# Feds Indict Three in 2011 Epsilon Hack — Krebs on Security

U.S. federal prosecutors in Atlanta today unsealed indictments against two Vietnamese men and a Canadian citizen in connection with what's being called "one of the largest reported data breaches in U.S. history." The government isn't naming the victims in this case, but all signs point to the 2011 hack of Texas-based email marketing giant **Epsilon**.

The government alleges the defendants made more than $2 million blasting out spam to more than one billion email addresses stolen from several email service providers (ESPs), companies that manage customer email marketing on behalf of major corporate brands. The indictments further allege that the men sent the junk missives by hijacking the email servers used by these ESPs.

"This case reflects the cutting-edge problems posed by today's cybercrime cases, where the hackers didn't target just a single company; they infiltrated most of the country's email distribution firms," said **Acting U.S. Attorney John Horn**. "And the scope of the intrusion is unnerving, in that the hackers didn't stop after stealing the companies' proprietary data—they then hijacked the companies' own distribution platforms to send out bulk emails and reaped the profits from email traffic directed to specific websites."

To be clear, prosecutors haven't specifically outed Epsilon as the victim, nor did they name any of the other email service providers (ESPs) allegedly harmed by the defendants. But a press release issued today Horn's office states that "the data breach into certain ESPs was the subject of a congressional inquiry and testimony before a U.S House of Representatives subcommittee on June 2, 2011."

That date aligns with a June 2, 2011 House Energy and Commerce Committee panel on the data breaches at Sony and Epsilon. Epsilon officials could not be immediately reached for comment.

**Update, 11:27 p.m. ET:** Epsilon confirmed that it is among the victims in this case. See the end of this story for their full statement.

*Original story:*

In early April 2011, customers at dozens of Fortune 500 companies began complaining of receiving spam to email addresses they'd created specifically for use with those companies. On April 2, 2011, Epsilon started notifying consumers that hackers had stolen customer email addresses and names belonging to a "subset of its clients."

Those clients were ESPs that send email to customers on behalf of some the biggest firms in the world. Epsilon didn't name which ESPs were impacted, but the voluminous complaints from consumers about spam indicated that those ESPs served a broad range of major companies, including JP Morgan Chase, U.S. Bank, Barclays, Kroger, McDonalds, Walgreens, and Honda, to name but a few.


*A scam web site that tried to sell copies of Adobe Reader.*

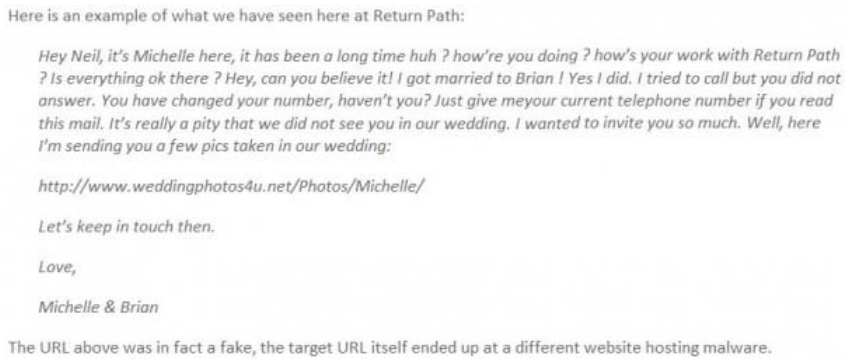
As I noted in that April 2011 story, consumers had complained of received junk email with links to sites that tried to sell versions of software made by **Adobe Systems Inc.** Some of the sites reportedly even tried to sell copies of **Adobe Reader** — software that Adobe gives away for free.

Sure enough, the men indicted today are accused of hacking into a major ESP to steal more than a billion email addresses, which

they allegedly used to promote knockoff versions of Adobe software (among other dubious products).

Prosecutors in Atlanta today unsealed indictments against **Viet Quoc Nguyen** and **Giang Hoang Vu**, both citizens of Vietnam who resided for a period of time in the Netherlands. The government also unsealed an indictment against **David-Manuel Santos Da Silva**, a Canadian citizen who was charged with conspiring with Nguyen and others to launder the proceeds of Nguyen's alleged computer hacking offenses.

The government alleges that Nguyen used various methods — including targeted email phishing campaigns — to trick recipients at email marketing firms into clicking links to sites which attempted to exploit browser vulnerabilities in a bid to install malicious software. For more on those targeted attacks, see my Nov. 24, 2010 story, Spear Phishing Attacks Snag E-Mail Marketers.



Here is an example of what we have seen here at Return Path:

*Hey Neil, it's Michelle here, it has been a long time huh ? how're you doing ? how's your work with Return Path ? Is everything ok there ? Hey, can you believe it! I got married to Brian ! Yes I did. I tried to call but you did not answer. You have changed your number, haven't you? Just give meyour current telephone number if you read this mail. It's really a pity that we did not see you in our wedding. I wanted to invite you so much. Well, here I'm sending you a few pics taken in our wedding:*

*http://www.weddingphotos4u.net/Photos/Michelle/*

*Let's keep in touch then.*

*Love,*

*Michelle & Brian*

The URL above was in fact a fake, the target URL itself ended up at a different website hosting malware.

*A copy of one spear phishing email sent to ESP employees in Nov. 2010.*

"Nguyen's phishing campaigns allegedly delivered malware, which allowed him backdoor access to the ESP employees' computer systems and enabled him to steal sensitive information, including the employees' access credentials for the ESP's computer systems," the government alleged. "Using stolen access credentials, Nguyen was not only able to allegedly steal confidential information by downloading the information from the ESPs' computer systems to a server that he controlled in the Netherlands, but was also able to utilize the ESPs' computer systems to launch spam attacks on tens of millions of stolen email addresses."

*Prosecutors released this photo of Nguyen, in undated Facebook profile photo.*

Vu allegedly assisted in the spamming. Da Silva allegedly helped launder the proceeds of the spam campaigns. Prosecutors say Da Silva ran an affiliate marketing firm called **Marketbay.com**, and that through that service he provided Vu and Nguyen a way to monetize their spam campaigns.

If recipients of the spam emails clicked through and paid for the products advertised in the junk email, those customers would be directed through Marketbay's affiliate links. According to the government, Da Silva knew Vu and Nguyen were using stolen email addresses and hijacked ESPs to drum up sales, which prosecutors allege generated more than $2 million for the men.

Vu was arrested by Dutch authorities in 2012 and was later extradited to the United States. He has pleaded guilty to conspiracy to commit computer fraud, and is slated to be sentenced in April 2015.

Da Silva was arrested in Ft. Lauderdale, Fla. on Feb. 12, and is expected to make his first appearance today before a federal magistrate in Atlanta. Nguyen is not in custody and remains a fugitive.

The indictment against Da Silva is here (PDF). The Nguyen indictment is at this link (PDF).

**Update:** As noted in the update above, Epsilon responded to a request for comment with the following statement:

"Epsilon confirms that it is among the victims of the cybercrime referenced in the Department of Justice's indictment unsealed on March 5 against three individuals for their roles in hacking email service providers throughout the United States. We are pleased with the outcome of the investigation carried out by the U. S. Secret Service and the resulting indictment by the Department of Justice, and thank them for bringing this criminal activity to prosecution. Data protection is,and always has been, the top priority at Epsilon, and businesses and law enforcement must work together to prevent this type of criminal activity."

Tags: David-Manuel Santos Da Silva, Epsilon breach, Giang Hoang Vu, marketbay.com, spear phishing, Viet Quoc Nguyen

This entry was posted on Friday, March 6th, 2015 at 2:45 pm and is filed under Other. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.