotic, which specializes in privileged access management. Non-federal computer systems are required to comply with NIST 800-171, which specifies security rules for handling data, including rules for how any such system stores, processes or transmits what the government refers to as "controlled unclassified information."

But many organizations self-certify their NIST 800-171 compliance, Jackson says, and agencies such as CPB should be regularly testing to make sure it's adequate. "Companies, including government agencies, have to perform due diligence on their contractors on a continuous manner," Jackson says.

Security experts say the loss of the facial images are particular concerning, given that they are used for biometric identification purposes, and of course biometrics can't be changed. Once the data becomes public, it could potentially be abused in perpetuity.

Neema Singh Guliani

Nevertheless, governments are increasingly collecting vast amounts of biometric data. Neema Singh Guliani, senior legislative counsel for the American Civil Liberties Union, says in a statement that the CBP is expanding its facial recognition program and collecting growing volumes of sensitive information about travelers, including their license plate numbers and social media identifiers.

"This incident further underscores the need to put the brakes on these efforts and for Congress to investigate the agency's data practices," she says. "The best way to avoid breaches of sensitive personal data is not to collect and retain such data in the first place."

Last month, Guliani warned that the U.S. government's facial recognition efforts are continuing to expand. The FBI, for example, has a facial recognition database comprising 640 million photos, she said, which equals nearly twice the size of the U.S. population. But questions remain over the legal framework via which the agency is allowed to collect such biometric information (see: *Facial Recognition: Big Trouble With Big Data Biometrics*).

Managing Editor Scott Ferguson and Executive Editor Mathew Schwartz contributed to this report.

About the Author

Jeremy Kirk

Managing Editor, Security and Technology, ISMG

Kirk is a veteran journalist who has reported from more than a dozen countries. Based in Sydney, he is Managing Editor for Security and Technology for Information Security Media Group. Prior to ISMG, he worked from London and Sydney covering computer security and privacy for International Data Group. Further back, he covered military affairs from Seoul, South Korea, and general assignment news for his hometown paper in Illinois.