Unitrends Ransomware
White Paper | May 2016

Take the Ransom Out of Ransomware

How to avoid having your data being held hostage

Take the Ransom Out of Ransomware

How to avoid having your data being held hostage

Ransomware is a form of malware that encrypts victim's files with unbreakable encryption and then demands payment, typically around $200 to $500 in bitcoins, in order to unlock and get your data back.

The Proliferation of Ransomware

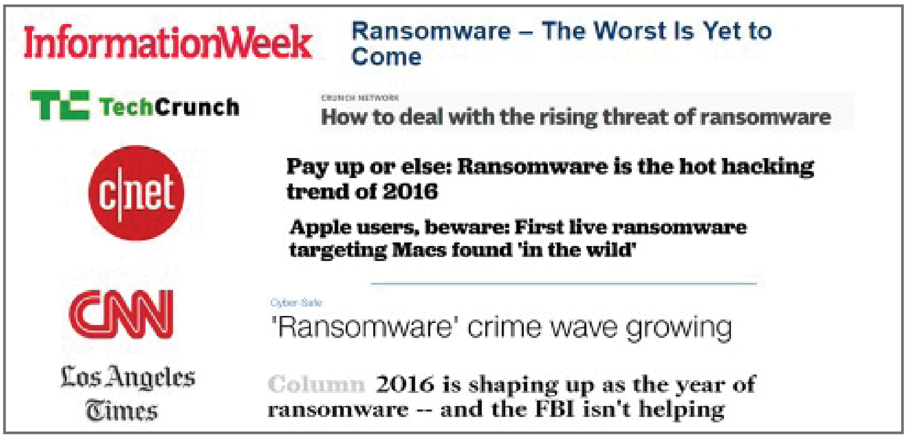
Ransomware has rapidly become one of the most widespread and damaging causes of downtime and data loss for IT systems. It has captured the attention of the press and end-users with leading publications calling 2016 "the year of Ransomware." Ransomware has become so prolific that it is no longer a question of "if" you are going to get hit with this type of malware. It is simply a question of when.

For users and organizations who are not prepared when ransomware attacks, there is little recourse. In fact, at a recent conference, Joseph Bonavolonta, 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 [if you haven't backed up]."

However, for organizations that take the necessary steps, the disruptions can be minimized and data loss can be avoided.

In order to more completely understand the steps that should be taken, this paper gives insight into the rise of ransomware and provides some guidance on protection, backup, and the recovery solutions that organizations should implement.

> "The ransomware is that good. To be honest, we often advise people just to pay the ransom [if you haven't backed up]."
>
> **Joseph Bonavolonta**
> **Assistant Special Agent in Charge of the Cyber and Counterintelligence Program**
> **FBI, Boston** "


InformationWeek
TechCrunch
c|net
CNN
Los Angeles Times

Ransomware – The Worst Is Yet to Come

CRUNCH NETWORK
How to deal with the rising threat of ransomware

Pay up or else: Ransomware is the hot hacking trend of 2016

Apple users, beware: First live ransomware targeting Macs found 'in the wild'

Cyber-Safe
'Ransomware' crime wave growing

Column 2016 is shaping up as the year of ransomware -- and the FBI isn't helping

Background on Ransomware

Ransomware is not new. In fact, forms of ransomware have been around for over a decade. Early forms of ransomware however were largely ineffective. They took on the form of “scare-ware” or “nag-ware”. They simply popped up messages on the screen in an attempt to convince the user that the system was infected with multiple viruses, or to show inappropriate images on the screen and then demand payment to remove them. These early forms did not permanently lock or encrypt files and they were typically fairly easy to remove or avoid. Criminals also had difficulty in collecting fees anonymously. As a result, when those annoying infections popped up occasionally, they were not the scourge that modern ransomware has become.

Everything changed in 2013 when the infamous CryptoLocker first appeared. Cryptolocker used powerful encryption technology to encrypt files and extort payment in bitcoins through anonymous transaction servers. It is a model that has proved highly successful in achieving its goal of extracting money from victims.

Numerous variations, copycats and versions have quickly become established around the globe. Besides CrytoLocker, the most popular variants include TorrentLocker, CrytoWall, CBT-Locker, TeslaCrypt, Locky, plus many others. They use a range of techniques for infection vectors and they employ an assortment of execution methods, but they all share the following major components.

- They use strong, unbreakable encryption. Often this is 256 bit AES, RSA or ECC (Curve) based encryption which is essentially unbreakable.
- They employ some form of online network communication such as I2P network proxies or TOR which can provide anonymous backend infrastructure.
- They require anonymous electronic Payment via bitcoins typically through TOR.

Each is 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.

The spam delivery vector requires interaction from the user. However, it has the advantage of being able to affect fully patched and up-to-date systems. They simply require a user to drop their guard one time to click on the delivery package. Many ransomware variants have been localized and are very convincing in order to dupe victims into clicking on their payloads.

Exploit kits rely on vulnerable software packages installed on the victim’s system. They have the advantage of not requiring any interaction from the user in order to infect the system. They utilize known security holes in existing software to penetrate into the system. Criminal organizations are now so systematic in their hacking methods that

Real World Examples

Ben @coloradogeek 17 March 2015
I get that staying ahead of **ransomeware** is hard enough and @Webroot DID ulitmately catch it, but the 50GB back restore is all **@Unitrends**

Richard Marsh @BackupPro 13 Mar 2015
Working late on a network infected with **#ransomeware.** So much for anti-malware software. Thank Goodness for **@Unitrends** backup and recovery!

Jeff DuPorter 24 Mar 2016 at 10:53 AM
Unitrends backup saved me from **ransomeware**. User opened an attachment in their personal email, and didn’t even realize it was a big deal because I was able to get the affected system fully restored within hours.

lists of vulnerable systems are now sold through coordinated efforts between malware creators with profits being split among collaborators.

As ransomware has become more widespread, the advances in technology and techniques used have also evolved. The first ransomware variants mostly attacked Microsoft Windows based systems. However, in recent months we have seen a new version that is now going after Apple Macs as well. Other advances have included highly localized versions that only target specific systems and targeted geographic areas. These variants are so specific to geography that the spam email message is often more effective because the messages are grammatically perfect and they employ the vernacular typically used in that region. Another feature of ransomware that has evolved since the early days has been the addition of a feature to prove to the end user that the ransomware provider does indeed hold the decryption keys. Most ransomware variants now offer the ability to get one file decrypted for free. This method is used to verify that payment will result in the unlocking of files.

How does an enterprise make sure they never have to pay ransom?

Protecting yourself from ransomware is a little bit like putting together a basketball or football team. A good team will be able to play both defense and offense. The best teams will also have deep benches filled with backup players who can step in at a moment's notice when needed.

For our ransomware offense we want to take some proactive measures that will attempt to keep ransomware out of all user and server-based systems.

- Keep all of your software and operating systems up-to-date. Ensuring that systems are up-to-date minimizes the chances that an exploit kit will be able to find an opening to exploit and deliver a ransomware package.
- Use antivirus software for virus detection on all systems. This is just good common sense to protect against ransomware at runtime. However, many organizations have told us that antivirus software was not sufficient to keep them safe from ransomware.
- Educate users on security protocols. Make sure that your users understand that they should avoid clicking on untrusted emails and attachments. Untrusted websites can also be a source for ransomware so users should be advised against running software, including macros embedded in Microsoft office applications, from locations that may not be trustworthy.

For our ransomware defense, we want to deploy counter-measures that can block the execution of ransomware and prevent it from encrypting our data.

- Disable ActiveX content in Microsoft Office applications. Code embedded in macros is a common infection vector.
- Have firewalls block TOR, I2P and restrict ports. Many ransomware variants require contact with a command-and-control server in order to encrypt files. Restricting access for unused IP ports and specifically blocking TOR and I2P can prevent these versions from successfully completing the required tasks.
- Block binaries from running from popular ransomware installation paths. Many ransomware variants install themselves and run out of a %TEMP% directory. Blocking binaries from being able to run from these paths can possibly thwart the execution of these versions.

Finally, and most importantly, you need to implement a good backup and recovery strategy. This is the surest way of guaranteeing that you can always recover your data regardless of whether your data loss occurred because of a hardware failure, human error, natural disaster, or ransomware attack.

What does a good backup strategy look like for ransomware protection?

In general we want to follow the "rule of three" for backup and recovery. The rule of three simply states that we want three copies of our data, across two different media types (e.g. disk and cloud or disk and tape), with at least one copy off-site. This is good, sound advice but with ransomware we want to look at a few more items to consider due to the unique nature of this type of data loss.

Make sure you backup data on all systems, not just mission-critical systems. Ransomware can attack both Windows and Mac based user systems and servers. We want to protect all of your data for users and for business processes. We do need multiple copies of data. However, with ransomware it's important to have some physical isolation between at least one copy of that data. That geographic isolation will help make sure that ransomware cannot spread across all copies of your data. We want to be able to roll the clock back to a point before we were infected in order to avoid having to pay the ransom.

Cloud empowered continuity

A good solution for ransomware protection will include both local and cloud-based backups. A hybrid cloud implementation provides many benefits. Using local backups, we can quickly recover infected systems with backups stored on the local backup appliance. Cloud-based backups provide an easy way to move copies of your backups off-site. Cloud, unlike tape, enables this process to be fully automated and still get the isolation we need for maximum protection. Ideally, your backup solution will provide the following capabilities.

- Flexible cloud deployment options. Each organization may have different preferences for deploying cloud resources. Some may prefer a private cloud they manage themselves. Others may want a hyper- scale implementation that utilizes a popular public clouds such as Amazon AWS, Microsoft Azure, or Google cloud. Others may prefer a purpose built cloud created and managed by their backup provider. There is no right answer but your backup provider should provide you with the flexibility to choose the one that make sense for you.
- Instant recovery capabilities provide the ability to spin up workloads in minutes from backups using the computer capabilities of the backup appliance to run those workloads while the production system is cleaned. Instant recovery allows us to minimize downtime from a ransomware attack and keep the business running.
- Linux-based backup software – not Windows-based. Most backup software runs on Microsoft Windows. Therefore, these solutions are vulnerable to ransomware attack. Having your Windows-based backup solution attacked is a worst-case scenario for ransomware intrusion. Running your backup software on Linux avoids this potential problem. At this time, ransomware is not frequently attacking Linux based systems.

Keep your business running with Unitrends

Unitrends is trusted by business visionaries and IT leaders and professionals who know that in today's digital world protecting their ideas and keeping their businesses running is nonnegotiable. The Unitrends Connected Continuity Platform™ enables organizations of all sizes to protect their data and assure business continuity for physical, virtual, and cloud based environments. The steadfast Linux-based platform delivers unmatched flexibility as needs evolve and provides 100 percent confidence in efficient, easy-to-use recovery and business continuity.

Backup, recovery, continuity

The platform encompasses a comprehensive, integrated portfolio of continuity services and solutions to protect data, provide disaster recovery and proactively test and assure complete recovery of multi-tier applications. Accessed through a super intuitive user experience, the Connected Continuity Platform combines powerful backup and recovery appliances, cloud continuity services, recovery assurance, disaster recovery services and continuity planning and tools into a full business continuity solution.

Protect everything, anywhere - Continuity for your business

Regardless of whether you are 100% virtualized, 100% physical, have legacy systems running older operating systems or are somewhere in between, your data and business need to be protected. Whether you are just starting on your journey to the cloud, or have a strategic cloud first commitment, your ideas and systems must be assured of continuity.

The Connected Continuity Platform has got you covered with protection for over 220 different versions of operating systems, hypervisors and applications and support for local, private and public cloud based environments. Within one platform that includes integrated backup and recovery capabilities, multiple cloud options, disaster recovery and recovery assurance capabilities and services, you gain 100% confidence that you can protect your business, recover lost data and systems and enable challenged IT leaders and teams to do more with less.

Industry's broadest cloud backup and recovery portfolio

- **Hybrid cloud-empowered backup and recovery appliances** with integrated operating systems as well as complete backup, archiving, replication, instant recovery and cloud integration capabilities. Addressing a broad range of environments, they are available in a choice of deployment options, as purpose built physical appliances or in a virtual format to run on your hardware.
- **Extensive range of cloud options** including long term retention services in the Unitrends Forever Cloud™ or integration with third party Hyperscale clouds including those from Google, Amazon and Rackspace are available. Integration with cloud comes standard with all Unitrends appliances.
- **Unmatched disaster recovery services** provide customized, white glove support from planning through building the environment through rapid spin-up and recovery. Unitrends DRaaS provides a guaranteed one hour SLA for recovery ensures that critical systems are up and running fast. Business continuity is further ensured with the ability to use cloud-based systems while the primary business site is repaired.
- **Automated recovery assurance testing** provides continuous proof that the IT data and multi-tier environment are fully recoverable. Automated testing certifies that RPOs and RTOs are achieved. Results are provided through comprehensive reports generated to satisfy regulatory and corporate policy compliance requirements and eliminate the need for manual IT testing.

Contact Unitrends today
for a customized quote on
randsomeware protection