Rentable Ransomware Now Available

May 2, 2016 â€“ Just in case you are not familiar with the term, ransomware is software that invades you PC, encrypts your important files and then demands a ransom from you. If you ever want to see your data again, you pay the ransom. But payment is no guarantee that youâ€™re dealing honorable crook. You could find yourself in a position that youâ€™ve lost your money and still never get access to your files again. In short, ransomware is very nasty stuff.

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);
})();

In most cases, ransomware gets installed on PCs by users who click on bad links. Once installed, the more sophisticated ransomware may be able to self-propagate across your entire network. That means that once you install it on one PC, it will eventually be installed on every PC in your network. For businesses, this can be devastating.

As bad as ransomware is, until recently it has been accessible only to the hackers that developed ransomware for their own use. Unfortunately, some industrious hackers have come up with a new plan. They are now copying the business model of some of the worldâ€™s largest software producers and have started selling â€œransomware as a service.â€•

The business model is fairly simple. Letâ€™s say you can gain access to a companyâ€™s computer network but you donâ€™t h the technical capability to develop ransomware of your own. No problem. You simply work with a hacker group that sells ransomware as a service. That hacker group supplies you a copy of the software, which you then install on your companyâ€™s computer network.

Once the companyâ€™s files have been encrypted, you set the amount for the ransom. As the money comes in, the hackers collect a feeâ€¦ it could be a flat fee or a percentage of the ransomâ€¦ and you get the rest of the money.

For corporate America, this model should be quite frightening. How many companies have disgruntled employees who wouldnâ€™t think twice about doing something like this? And even if your employees are upset with you, if they are having personal financial problems the temptation to defraud you in this way could prove to be too much.

Unfortunately, there has been a push across the United States to prevent employers from checking the credit history of many of their employees. That means that as an employer, there is a good chance that you donâ€™t know which of your employees are having financial issues. And since it is now common for everyone from receptionists to the CEO to have computer network access, most organizations will have significant exposure to this type of fraud.

Companies would be well advised to develop network security protocols that limit the ability of employees to install any type of software. They should also consider daily backups of their data at specific times during the day. This would insure that any ransomware installation could only threaten a limited amount of company data.

Companies should also assess the need for employee network access and take a look at state laws to see if they can legally check the credit of employees who are granted access.
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