Akin Gump
STRAUSS HAUER & FELD LLP

Privacy and Data Protection Alert

August 6, 2014

Russian Hackers Reportedly Obtain Internet Credentials of More Than 500 Million Users

On August 5, *The New York Times* reported that Russian hackers have obtained what could be the largest collection of confidential data in history. The security firm that discovered the breach continues to alert affected companies to possible exposure. Although the hackers remain anonymous, affected companies have unconventional legal tools at their disposal to limit the damage.

Background

According to *The New York Times*, “a Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion username and password combinations and more than 500 million email addresses.”[1] Hold Security, the consulting firm that discovered the breach, has declined to publicly identify specific victims to date, but the list will undoubtedly include some of the largest companies in the United States. The hackers are reportedly “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.”[2] The perpetrators have yet to sell the illegally obtained usernames, passwords, or other confidential information, but are apparently profiting by spamming social networking sites like Twitter.

Analysis

Internet Service Providers (ISPs) can serve as a powerful partner to neutralize, if not identify, an anonymous online threat, but it usually takes a court order to get their attention. Here, the hackers’ conduct is actionable under a wide range of laws. For example, the Computer Fraud and Abuse Act generally makes it a crime to intentionally access a computer without authorization and obtain information for commercial advantage or private financial gain. *See* 18 U.S.C. § 1030(a)(2). Other possible actions include the Electronic Communications Privacy Act, 18 U.S.C. § 2701, the CAN-SPAM Act, 15 U.S.C. § 7704, the Lanham Act, 15 U.S.C. § 1114, and even common law conversion.

Affected companies do not need to identify the hackers to take immediate action. Victims of the latest cyber-attack may file so-called “John Doe” lawsuits, referring to the defendants with any information available, such as aliases and messaging addresses. Such actions could theoretically be brought in any federal court in the United States upon a showing that the Russian hackers directed their malicious activities toward networks and users located within a given federal district.

[1] Nicole Perlroth and David Gelles, “Russian Gang Amasses Over a Billion Internet Passwords”, *The New York Times*, Aug. 5, 2014, http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

[2] *Id.*

Once the hackers fail to answer the complaint within 21 days, federal courts have authority to enter emergency restraining orders against the John Doe defendants to avoid immediate and irreparable harm to the companies. Such an order and default judgment would provide a powerful tool even against anonymous hackers. Affected companies could then contact the ISPs connected to the hackers' IP addresses. With a court order in hand, ISPs would start the process of disabling traffic involving the hackers' IP addresses and begin limiting the damage.

As we have seen in recent cybercrimes, companies can ill-afford to resort to what *The New York Times* refers to as the "patch and pray" defense.[3] Even against an anonymous threat, there are ways to go on offense immediately.

[3] *Id.*

Contact Information

If you have any questions regarding this alert, please contact:

Mark J. MacDougall
mmacdougall@akingump.com
202.887.4510
Washington, D.C

Kristine L. Sendek-Smith
ksendeksmith@akingump.com
202.887.4078
Washington, D.C.

Connor Mullin
cmullin@akingump.com
202.887.4493
Washington, D.C.

This document is distributed for informational use only; it does not constitute legal advice and should not be taken as such.