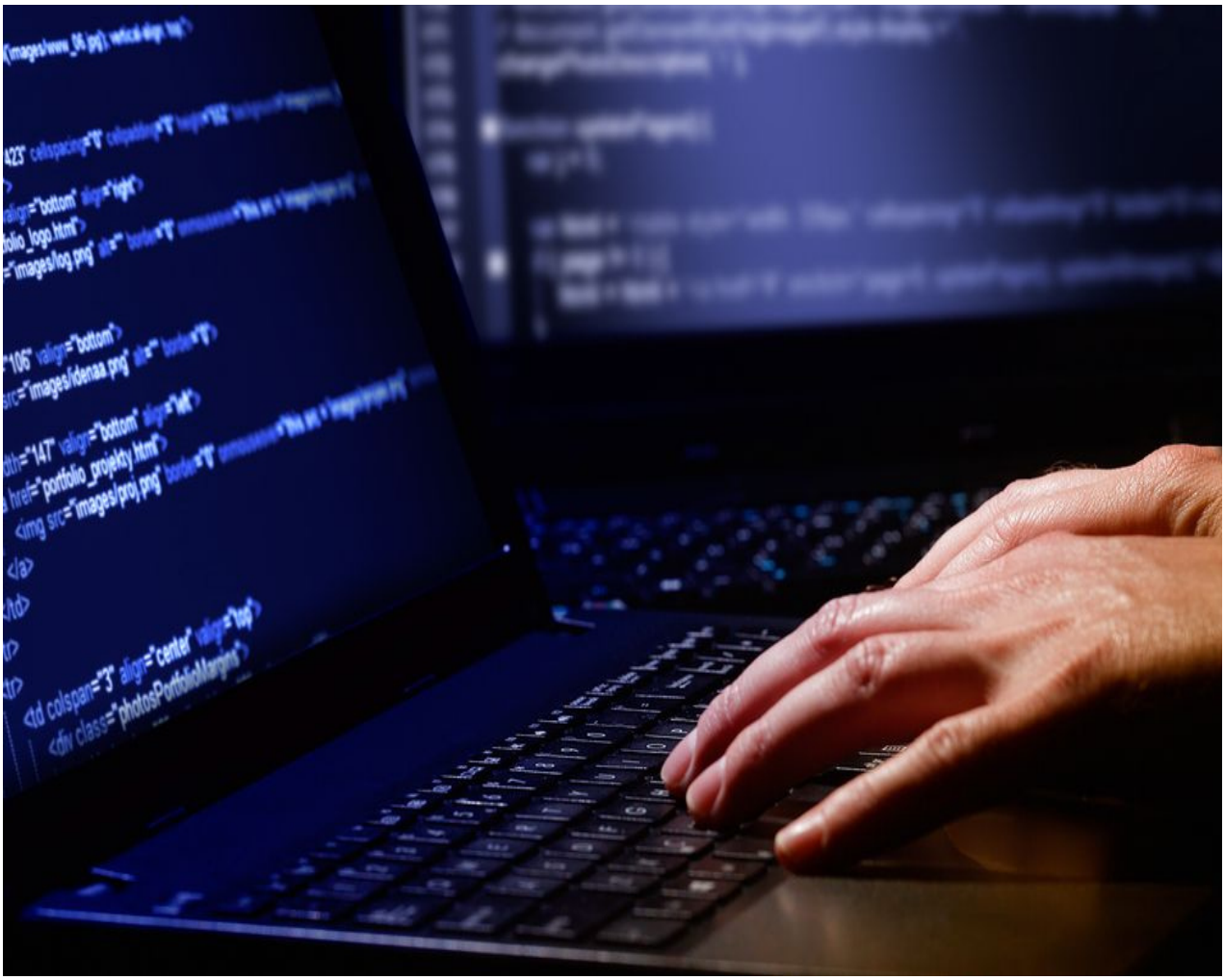
The Virgin Islands Consortium

Russian Gang Amasses Over A Billion Internet Passwords

Technology / **Published On August 05, 2014 10:24 PM /**

Ernice Gilbert August 05, 2014



(The New York Times) -- A Russian crime ring as amassed the largest known collection of stolen Internet credential, including 1.2 billion username and password combinations and more than 500 million email addresses, security researchers say. Security has a history of uncovering significant hacks, including the theft last year of tens of millions of records from Adobe Systems.

The records, discovered by Hold Security, a firm in Milwaukee, include confidential material gathered from 420, 000 websites, ranging from household names to small internet sites. Hold Security would not name the victims, citing nondisclosure agreements and a reluctance to name companies whose sites remained vulnerable. At the request of

The New York Times, a security expert not affiliated with Hold Security analyzed the database of stolen credentials and confirmed it was authentic. Another computer crime expert who had reviewed the data, but was not allowed to discuss it publicly, said some big companies were aware that their records were among the stolen information.

Alex Holden, the founder and chief information security officer of Hold Security, has a history of helping uncover significant data breaches. Credit Darren Hauck for The New York Times “Hackers did not just target U.S. companies, they targeted any website they could get, ranging from Fortune 500 companies to very small websites,” said Alex Holden, the founder and chief information security officer of Hold Security. “And most of these sites are still vulnerable.”

There is worry among some in the security community that keeping personal information out of the hands of thieves is increasingly a losing battle. In December, 40 million credit card numbers and 70 million addresses, phone numbers and additional pieces of personal information were stolen from the retail giant Target by hackers in Eastern Europe.

And in October, federal prosecutors said an identity theft service in Vietnam managed to obtain as many as 200 million personal records, including Social Security numbers, credit card data and bank account information from Court Ventures, a company now owned by the data brokerage firm Experian.

But the discovery by Hold Security dwarfs those incidents, and the size of the latest discovery has prompted security experts to call for improved identity protection on the web.

“Companies that rely on usernames and passwords have to develop a sense of urgency about changing this,” said Avivah Litan, a security analyst at Gartner, the research firm. “Until they do, criminals will just keep stockpiling people’s credentials.”

Websites inside Russia had been hacked, too, and Mr. Holden said he saw no connection between the hackers and the Russian government. He said he planned to alert law enforcement after making the research public, though the Russian government has not historically pursued accused hackers.

So far, the criminals have not sold many of the records online. Instead, they appear to be using the stolen information to send spam on social networks like Twitter at the behest of other groups, collecting fees for their work.

But selling more of the records on the black market would be lucrative.

While a credit card can be easily canceled, personal credentials like an email address, Social Security number or password can be used for identity theft. Because people tend to use the same passwords for different sites, criminals test stolen credentials on websites where valuable information can be gleaned, like those of banks and brokerage firms.

The hacking ring is based in a small city in south central Russia, the region flanked by Kazakhstan and Mongolia. The group includes fewer than a dozen men in their 20s who know one another personally — not just virtually. Their computer servers are believed to

be in Russia.

“There is a division of labor within the gang,” Mr. Holden said. “Some are writing the programming, some are stealing the data. It’s like you would imagine a small company; everyone is trying to make a living.”

They began as amateur spammers in 2011, buying stolen databases of personal information on the black market. But in April, the group accelerated its activity. Mr. Holden surmised they partnered with another entity, whom he has not identified, that may have shared hacking techniques and tools.

Since then, the Russian hackers have been able to capture credentials on a mass scale using botnets — networks of zombie computers that have been infected with a computer virus — to do their bidding. Any time an infected user visits a website, criminals command the botnet to test that website to see if it is vulnerable to a well-known hacking technique known as a SQL injection, in which a hacker enters commands that cause a database to produce its contents. If the website proves vulnerable, criminals flag the site and return later to extract the full contents of the database.

“They audited the Internet,” Mr. Holden said. It was not clear, however, how computers were infected with the botnet in the first place.

By July, criminals were able to collect 4.5 billion records — each a username and password — though many overlapped. After sorting through the data, Hold Security found that 1.2 billion of those records were unique. Because people tend to use multiple emails, they filtered further and found that the criminals’ database included about 542 million unique email addresses.

“Most of these sites are still vulnerable,” said Mr. Holden, emphasizing that the hackers continue to exploit the vulnerability and collect data.

Mr. Holden said his team had begun alerting victimized companies to the breaches, but had been unable to reach every website. He said his firm was also trying to come up with an online tool that would allow individuals to securely test for their information in the database.

The disclosure comes as hackers and security companies gathered in Las Vegas for the annual Black Hat security conference this week. The event, which began as a small hacker convention in 1997, now attracts thousands of security vendors peddling the latest and greatest in security technologies. At the conference, security firms often release new research — to land new business, discuss with colleagues or simply for bragging rights.

Yet for all the new security mousetraps, data security breaches have only gotten larger, more frequent and more costly. The average total cost of a data breach jumped 15 percent this year from last year, to $3.5 million per breach, from $3.1 million, according to a joint study last May, published by the Ponemon Institute, an independent research group, and IBM.

Last February, Mr. Holden also uncovered a database of 360 million records for sale, which were collected from multiple companies.

“The ability to attack is certainly outpacing the ability to defend,” said Lillian Ablon, a security researcher at the RAND Corporation. “We’re constantly playing this cat and mouse game, but ultimately companies just patch and pray.”