RaaS Makes It Possible for Anyone to Kidnap Your Vital Data

By Chuck Cook, RenovoData

Would-be extortionists can now order easy-to-implement ransomware kits on the Dark Web. Just over a decade ago, IT users began experiencing attacks of ransomware, and in the intervening years it has become the most widespread and damaging variety of malware, gaining international notoriety as a threat to individuals and organizations large and small. Ransomware enters systems through fake emails or other notifications, capturing data and holding it captive until a ransom is paid. Even then, hackers often do not release the data. In fact, many ransomware weapons do not even have a way to be disarmed, even by the hackers, so payment is useless.

The FBI and other law enforcement agencies worldwide began to go after ransomware perpetrators as soon as the malware first appeared.

Because 3PL and trucking companies' operations are so fast-moving, computer users are required to work quickly and efficiently. This increases the possibility of rapid and mistaken reactions to tempting messages that seem to come from vendors, coworkers, or customers, so an extra layer of caution is imperative.

What's more, the risk of attacks is on the rise because new tools are available for people with no technical expertise to create powerful ransomware. It is likely that many of these beginner crooks plan to go after specific companies or industries, meaning that 3PL and trucking companies are in greater danger.

Until recently, ransomware was the work of skilled hackers, but now anyone can get in on the act. The new category is RaaS—Ransomware as a Service. It is presented like ordinary, legitimate products and services.

Anyone who can use a computer can go to the Dark Web, buy an RaaS kit, build an effective ransomware program and attack individuals and businesses. In most cases, there is no initial fee, and payment to the RaaS provider is made in the form of percentages of the extorted funds. Some RaaS offerings are marketed as branded products and others are simply customizable generic packages.

One of the best-known ransomware brands is CryptoLocker, which debuted in 2013. It was so successful that imitators such as Xorist, CryptoBit, CryptoDefense, and Cryptowall soon appeared.

The FBI and other law enforcement agencies worldwide began to go after ransomware perpetrators as soon as the malware first appeared. While law enforcement has achieved considerable success, new varieties of malware appear constantly. Predictably, RaaS has added significantly to ransomware's proliferation.

Recently, a package called Satan is the leading international RaaS threat. It is well-made, cleverly marketed, and comes with thorough, well-written instructions. Along with being highly destructive, it is skillfully designed to stymie malware-preventing software.

Satan has many imitators, which offer their own enhancements and features. Some are specialized to the extent that they can target certain industries, companies, or regions. This raises the risk to 3PL and trucking companies, in part because they have so many connections to other companies that messages can more easily be disguised by a hacker who knows something about the business. A user who is accustomed to corresponding with many organizations is less likely to notice an address similar to that of a frequent contact.

In a departure from the ransomware norm, some Satan variations require a pre-delivery fee, plus a share of stolen funds ranging from 5 percent to 30 percent or more. One such product is built on the platform of a pirated ransomware-blocking program, so it is geared to anticipate and overcome defensive actions. Moreover, some producers offer lines of malware that can be combined with ransomware to do even greater damage.

Ransomware is a growth industry, and its variants are increasing rapidly, and now RaaS is expanding the instances of attack. Internationally, law enforcement authorities are working together to put an end to these threats, but the war is far from won.

Until it is, what can you do to protect their data? Essentially, the answer is the same as it has been since the emergence of malware: solid system security and recovery capability.

For individuals and small businesses, backing up data frequently on detachable media is easy and effective, but medium-to-large organizations' systems are too complex for such simple solutions. This is especially true for 3PL and trucking companies, since they have so many points of vulnerability in the form of hardware, software, and outside contacts.

The first rule for users at any level is never to open unsolicited emails or other correspondence from unknown sources, and if messages are opened carelessly, never to open attachments within them. Users should make time to always look carefully at addresses, since skillful hackers can often concoct messages that, as mentioned, appear to come from familiar sources. Another common ruse is the use of panic-inducing popups such as "WARNING! Your computer is infected with a dangerous virus. Click here immediately to remove it!" Of course, "clicking here" will cause a viral infection.

Setting up sound user practices is the first step. For 3PL and trucking companies in particular, this should include keeping all employees informed of the need for good practices and the dangers of failing to follow them.

The next step is the establishment of solid data backup and recovery capabilities. This is a case where knowledge is indeed power, so you should become familiar with the basics of ransomware and plan to stay abreast of the latest threats. Only then can you install strong, effective defenses.

Rely on cloud backup as your chief means of immunizing your data against malware. But first, be sure to learn all you can about cloud-storage methods and services, because, while the concept of cloud backup is the same between vendors, available offerings vary widely in quality, functionality, cost, and vendor performance.

A solid disaster recovery process requires thorough, well-informed planning. Take time to consult experts, to study current literature, and to look into available solutions. You may be overwhelmed by the number and variety of offerings, but with diligent investigation you will find reliable tools and methods.

Finally, make sure that the vendors you select know enough about 3PL and trucking companies' operations to provide the right tools and processes.

The author, Chuck Cook, is President of RenovoData.
Michele Vayla, Marketing Director, may be reached at mvayle@renovodata.com or 877-834-3684.