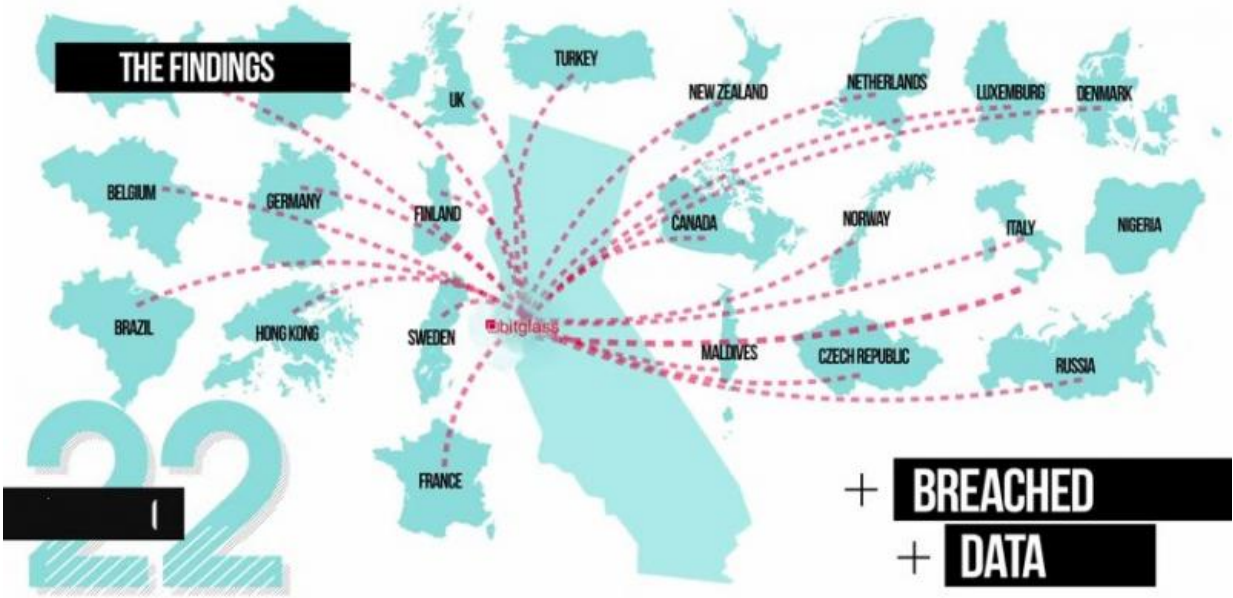# BitGlass experiment highlights the speed at which stolen credit card information is disseminated

April 8 2015, by Bob Yirka

California based BitGlass, a security broker and data protection company, has conducted an experiment to learn more about what happens to consumer data when it is stolen—in this case, credit card information. They have published the details of their experiments and results on their web site.

As representatives for the company note, little is known about what happens to credit card information when it is stolen off a breached server, as has been carried off infamously of late with companies such as Target, Home Depot, and PF Chang. To learn more, researchers at the company created an Excel file and filled it with dummy credit card information—along with a call-back watermark. They then posted the file on seven "darknet" sites and several other upload sites. When anyone opened the file, the watermark caused the user's IP address, geographic location and access device type to be sent back, allowing the researchers to track file access. All they had to do was sit and wait for someone to take the bait.

Initially, there was not much action—during the first week the file got only 200 views, but then, things changed, over the course of the next four days, they file was read by 800 more people—after 12 days they found the file had been opened and read 1,081 times by people in 22 countries. And that, the researchers surmise, is likely the very tip of the iceberg. People and groups who work the dark underbelly of the Internet use IP masking techniques, thus, it was impossible to track down actual human beings. But, because of the nature of the addresses, the team suspects that the majority of action on the file was done by organized groups in Russia and Nigeria. The team suspects that the data in the file made its way to unknown places as well, and likely was opened by many more people. They even had one report of someone attempting to buy something online using one of the fake credit card numbers they had placed in the file.

The team at BitGlass believe their study has revealed two important things; the first is that people really are using stolen credit card information as both currency (by selling it) and by attempting to make purchases with it. The second is that there appears to be a critical time lag between a breach and when stolen data becomes widely dispersed, which suggests if breaches were detected and reported earlier, it might

be possible to prevent data from making its way to crime networks across the globe.

   More information: — pages.bitglass.com/Bitglass_Wh … our_Data_Report.html

— www.marketwired.com/press-rele … dark-web-2007082.htm

© 2015 Tech Xplore