CATIC

Ransomware Downs Cloudstar in Crippling Attack

We have seen several ransomware attacks target companies of an IT nature. Recently, Kaseya suffered a destructive attack, which you can read about here. Now, similar to the Kaseya event in ferocity, Cloudstar, an IT cloud-hosting company for real estate, insurance, etc., has been affected by a highly sophisticated ransomware attack. Cloudstar announced that "due to the nature of this attack, […] our systems are currently inaccessible." Cloudstar's attack is of importance in this instance because the company provides support to more than 42,000 customers. Many of these customers work within the title settlement industry. Since the real estate market is currently soaring, many settlement agents may have issues with their upcoming closings, especially if Cloudstar systems remain down. As one may recall from past agent articles, time and recovery are crucial elements of responses to ransomware-led attacks. When systems and data become unavailable for periods of time, money is lost, and frustrations grow.

Although the news is still developing around what happened with Cloudstar, here are a few items that have been made public:

- As of July 19, 2021, all of Cloudstar's systems are down with the exception of 365 and email encryption.
- A rough estimate indicates that Cloudstar's services may be down for 10-14 more days.
  - Since Cloudstar's services are cloud/web-based, restoration takes longer, as the amount of customer data that needs to be retrieved is far greater.
- Cloudstar has declined to comment on how many of its 42,000+ customers were affected by this attack.
- It is still unclear who is behind the attack. Early assumptions indicate that it is likely state-sponsored, which means that a group of bad actors work in concert with one another and have the support of their nation-state in doing so.
  - Cloudstar has already begun the process of negotiating with the "ransomware gang," as they noted.
- Other title software products, such as Qualia, CATIC's PrepExpress, etc., are offering agents assistance on their closings to help them get through this attack as well.

While Cloudstar does have an arduous road to recovery, companies across the globe can potentially avoid being a victim of ransomware by following the steps below:

- Ensure your AV software is up to date.
- Keep all of your systems up to date with the latest patches, so you are not exposed to new and/or existing vulnerabilities.
- Have spam filters that can possibly catch ransomware-esque files and links.
- Perform regular backups.
- Create a disaster recovery plan. Should your company fall victim to a ransomware attack, the set of tools and procedures currently in place can help in recovering from a cyber catastrophe.

Like the above steps for maximizing the protection of corporate data, IT-based companies, such as KnowBe4, a security awareness platform, have offered products to help you understand how at risk a company network can be. More specifically, KnowBe4's ransomware simulator, "RanSim," can provide a quick glimpse of your current network efficiency. The premise of this product is to simulate over twenty ransomware infections and one cryptomining scenario to uncover any problem areas within your company's network. KnowBe4 has explained that RanSim has the following features:

- 100% harmless simulation of real ransomware and cryptomining infections.
- Does not use any of your own files.
- Just download the install and run it.
- Results in a few minutes!

If you would like to obtain a copy of RanSim, follow the link below to review more details about this product, along with any disclaimers of KnowBe4 that might be worthwhile for your IT department to consider: https://www.knowbe4.com/ransomware-simulator

Statistics were derived from theregister.com, thetitlereport.com, and rismedia.com*

Please contact CATICITSecurity@catic.com if you have questions on this article.