Unitrends Ransomware
White Paper

Beat Ransomware in 5 Easy Steps

Be Prepared to Fight or Be Prepared to Pay

Beat Ransomware in 5 Easy Steps

Be Prepared Fight or Be Prepared to Pay

> 4 times in 2016 we were hit by ransomware, and had to restore large amounts of data.
>
> ***James Pomeroy***
> ***Brownlee LLP***
> ***Calgary, Alberta, Canada***

Why you should care

Ransomware has become a Board-level conversation. The threat from ransomware continues to grow as experts say that up to 40% of all email spam contains ransomware. Ransomware has become so prolific that it is no longer a question of "if" you are going to get hit with this type of malware, but when. Don't believe us, listen to the FBI. At a recent conference, Joseph Bonavo¬Ionta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program in the FBI's Boston office, said "The ransomware is that good. To be honest, we often advise people just to pay the ransom."

A solid backup vendor and process is the only protection from an attack, but not all backup vendors completely solve the issue. This paper provides a playbook of five steps organizations should use to protect themselves from the excessive downtime, data loss and business disruption of a ransomware attack.

What is ransomware?

Ransomware is a form of malware that encrypts victim's files with unbreakable encryption and then demands payment, typically around $200 to as much as $40,000 in bitcoins, in order to unlock and get your data back. They use strong, unbreakable encryption. Often this is 256 bit AES, RSA or ECC (Curve) based encryption which is essentially unbreakable. Large numbers of files get infected as it spreads across the network and directories. Attacks are typically delivered through spam messages, exploit kits or "malvertising". CBT-Locker and Torrent-Locker typically prefer spam email campaigns as a delivery vector. While CryptoWall and TelsaCrypt prefer to use exploit kits. Both spam and exploit kits have been proven to be highly effective ways to get into both end user and server-based systems. Newer versions even delay notifying users so they can infect a maximum number of files.

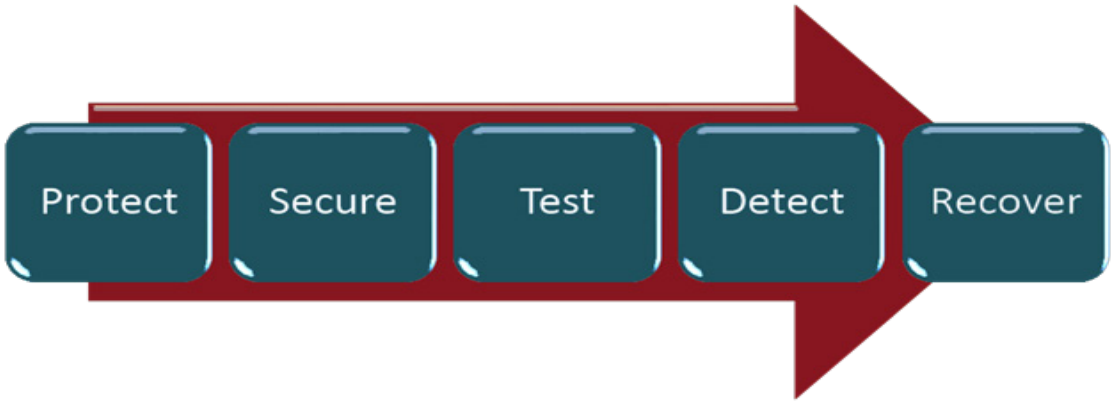
Who is susceptible?

While it may seem like a scare tactic, the truth is that all industries are vulnerable to ransomware. Email, databases and business applications run on similar infrastructure and operating systems across all industries. All are equally vulnerable. However, due to their user community, some industries are more vulnerable than others – those that support large numbers of technically unsophisticated users. Organizations such as schools, retailers and even healthcare provide computing resources to users that are not particularly savvy about the places they visit on the web or the types of email attachments they open. Schools in particular support users highly susceptible to "click-bait" sorts of content. IT organizations can try and educate as much as they can, but it only takes one individual clicking on one file to infect an entire IT infrastructure.

Yes, I've had 2 separate ransomware incidents where users informed me that files they had access to were encrypted with a message about paying a ransom. – *Gary Halbedel, Bethlehem NY School District*

Playbook to beat ransomware

From assisting and observing how successful organizations deal with ransomware we offer this very practical five step approach to prepare for, limit and recover from ransomware. The customer quotes included in this paper are testaments to the effectiveness of the advice.



"We got a very bad crypto virus that spread to our main file server. We had to restore 3TB+ of data and over 2 million files. With our 933S appliance, we were able to restore the files within a few hours. If we still had the LTO backups, this same restore would have taken over a week to perform." – *Exco Engineering*

Step 1 - Protect yourself

The only way to protect your organization, data and computing infrastructure is to perform frequent backups. This greatly reduces data loss in the event of an attack. The FBI also encourages that you secure your backup files in locations not directly connected to you production servers. Unitrends strongly recommends that you follow the 3-2-1 rule; 3 copies of your data, 2 different types of media, 1 copy off-site. You need to isolate and completely disconnect one copy of your backups to keep them from being corrupted by the ransomware attack. For enterprises that exist in only one location, the cloud can be an inexpensive and easier solution to the manual process of creating and moving physical tapes.

"While I can't release details we did have an incident involving ransomware that affected several of our systems. And utilizing our Unitrends data protection infrastructure we were able to respond, contain, eliminate the infection and recover in a matter of minutes! With our old data protection solution this would have taken days! – *John Little, Gila Regional Medical Center*

Step 2 - Secure your Infrastructure

Ransomware was a $1 billion dollar industry in 2016 and is expected to triple in 2017. It's an industry that is constantly evolving with new versions of the software being released and downloaded every day. There is already a ransomware as a service [RaaS] model, which provides automatically generated ransomware executables for anyone who wants to get rich by infecting potential victims. The bottom line is that creating or buying your own ransomware appliance has never been easier.

Because of the wide prevalence of Windows server, ransomware criminals predominantly target Windows-based servers, appliances, PCs, and devices. Rather than protecting your infrastructure, a Windows-based backup appliance can become just another victim of a ransomware attack. Acquire a backup and business continuity solution that is written in hardened-Linux rather than Windows code.

"The Ransomware Attack was the Bit-locker Hack where a banner pops up and tells you to pay up or lose everything forever. At first we thought it was a few corrupt files on the network that people were reporting. That quickly escalated, when we realized that too many files were suddenly being identified as un-openable. Then came the Laptop User Complaint that there was a Window Open that would not close or go away...When we went to investigate that is when we found the answer to what was going on with the Network Files. This all took place over a period of about half a day with recovering just over 500GB of files in all." – *Vance Watkins, Gerson Corporation*

Step 3 - Test, Test and Test Again

It is critical that you always know exactly the time of your last good backup. This is the point that you can be assured that your data is fully protected and available for recovery. Testing should include running trial recoveries up to the point of actually launching a backup application. This ensures that all files, settings, applications and data are available for faster recovery.

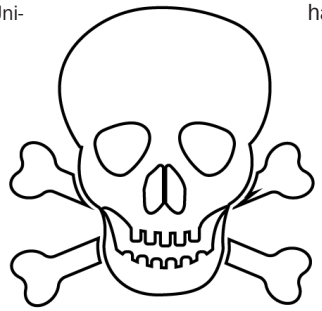
Even the FBI agrees that the only truly effective way to combat ransomware is to regularly back up data and verify the integrity of those backups. Testing provides many advantages in the fight against ransomware. Testing ensures:

- backups are not infected with the ransomware and can be used for data recovery
- recovery will be successful for both physical & virtual machines
- RPO and RTO compliance reports can be generated for HIPAA and other certifications

Testing must be performed no matter where the backup files are located, locally, at a DR site, or in the cloud. Testing should also be fully automated to ensure it is done regularly and not left to "best efforts" of limited IT resources. More advanced backup solutions

automatically test all of your backups, together, and ensure that they recover at the application level.

"The appliances and services are stable and reliable. Our Unitrends appliance literally paid for itself after being able to restore the 2 million+ files affected by ransomware earlier this year. "– *Exco Engineering*



Step 4 - Proactive Detection

Early detection is key to reducing the amount of data that is lost. According to a recent report from a leading analyst: "There might not be a ransom demand immediately; therefore, it is imperative that the activity be noticed quickly. Combined with running select backups during the day, reporting on storage anomalies can help identify that an attack has occurred or is actively underway. This ability to recognize the changes ransomware has made to file structures is called predictive analytics."

Unitrends appliances protect on-premises physical and virtual workloads, cloud workloads, and provide continuity for them across sites and cloud infrastructures. As data is ingested into the Unitrends appliances, the predictive analytics engine analyzes it and utilizes a probabilistic method to identify anomalies to match behaviors that a system would represent if infected with ransomware. An immediate notification is sent to the IT administrators to check for malware in the affected system(s). This proactive detection capability is applicable to physical machines as well as virtual machines and workloads within each. The more frequent the backups the more quickly an attack will be discovered.

"We recently had a ransomware infection pop up on our network. It was (thankfully) identified quickly and the infected machine was shut down, but not before several hundred gigs of data were affected. I spent about an hour going through our servers identifying network shares that would need to be recovered, and about 20 minutes in the Unitrends interface kicking off backups. The inline deduplication provided by our appliances allows us to perform hourly backups of our file servers (and keep 100+ days of retention onsite!), so we only had to deal with minimal loss of data from restores. - *Boston Architectural College*

Step 5 - Fast Recovery

Enterprises need a set of tools and applications that will automatically take action to protect data and apps against just about any type of issue, including ransomware. Vendors such as Unitrends, provide software and services that can support easy and automated restoration of production data to their state prior to the attack. This rapid restoration greatly reduces the amount of downtime and impact to an enterprise. Backup and continuity appliances from Unitrends can act as recovery platforms until production servers are scrubbed and brought back into service. Since clean, tested backup data is already on the appliance, recovery can take just seconds. Cloud recovery can take just as little time if the previous four steps have been followed properly.

'After deployment of Unitrends for about 60 days, I had taken the day off to go fly fishing. Once I came back into cell phone range, I had a multitude of messages indicating no one could access any files on one of the Terminal Servers. Quickly logging in from my phone, I determined that every single user folder item was encrypted for ransomware. I was able to restore to a point before corruption while connected with my cell phone and within 30 minutes, the server was running and accepting client connections with available access to all document folders. We did lose a few documents, but it could have cost us so much more." – *Scott Bacon, Broadway Carpet*

Conclusion

Ransomware is a major threat to every organization and their IT assets. Ransomware is now a board-level conversation as stories of crippling attacks are widely prevalent in the press. Some you may have heard of:

- A ransomware attack lead Los Angeles Valley College (LAVC) to fork over $28,000 after they realized that a ransomware infection left them with no way to recover their organization's encrypted data.
- Last year Hollywood Presbyterian Medical Center paid the equivalent of $17,000 to resolve a ransomware infection. The ransomware didn't just encrypt files but severely affected operations for about 10 days, forcing staff to go back to paper records and fax machines. They had backups, but were unable to recover with them.

If you follow this 5 Step Playbook and prepare properly an attack no longer has to include major data loss, corporate embarrassment, and extended downtimes. Unitrends has worked with thousands of companies to ensure they can quickly detect and recover from a ransomware attack.

As always, all Unitrends products are backed by our expert Customer Support Team, which consistently receives a 98% satisfaction rating for our customers across the globe. Our local partners can also work with you to learn your unique needs and suggest the right solutions to match.

For more information, please visit unitrends.com or talk to a Unitrends Partner.