Solution Brief

Recovering from Ransomware with Barracuda Backup

Ransomware is a malware variant that locks an end user's computer or encrypts their files, then demands a sum of money to allow access or decryption. What's worse, if an organization hands over the cash, there are often times when the attacker doesn't play nice and still withholds the key even after payment. Ransomware is problematic for businesses because it not only results in financial loss, but also tainted credibility and lost productivity. However, this situation can be avoided if your organization has taken the steps to implement a ransomware protection plan. In this solution brief, we will discuss some of the steps you can take to prevent ransomware attacks, as well as how to quickly recover from them using Barracuda Backup.

Introduction

Due to the sophistication of today's threat landscape, ransomware can be difficult to catch right at the door. Once this malicious malware crosses the threshold, a business user is hit by a daunting message, informing the user that their computer and files have been seized, and payment is required. What's equally perturbing is that ransomware doesn't discriminate—it can happen to the mom and pop shops to large enterprises. It's not a matter of if a business will get hit, but when.

Protecting Your Organization from Ransomware

Attackers have created many different variations of ransomware over the past few years, such as CryptoLocker, CryptoWall, TorrentLocker, TeslaCrypt, Locky, and Samas. Each of these variations use new methods of infecting their victims' computers, thereby compromising the data and network of many organizations worldwide.

So how can an organization protect itself from ransomware attacks? Luckily, there are numerous precautions that can be implemented to prevent and recover from a ransomware attack. However, a proper malware protection strategy can be summed up into three categories: education, security, and backup.

Education

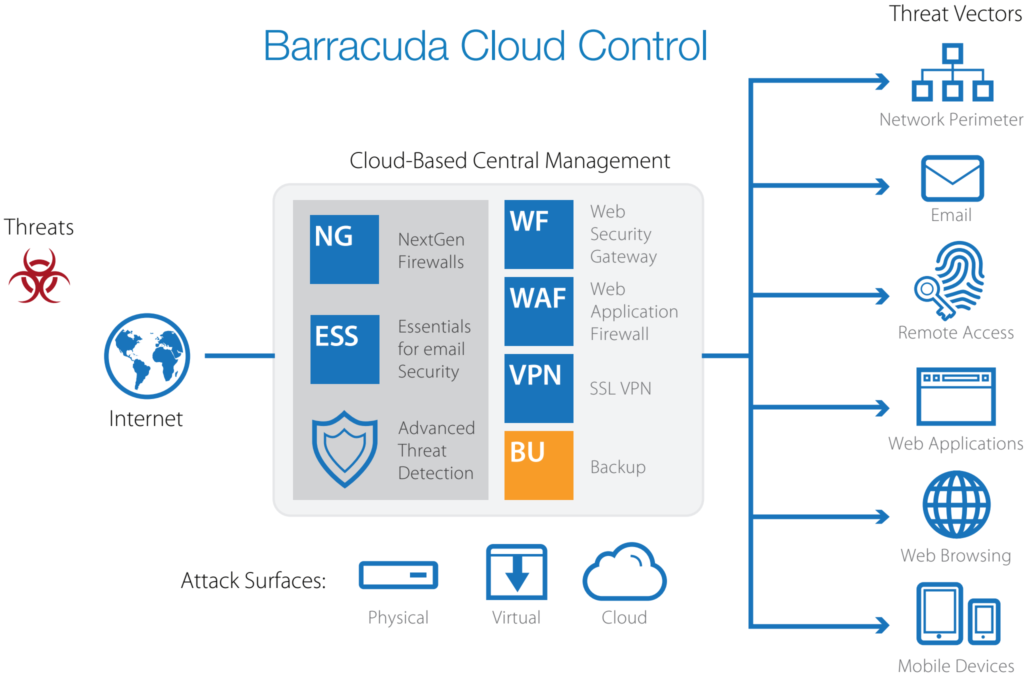
Education is the first line of defense against ransomware. In order for malware to successfully infect a system, it needs some form of user interaction. In a research survey conducted by Osterman Research, and sponsored by Malwarebytes, emails with malicious links or malicious attachments account for 59 percent of ransomware infections. Educating your users about the different types of email and web-based threats can drastically reduce the risk of being infected.

Security

Having multiple layers of defense against web- and email-based threats is essential in preventing malware from entering your organization's network. Since most ransomware attackers target end users, preventive measures on workstations, such as antivirus programs and keeping the operating systems up-to-date, are crucial. While having good antivirus software and patched operating systems are a good start, more advanced layers of security are going to be necessary to prevent most of the threats from even reaching their intended targets. These security measures include securing your network perimeter with a capable firewall, securing your email solution with an email security gateway or service, and having a web application firewall to prevent access to malicious web content.

Backup

Having a sound backup and recovery plan is usually one of the most overlooked measures in the fight against ransomware, but it is the most crucial. Even with all of the preventive measures listed above, there is still a chance that an end user will become infected with ransomware and put your organization's critical data at risk. Successful backups with an effective retention policy enables organizations to recover from ransomware attacks without having to pay any ransom to the attackers, or losing the data altogether. Regularly performing and testing backups will help limit the impact of data or system loss and expedite the recovery process.



Protecting Against Phishing, Ransomware, and Advanced Persistent Threats (APTs) with Barracuda

Not Just Any Backup and Recovery Solution

In an Osterman Research survey, 49.4 percent of companies surveyed indicated that they had been hit with one or more ransomware attacks in the last 12 months. As mentioned earlier, it is not a matter of if, but when your organization will be attacked. Recovering your data and recovering it fast is critical. So how can Barracuda help?

Increased Backup and Recovery Speeds

The entire focus of Barracuda Backup version 6.3 is on increasing backup, offsite replication, and recovery performance – giving customers a quick and efficient way to restore their data and recover from a ransomware attack or disaster. By introducing multi-streaming technology into the Barracuda Backup Agent for Windows and Linux, initial backup and recovery speeds are increased by up to 3X. Shorter backup windows allow you to run backups more often, thereby shortening your recovery point objective (RPO). In addition to faster backups, recovery performance is also increased by the presence of multiple streams of data being written to the target location at once. This helps lower your recovery time objective (RTO) and gets your business back up and running quickly.

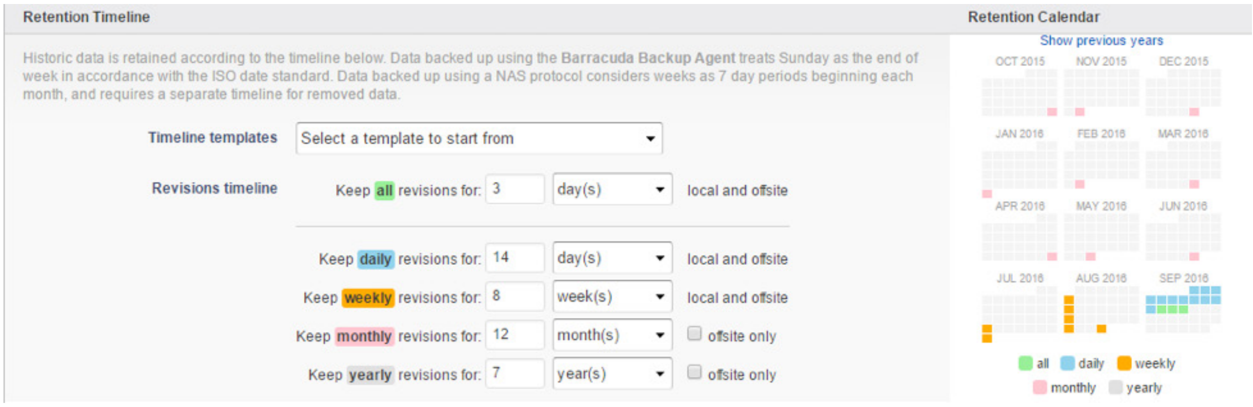
> *With Barracuda Backup, we were able to quickly restore our stolen data, allowing us to address this attack with minimal business impact.*
>
> ***A.J. Murray,***
> *IT Manager*
> *Hayward Tyler*

Enhanced Offsite Replication

While increased backup speeds are great, they are worthless if disaster were to strike in the period of time before the backups were fully replicated offsite. That's why Barracuda Backup 6.3 also includes performance enhancements to the replication queueing system. Combined with Barracuda's inline replication, which begins sending data offsite as soon as data reaches the backup appliance, the new queuing systems helps to further protect customers from a disaster scenario.

Efficient Data Storage and Retention

With its efficient inline deduplication engine, Barracuda Backup is capable of storing more data for longer periods of time. Having an effective retention policy is key to recovering from a malware attack. Barracuda Backup provides flexible and easy-to-configure retention. Policies can be created on a per-server basis with more maximum granularity and control, or on a global basis for simplicity.



Retention Timeline

Historic data is retained according to the timeline below. Data backed up using the **Barracuda Backup Agent** treats Sunday as the end of week in accordance with the ISO date standard. Data backed up using a NAS protocol considers weeks as 7 day periods beginning each month, and requires a separate timeline for removed data.

Timeline templates: Select a template to start from

Revisions timeline:

Keep **all** revisions for: 3 day(s) local and offsite

Keep **daily** revisions for: 14 day(s) local and offsite

Keep **weekly** revisions for: 8 week(s) local and offsite

Keep **monthly** revisions for: 12 month(s) ☐ offsite only

Keep **yearly** revisions for: 7 year(s) ☐ offsite only

Protection Against Advanced Threats

New variants of ransomware, such as Samas (released in 2016), have begun targeting resources on an organizations network. This ransomware encrypts specific files on a system and may encrypt files on mapped network drives. In some cases, certain variants also target and encrypt files on unmapped, open network shares that can be accessed using the user's credentials. Barracuda Backup is protected against these types of targeted malicious attacks. Additionally, unlike other backup solutions that may store backup files to a network share, Barracuda Backup does not present itself as a network share. The data stored on Barracuda Backup is inaccessible to any other devices on an organization's network and the data itself is stored in a proprietary format, which prevents data from being read or accessed by anything other than Barracuda Backup.

Conclusion

While there are solutions that help stop ransomware in its tracks, there are cases where new and complex threats still make it onto the end user's computer. Having a robust backup solution in place helps organizations skip the ransom, and immediately and successfully recover their data. Barracuda Backup does this with ease with fast backup and recovery speeds, an enhanced offsite replication engine, and efficient long-term storage and retention.