The Goal Of New Malware Is Destruction Of Your Business

February 6, 2018 - Over the years we've seen cybersecurity threats to business grow. It used to be that both businesses and individuals were targets for computer viruses and Trojans that were, by today's standards, pretty benign. In many cases, they were designed to load one advertisement after another in an attempt by their designers to get paid for every ad shown. Then came viruses designed to steal financial information, phishing attacks designed to trick victims and more recently ransomware, designed to force victims to pay a ransom or lose all of their data. But now a new threat that poses as ransomware is actually far worse. Not only is a ransom extorted from victims, but in the end the people behind these programs destroy the data on infected computer systems even after a ransom is paid. The goal is to completely destroy your business.

IT News Africa is calling this new breed of ransomware "destructionware." It's an appropriate name given the outcome to businesses that get hit with it. And like other sophisticated malware programs, once a single computer on your network becomes infected with destructionware, the program has the ability to duplicate itself and then propagate across all of the computers on your network.

You might ask why anyone would want to cripple your business in this fashion. The fact is that there are many reasons. It could be that you fired someone recently. Or it could be that you have an existing disgruntled employee. Both would have motive. Another possibility is that you have a smaller, weaker competitor that is looking to reduce competition.

The fact is that none of these people need to be able to program themselves. Malware can be purchased on the dark web as a service. Just tell the hackers you purchase it from who your target is and what you want to accomplish. Pay a fee and you'll have your devious little program in no time flat. You'll probably even be able to set it up in such a way that any ransom paid will be deposited overseas and then sent back to you anywhere you liveâ€¦ for an additional fee of course. This makes catching the person behind such an attack very difficult.

Companies large and small need to be concerned about this type of an attack. They need to have policies about who can load or make changes to their system software. They need to be stripping links out of email messages and making them unclickable. But even this won't offer complete protections. The only way they can actually immunize themselves is to be doing daily data backups; something that most companies don't do. Criminals know this and they take advantage of it.

Will 2018 be the year of destructionware? The answer remains to be seen. It doesn't really matter what happens, as long

as it happens to someone else. But it will matter to you a lot if you become a victim, even if you are the only victim this year. The bottom line is that now is the time to start backing up your data. Not doing so could result in the annihilation of your business.

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