

Hackers Targeting Real Estate Agents And Their Customers In Malware Attacks

February 13, 2018 - There is a growing trend in financial crimes and malware attacks. Real Estate Agents and their clients are being heavily targeted right now with a number of different scams; all of which have the same goal. Their aim is to separate home buyers and sellers from their money.

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);  
})();
```

Hackers are actively attempting to infiltrate the databases maintained by most real estate offices. These databases typically include contact information for existing and potential real estate buyers and sellers. Once they have their hands on this data, the online attacks begin. Unfortunately, they take many forms.

There are scams that appear to come from online retailers for large purchases. Click on the links in the message and your computer becomes infected. In some cases, you'll download software that scours your computer for financial records. In others, you'll be downloading ransomware.

Another scam sends an email message to buyers that appears to be a change of wire transfer instructions. This particular scam is extremely detrimental because it can lead to the buyer's entire deposit being stolen. Given that many buyers deposit 20% or more of the purchase value as their down payment, the amount of money at stake and the impact on victims is tremendous.

Real estate offices also make attractive targets. One recent attack looked like an email message that contained a link to secure title documents. The message was sent to a Realtor® and the entire body of the message was actually a clickable. A single mouse click anywhere in the body of the message would have infected the firm's computer system. There is no telling the amount of damage this scam would have caused if it had been successful.

The reason for the apparent increase in activity in the real estate industry is simple to understand. Home purchases are the largest single purchase that most people will ever make. As such, there are huge sums of money changing hands. There is also a lot of personally identifiable information contained in real estate data basis. Crooks know all of this so they are targeting the industry.

Anyone involved in a real estate transaction can significantly reduce the risk of becoming a victim by taking the time to make a few phone calls. If you receive a message having to do with wire instructions, pick up the phone and call both

your agent and your escrow officer to make sure the documents are legitimate. Before opening any attachments, or following any links, talk to your agent to make sure he actually sent the message to you.

Real estate transactions involve a lot of paperwork. It's very easy to get a little sloppy about following computer security protocols, but that also makes it fairly easy to make a mistake that can cost tens of thousands of dollars.

by Jim 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