The New Hacking Threat that Everyone Needs to Know About

September 20, 2019 - Let's say you're running a business and you buy a new software suite from a trusted software developer. To be clear, this software isn't from some fly-by-night company you've never heard of. It's a known industry source that has a good reputation and which you trust. You download install it onto a server that you know has absolutely no viruses. Do you think your first thought might be that the software package you installed has hidden malware in it? Probably not, but maybe it should be.

That scenario is exactly what happened with two hotel chains according to an article in DigitalMunition. They installed client booking and payment software from a company called Roomleader that turned out to contain some very sophisticated malware. And it happened because Roomleader's own supply chain was compromised.

NOTE: Nearly 200 hotels were compromised. The malware installed was a credit card skimmer that worked only on cell phones, but which didn't impact computer-based bookings. DigitalMunition speculates that this was to avoid early detection by anti-virus software. If you want to know more details about this particular attack, read the article we linked to, above.

This scenario raises a lot of questions. It isn't uncommon for software developers to contract with other companies or individual developers for certain work. But what if the company you're contracting with has a problem? What if they contract with an individual programmer who has other motivations? And how do all of the legitimate parties in the supply chain protect themselves?

None of the answers to these questions are clear and laws around the globe would appear to be holding the wrong parties accountable for this sort of crime. In this case, who would you blame? The hotel companies purchased software which they had every reason to believe was secure. The chances are that this issue will cost them money. And the software company selling the product certainly wouldn't have released it if they had any reason to think that it was compromised. Since we don't have details yet on what led to the supply chain issues, we don't have any way of knowing if the portion of the software that was compromised was developed in-house or outsourced. But even if it was outsourced to third parties, it's certainly going to cost them money.

Meanwhile, the hackers behind this plot go on their merry way.

There is no doubt that consumers were hurt in this attack and that they should have some recourse. But the companies were hurt too. What's their recourse? That's a question for lawmakers and it is one that needs to be addressed sooner rather than later. While it is quite likely that larger businesses will be able to absorb the costs associated with cases like this, it's a different story for small businesses.

If you are a one-man shop, or even if you have two or three employees, unless you work in the IT industry there is a pretty good chance that you're not technical in nature. You shouldn't face the prospect of going out of business simply for installing software from a trusted source. But that is a very real possibility the way the laws are currently written.

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 ACCESS