Why Isn't The Federal Government Shutting Down Websites That Sell Stolen Credit Card Numbers?

December 3, 2014 - It may surprise you to learn that one year after the Target data breach, credit card numbers that were stolen in that breach are still for sale on the internet. In fact, there are a number of sites that cater to hackers all over the world, forming a virtual market place for the sale of stolen credit card information. These sites are well known to the hacking community, those who purchase stolen credit cards and to law enforcement agencies around the globe. This begs the question, why isn't government attempting to shut these sites down?

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

A few years ago, the federal government began to move aggressively against websites engaged in file trading. These sites typically trade "torrent" files that allow anyone to share files at very high data transfer speeds. The files that are traded on them are often first run movies, music and software; all at no cost to the people doing the trading. In other words, users of these sites were steeling the intellectual property of companies that created the files being traded.

To stop this type of behavior, US law enforcement agencies began to seize websites that were involved in file trading. At the same time, they issued arrest warrants for the people behind the sites and worked with international law enforcement agencies such as Interpol to make arrests.

After a website was seized, visitors to the site would see a warning with the FBI's logo on it, warning them that file trades that included copyrighted material was illegal and could result in large fines and possible imprisonment.

Those governmental efforts made it much more difficult for file traders to find the content they wanted and convinced many people involved in file trading to leave it behind them.

The comparison of file trading sites to those engages in the sale of stolen credit cards isn't "apples to apples" because of where the sites are located. Most of the large file trading sites were located in Western Europe and North America; areas with strong law enforcement agency presence and governments which typically cooperate with each other on law enforcement matters. Most the sites involved in credit card number sales are located in places like Russia and the Ukraine; places with weaker law enforcement agencies or which don't have the same incentive to cooperate with countries in the west.

These differences mean that it is unlikely that the people behind these sites will be arrested any time soon. But that is no reason to allow their sites to continue their operations.

The US government could simply obtain court orders to seize the domain names for any sites they know of. Visitors to those sites could then be redirected to a warning that is similar to the one that is used on file trading sites.

We know that this won't stop new sites from popping up on the internet, and we have no illusion that this would stop future data breaches. But there is absolutely no reason for law enforcement agencies to sit back and allow these sites to continue to operate in the open; making the resale of stolen credit card data a simple matter. It is time for the federal government to complicate the lives of those engaged in credit card number resales.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS