

Hackers release more data obtained from 'intelligence' firm, Stratfor

by Elinor Mills via stele - CNET News *Saturday, Dec 31 2011, 6:23am*

international / mass media / other press

Hackers are the only EFFECTIVE force of opposition to the nefarious ruling elites today

Hackers released more data obtained from a breach of Stratfor, including e-mail addresses and credit card numbers, the geopolitical intelligence firm confirmed to CNET today.



Goldman Sachs employee and Oz Priministerial candidate, Malcolm Turnbull's data exposed

In a post on Pastebin by someone using the "AntiSec" moniker, there are links to downloads of data on different sites, some of which were removed by midday today. The data dump follows the release of a list of Stratfor (Strategic Forecasting) clients on December 25 and a warning from hackers that they had more sensitive data to release, including unencrypted credit card data.

"It's time to dump the full 75,000 names, addresses, CCs and md5 hashed passwords to every customer that has ever paid Stratfor. But that's not all: we're also dumping ~860,000 usernames, email addresses, and md5 hashed passwords for everyone who's ever registered on Stratfor's site," the post says, adding that 50,000 of the e-mail addresses end in .mil or .gov domains.

"We almost have sympathy for those poor DHS employees and australian billionaires who had their bank accounts looted by the lulz ... But what did you expect?" the post says. "All our lives we have been robbed blindly and brutalized by corrupted politicians, establishmentarians and government agencies sex shops, and now it's time to take it back."

The post then goes on to warn that hackers will attack "multiple law enforcement targets from coast to coast" on New Year's Eve and that there will be "noise demonstrations" outside of jails and prisons around the world in solidarity with the prisoners.

"Stratfor regrets the latest disclosure of information obtained illegally from the company's data systems," the company said in a statement. "We want to assure our customers and friendsthis was not a new cyberattack, but was instead a release of information obtained during the previous security breach. The latest disclosure included credit card information of paid subscribers and many

e-mail addresses of those who receive Stratfor's free services."

Asked to comment on the timing of the breach and why the company was not using encryption, Stratfor provided this statement: "We don't have any information on that at the moment. But I want to assure you Stratfor is working with law enforcement to investigate the cyberattacks and will release results soon. In the meantime, we will be providing periodic updates on our response to the attacks."

Meanwhile, the company is offering to pay for a one-year subscription to identity protection services for anyone affected by the breach. The corporate Web site will not be back up for another week or so, Stratfor CEO George Friedman wrote in a post on the company's Facebook page that was also sent to subscribers via e-mail.

"To say we wish this hadn't happened is a massive understatement," he wrote. "As I have stated in prior emails to you, I sincerely apologize for these unfortunate events. Our investigation and coordination with law enforcement is ongoing, and we will continue to update you as more details become available."

On Thursday, the hackers said they had breached the Web site of SpecialForces.com and claimed to have 14,000 passwords and data on 8,000 credit cards, although the data was encrypted. The hackers also claim to have copies of as many as 2.7 million Stratfor e-mails that they plan to release.

AntiSec, which is a coalition of members of the de-centralized Anonymous group of hactivists and the more mischievous LulzSec offshoot, claimed credit for attacks earlier this year on police, sheriffs and other law enforcement agencies in the U.S. and Italy, defense and government contractors including Booz Allen Hamilton and HBGary Federal, and government agencies in Chile, Zimbabwe, and Brazil.

Stratfor may have hit the hackers' radar when it warned members of Anonymous in November not to wage war on the Zetas drug cartel in retaliation for the alleged kidnapping of an Anonymous member. "As Mexican cartels have targeted online journalists and bloggers in the past, hackers could well be targeted for reprisal attacks," Stratfor wrote in a report on OpCartel.

© 2011 CBS Interactive



<http://tinyurl.com/7cadejd>

Cleaves Alternative News. <http://cleaves.lingama.net/news/story-2912.html>

