Expert wants to help nab Russian password thieves

August 6 2014, by Martha Mendoza

Chief Information Security Officer Alex Holden of Hold Security, LLC appears during the Black Hat USA 2014 cyber security conference on Wednesday, Aug. 6, 2014, in Las Vegas. Russian hackers have stolen 1.2 billion user names and passwords in a series of Internet heists affecting 420,000 websites, according to Holden, whose firm uncovered the breach. (AP Photo/David Becker)

The hackers are a tight knit group, 10 or 11. They live in a Russian town, and have real jobs. But in their down time, the cybercriminals have spent the past seven months gathering a hoard of personal data, stealing 1.2

billion user names and passwords in a series of Internet heists affecting 420,000 websites, according to Alex Holden, Chief Information Security Officer for Hold Security, whose firm uncovered the breach.

The Russian hackers had been collecting databases of personal information for years, but Holden told The Associated Press Wednesday that in April the group began deploying a new online attack technique that quickly shot from computer system to computer system as unwitting infected users visited random websites.

"Their cache of stolen goods grew quite quickly," said Holden, who has not revealed details about the websites that were breached or the names of other victims.

A native of Kiev who now lives in Milwaukee, Holden has conducted research that contributed to other exposures of major hacks, including a breach at Adobe that exposed tens of millions of customer records. He said he had been tracking the Russian criminals for seven months, but only was able to begin reviewing their massive cache of databases during the past few weeks. He timed his announcement to coincide with the annual Black Hat USA cybersecurity conference this week in Las Vegas, where it created quite a buzz.

Brian Krebs, who investigates online cybercrime and blogs about it, said his phone and email were inundated while he was at the conference Wednesday with people asking about Holden's announcement.

"Alex isn't keen on disclosing his methods, but I have seen his research and data firsthand and can say it's definitely for real," said Krebs. "Without spilling his secrets or methods, it is clear that he has a first-hand view on the day-to-day activities of some very active organized cybercrime networks and actors."

More than a day after his discovery was revealed in a New York Times report, Holden said he had not heard from any law enforcement agencies. He said he hopes investigators do contact him and added that his firm would be happy to cooperate.

Chase Cunningham, lead threat intelligence agent for cloud security company Firehost, spent years tracking Russian crime syndicates with the FBI and the NSA. At Black Hat on Wednesday, he said Hold Security has "uncovered one of the largest caches of data ever seen."

To date, Hold Security says it has only seen the Russian hackers use the personal data to spam social media, for example, hijacking a Twitter account and posting a weight loss ad. And Holden said he's only seen payments ranging from $200 to $1500 —although he's unsure if that's per person or for the entire group— for creating that spam.

Cunningham said he expects the Russian criminals will do much more with their illicit collection, which could prove lucrative.

"They can make money hand over fist with this," he said.

© 2014 The Associated Press. All rights reserved.

Citation: Expert wants to help nab Russian password thieves (2014, August 6) retrieved 2 May 2024 from https://phys.org/news/2014-08-expert-nab-russian-password-thieves.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.