Ashley Madison hack could mean trouble for some feds, troops

By Kevin Lilley *11:27 a.m. EDT August 20, 2015*

(Photo: Getty Images/iStockphoto)

The release of personal information reportedly belonging to more than 36 million members of adultery-focused dating site AshleyMadison.com contains 15,000 email addresses with military or federal government domains, according to a separate online data dump.

The unverified totals, posted by Twitter user @t0x0pg and cited by Wired magazine and other media outlets, include 6,788 addresses ending in "us.army.mil," another 1,665 ending in "navy.mil," 809 ending in "usmc.mil" and 206 in "mail.mil."

The data dump also includes more than 875 .gov addresses linked to federal agencies, including 44 addresses from the White House domain. The remainder were state and local addresses or obviously fake.

The presence of an individual's email account in the leaked files doesn't indicate its owner participated in services offered by the website, which uses the slogan "Life is short. Have an affair." It may not mean the owner even signed up in the first place.

"People would put whatever email address on there, and Ashley Madison wouldn't check it," said Robert Graham, CEO of Errata Security (http://blog.erratasec.com/), a cybersecurity consulting company he's run for the past 10 years. "People could lie, and they often did lie."

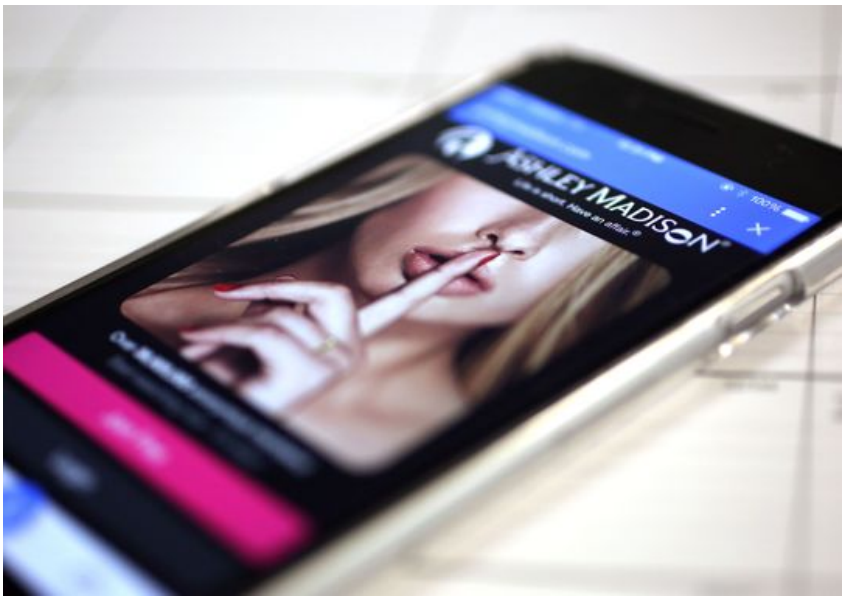
Graham couldn't confirm the dot-mil and dot-gov totals, but he said the figures roughly correspond to what he'd seen in his analysis of the leaked data (http://blog.erratasec.com/). He also put the total accounts at above 36 million, slightly below the site's claimed 40 million members.

While a functioning email address wasn't required to register at AshleyMadison.com, users interested in connecting with other users generally were required to pay for the privilege. The credit-card payments and billing addresses, also part of the nearly 10-gigabyte dump, are more reliable personal identifiers, Graham said.

"Most of the people that paid money used their real name," said Graham. "That is a hard data point."

This would link the individuals to their profile sheets, which include the basics sought by most dating websites like age, height, and weight, Graham said, but also offered "very lurid fantasies," in some cases.

Even users who may think they remained anonymous throughout the process could be tripped up by GPS-locator details included in the hack, Graham said – if a user created an account using their cellphone while in their house, for instance, the account could be traced to their GPS coordinates.



Hackers have posted the data on tens of millions of AshleyMadison.com members. One analysis of the information reportedly found that about 15,000 of them had provided dot-gov or dot-mil email addresses. *(Photo: Jennifer Milbrett/Staff)*

Breach basics

The Twitter-posted data set, which does not reveal full email addresses, says 55 users registered with "usarmy.mil," four signed up with the nonexistent "yahoo.gov" and two used "u.s.army.mil," among other nonfunctioning domains and likely typos.

Other, more specialized military domains – aircraft carriers, reserve and National Guard branches, unit-specific email addresses, and so on – also are represented on the list in smaller numbers, reportedly culled from the main data set. That data was released late Tuesday by the a group calling itself the Impact Team, which claimed last month to have hacked the site and pledged to publish the data unless Avid Life Media, creator of AshleyMadison.com and sister sites like CougarLife.com, shuttered its websites.

"We have explained the fraud, deceit, and stupidity of ALM and their members," the hackers said in a statement accompanying the release. "Now everyone gets to see their data."

In response, Toronto-based ALM called the hack "an illegal action against the individual members of AshleyMadison.com, as well as any freethinking people who choose to engage in fully lawful online activities," and said U.S. and Canadian authorities were on the case.

It's unclear whether the Pentagon will investigate the identities revealed in the data leak. Adultery, under the Uniform Code of Military Justice, is outlawed.

The potential repercussions might not be as severe for civilian employees.

"The implications are different between the military and the civil side," said Jim Tozzi, both a veteran and former deputy administrator for the Office of Regulatory Affairs in the Office of Management and Budget.

Most of the civilian agencies don't have specific policies on adultery, Tozzi said, so long as it does not involve employees within the same agency.

"Let's say someone used that site: What injury is done to the government?" he said.

Tozzi pointed out these .gov email addresses are used to communicate with constituencies, meaning many are public knowledge already. While many agencies have policies prohibiting use of official email for non-official purposes, the actual impact in this case is likely minimal.

The bigger issue would be cybersecurity vulnerabilities caused by federal employees surfing the site itself.

"If the use of a non-government site increases the cyber threat to the government, that's different. But I haven't heard of that in this case," Tozzi said. "Other than that, I don't think anybody cares," other than the people whose names might be released.

A variety of blogs, social-media posts and media reports offer links purportedly directing readers to websites that claim to offer a search function for those interested in AshleyMadison.com clients. While Graham said the technical background to put such a site together could be found in "a teenage kid with a little bit of web programming knowledge," it did offer an opportunity for more potential problems.

"If one of those sites asks for your husband's [AshleyMadison.com] password, it's probably a scam site," he said, adding that the "standard browse-the-Internet" security rules should apply to such offers.

While it's possible some users offered a fake military email account as part of a false identity, it wouldn't have helped – the AshleyMadison.com sign-up page instructs users that the email address "will never be shown or shared."

Senior Staff Writer Aaron Boyd contributed to this report.

Read or Share this story: http://fedtimes.ly/1LkFGTX

MORE STORIES

Presidential program that led to Digital Service, 18F, now permanent

(/story/government/it/2015/08/17/innovation-fellows-permanent/31853633/)

(/story/government/it/2015/08/17/innovation-fellows-permanent/31853633/)

Aug. 17, 2015, 1:32 p.m.

FBI tries to recruit hackers as cyber special agents

(/story/government/cybersecurity/2015/08/18/fbi-recruits-hackers/31867247/)

(/story/government/cybersecurity/2015/08/18/fbi-recruits-hackers/31867247/)

Aug. 18, 2015, 12:37 p.m.

Institutional wisdom as a tool for effectiveness

(/story/government/management/blog/2015/08/17/ins wisdom-tool-effectiveness/31851773/)

(/story/government/management/blog/2015/08/17/institut wisdom-tool-effectiveness/31851773/)

Aug. 17, 2015, 12:23 p.m.