KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

August 21, 2014

Russian Hackers Stockpile Over 1 Billion Internet Credentials

Industry Leaders Across All Sectors Likely Impacted

A Russian hacking group reportedly engaged in the largest known cyberattack by amassing over 1.2 billion unique sets of usernames and passwords and 500 million email addresses from more than 420,000 web and FTP sites. The attack was uncovered by Hold Security, an information security company based in Milwaukee, which has been investigating the attack for several months. Various news reports have confirmed the company's findings.[1] Among the victims are "leaders in virtually all industries across the world,"[2] including "the auto industry, real estate, oil companies, consulting firms, car rental businesses, hotels, computer hardware and software firms and the food industry," but Hold Security is not naming specific victims.[3] The security firm intends to reach out to individual victims confidentially.[4] The Russian hackers reportedly utilized a hacking technique known as a SQL injection, which exploits a security vulnerability in an application's software to inject malicious code.[5]

Companies that are victims of the cyberattack that collect information from California and Florida residents may have an obligation under those state data breach notification laws to notify affected individuals and government agencies. In California and Florida, personally identifiable information includes an email address or username in combination with a password, among other data elements. If consumer usernames or email addresses and passwords were stolen by the Russian hackers, companies that collect that information from California or Florida residents may have a duty to notify the consumers and report the breach to government authorities.

In addition, even the state data breach notification laws that do not define personal information to include usernames and passwords may be implicated if there is evidence that the hackers use the stolen usernames and passwords to gain access to a consumer's account and are able to obtain additional personal identifying information about the consumer from the website. For example, the hackers could use the login information to gain access to the user's account information, including potentially the consumer's name, date of birth, address or account numbers. Although there are no reports that the hackers have used the username and password information to gain access to additional personal identifying information

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Elizabeth K. Hinson
+1 404 572 2714
bhinson@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

available on the websites, if that activity is suspected, entities may have an obligation under state data breach laws to notify consumers.

This massive attack highlights the need for increased website security across all industries. Companies should no longer rely on "trusted" web applications to adequately protect their information. Instead, companies should focus on implementing their own network defenses. Website managers should immediately start testing their sites for intrusions and update any patches available for their web servers, database servers, and applications. Clients should also contact third-party service providers to ensure that those vendors are monitoring for fraud and updating any security patches. Clients should take proactive measures immediately, such as performing a risk analysis to assess potential risks to the personally identifiable information they collect and maintain. Clients should ensure that they collect only data that is necessary and adopt technical measures to protect data, including encryption or suitable hashing mechanism. Clients should also update privacy policies and procedures, and implement procedures to identify and respond to breach events.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

---

[1] *See* Press Release, "You Have Been Hacked!", *available at* http://www.holdsecurity.com/news/cybervor-breach/; *see also* Nicole Perlroth & David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, N.Y. TIMES (Aug. 5, 2014), *available at* http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0; Danny Yadron, *Russian Hackers Steal 1.2 Billion Usernames and Passwords, Security Firm Says*, WALL ST. J. DIGITS BLOG (Aug. 5, 2014 8:43 PM), *available at* http://blogs.wsj.com/digits/2014/08/05/security-firm-russian-hackers-amassed-1-2-billion-web-credentials/.

[2] *See* Press Release, *supra*.

[3] *See* Donna Leinwand Leger, Elizabeth Weise & Jessica Guynn, *Russian Gang stole 1.2 billion Net passwords*, USA TODAY (Aug. 5, 2014), *available at* http://www.usatoday.com/story/tech/personal/2014/08/05/russian-gang-stolen-passwords/13639285/.
[4] *See* Press Release, *supra*.
[5] *See* Nicole Perlroth & David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, N.Y. TIMES (Aug. 5, 2014), *supra*.