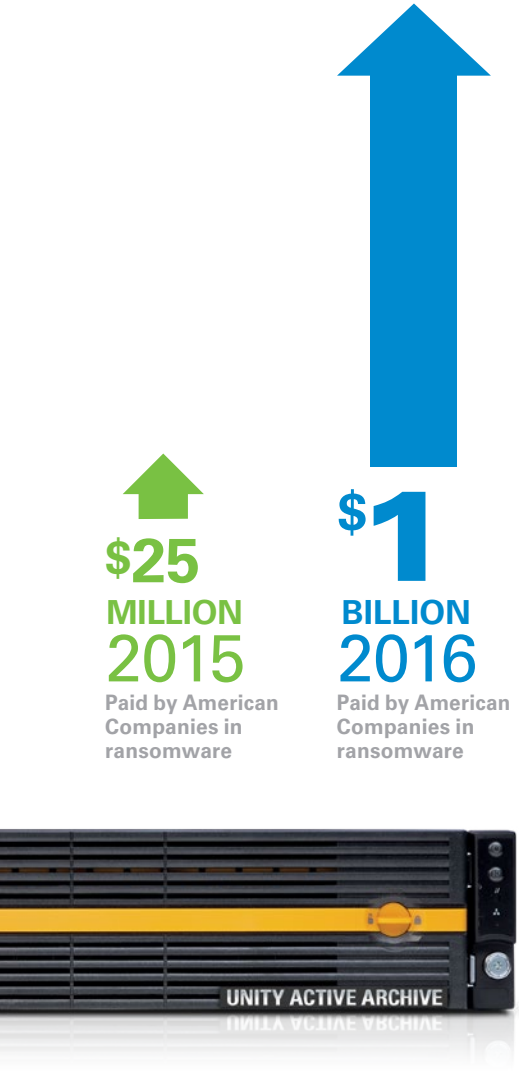
NEXSAN

HOW TO FIGHT RANSOMWARE WITH UNITY® ACTIVE ARCHIVE

Unity Active Archive's built-in resistance to file tampering or destruction gives you real-world protection against ransomware attacks.

(Rev. 3/8/17)

NEXSAN



[Reuters. April 12, 2016. "Ransomware: Extortionist Hackers Borrow Customer-Service Tactics." http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X]

Of all the cybercriminal threats out there, being attacked by ransomware is among the most devastating. It spreads quickly throughout your network, is a nightmare to remove from your machines, and makes any encrypted files inaccessible until you pay the ransom. Unless you have copies of those infected files that you absolutely know to be untouched by the ransomware (and conventional backup solutions simply cannot assure that), you are basically out of luck.

In a nutshell, ransomware extortionists attack your computer network with malware that encrypts every file, and then demands a large ransom payment to a "darknet" site before the decryption key is provided. If you don't promptly send payment, the criminals threaten to delete the decryption key and all your encrypted data will be lost forever. Usually the crooks supply the key after payment is received, but like any other extortionist, they may make further demands or just cut off further communication altogether.

Typically, however, they will send the decryption key, and this is why so many organizations simply suck it up and send the payment. In 2016, the FBI had received reports that American companies paid an estimated $1 billion in ransomware payments, as compared to $25 million in all of 2015. These staggering costs are just the tip of the iceberg compared to the lost productivity and all-too-frequently lost data that result from a ransomware attack.

And the situation's getting worse: With the potential for such massive profits, cybercriminals can afford to pay highly-skilled programmers to create thousands of new types of ransomware attacks every month—which makes detecting them much more difficult. Ransomware has become a major industry, ranking number one in growth rate among illegal enterprises.

Some industry pundits have taken a "blame the victim" attitude, claiming that common ransomware targets (hospitals, schools and police stations) are vulnerable because "they all lack sophisticated cybersecurity like anti-virus, backup, and disaster recovery." But we think those claims are unwarranted, as virtually all of the customers we've spoken to have implemented at least two of these cybersecurity measures.

Here's the real issue: Anti-malware products are not infallible, and when they fail, conventional computer architectures readily allow data corruption by malware that masquerades as the authorized user. We're going to talk about several common-sense precautions you can take to combat this, but for cases where those precautions aren't enough, we'll show you how Unity Active Archive—our hardened archive technology—blocks attempts by malware to delete or corrupt your valuable data.

BACKGROUND - JUST WHAT IS RANSOMWARE?

Simply put, ransomware is a specific type of malware which encrypts your data, then demands a ransom payment before it will decrypt your data. It can vary as to exactly how it infects your computers, whether it communicates with a remote key server or if it generates the key internally, and the specific mechanism for collecting payment. It may have a name like "Locky," "Cryptolocker," "Cerber" or "Ransom32" but you shouldn't be lulled into a false sense of security by thinking that published lists of ransomware names (and their properties) give you a complete picture of all the threats you need to defend against.

In reality, each of those threats may have thousands of variants with distinctly different behaviors; for example, cybercriminals will often capture a specimen of an existing strain of ransomware, make a few changes (including the method of payment demanded) and use it to attack their own list of targets. Often these new variants will elude detection by anti-malware software until a new batch of updates is developed and distributed.

If the ransomware generates or stores its decryption key internally, then it's at least theoretically possible that an anti-malware software vendor might be able to create a tool which removes the infection and decrypts the data without making a ransom payment. Unfortunately, ransomware is increasingly using a remote key generator that's stored in a hidden "dark web" location, accessed via untraceable technologies such as Tor and using unbreakable military-grade encryption such as AES-256.

As a practical matter, if you get hit by this latter type of ransomware, the only way to decrypt your files is to pay the ransom (usually at least $1,000, but it can be much more), and hope the key arrives and the decryption process goes smoothly. The mechanics of paying the ransom vary, but usually involve a cryptocurrency such as Bitcoin (which itself may be too technically challenging for many victims).

Of course, paying the ransom doesn't guarantee you'll be able to recover your files. The criminals might just take the cash and not provide the key, though this appears uncommon. Because the payment process is deliberately convoluted, there are many opportunities for breakdowns in communications where the payment doesn't go through or the key doesn't reach the victim. More common, however, is that some or all of the files will be damaged during the victim's well-meaning but misguided troubleshooting and repair attempts in the initial confusion of the attack, leading to problems with their decryption attempts after paying the ransom.

Nexsan 900 E. Hamilton Ave., Suite 230, Campbell, CA 95008 | 1.408.724.9809

COMMON-SENSE PREVENTATIVE MEASURES YOU CAN TAKE

Because ransomware gets into your network using the familiar paths taken by previous generations of malware, many of the same preventative measures used to fight those earlier threats can help you reduce risk today:

- Teach your users not to visit unapproved websites or click on links within emails unless they were specifically expecting those email links and have no other way to get to the site (for instance, a password reset link). We have found it very helpful to do a live demonstration for users showing them how the URL behind a link may be very different from what they think it is.
- Regularly patch and update the management tools on all your networked devices, including switches, servers, and BYODs. New malware exploits are now published within days of patches being available, so unfortunately your window of relative safety is getting shorter and shorter.
- Find ways to establish non-native rendering of PDF and Microsoft Office documents, so that a browser or a custom app sees a sandboxed, safe view. Note that many exploits hide inside rich document formats.
- Make sure that your users—and especially your administrators—run in the least privileged mode possible while still being able to maintain reasonable productivity. Of course, this is not foolproof as malware has proven very adept at escalating to root or admin privilege levels.
- Disable Remote Desktop Protocol (RDP) unless used in carefully-controlled maintenance procedures.
- Enable your firewalls and deploy all the latest patches; note that some of the newer firewalls can help block traffic from known ransomware, though the jury is still out on their real-world effectiveness.
- Run frequent backups, your last line of defense against utter disaster. That said, consider the practicalities of meeting your recovery time objectives. An "inexpensive" cloud backup service might require the "not-inexpensive" expedited service of copying your data to USB drives and paying a courier to deliver them.

Even with all these precautions, we know of many organizations that have fallen victim to ransomware and other malware. For example, a hospital with a very careful IT department still suffered a massive ransomware attack that encrypted all of their patient radiology studies. Obviously, no hospital wants to be on the news for losing its patient records and being down for days while it attempts to recover files from backups. In this particular case, the hospital's downtime was only a matter of minutes because it had previously deployed a Nexsan hardened archive solution.

Nexsan 900 E. Hamilton Ave., Suite 230, Campbell, CA 95008 | 1.408.724.9809

Figure 1: *Unity Active Archive's unique file serial numbers enable easy identification of missing files.*

Figure 2: *Unique fingerprint enables recurring checks for corrupted files.*

HOW UNITY ACTIVE ARCHIVE PROTECTS YOU AGAINST RANSOMWARE

Unity Active Archive was purpose-built to be a secure, hardened archiver for important, unstructured data. Delivering a higher level of integrity and assurance than conventional servers and storage, Unity Active Archive is designed to provide a superset of the storage requirements of compliance regulations like HIPAA, SEC17a-4, Dodd-Frank, FDA 22, Sarbanes Oxley, and PCI. In other words, Unity Active Archive enables you to meet these stringent security standards...and exceed them.

By deploying Unity Active Archive you'll achieve these two major benefits:

- Unity Active Archive provides protection against unauthorized or accidental changes or deletions of your files, by people, viruses or ransomware that have escalated to superuser privileges or have compromised your Active Directory server in some way. Even when organizations supplement their conventional storage environments with a document management package or PACS archive, their security still ultimately relies on protecting the passwords of admins and authorized users—and by extension, the computers and BYOD devices they use - as most malware exploits attempt to gain superuser status.
- Because Unity Active Archive resists attempts by privileged accounts to change or modify files, it helps remove the temptation for authorized users to make unauthorized changes; those users will be unsuccessful and they will be caught. Any attempt to overwrite a file merely creates a new version. By default all versions are stored, but version-limiting options enable you to protect against DDoS attacks that attempt to consume all of your available storage space with unwanted and corrupt versions.
- Unity Active Archive includes auditing, integrity, and self-healing features that let you easily implement multi-decade retention times. It keeps two copies of each file in independently-protected object stores, and applies two cryptographic hashes (think of these as unique digital fingerprints of the file contents) that are separately stored in a hardened blockchain internal to the device. Additionally, Unity Active Archive issues a globally-unique consecutive serial number to each file so that it can be tracked throughout its lifetime. These techniques protect against bit rot, silent data corruption and software errors—invisible issues that can cause huge problems with your files.

Even if you're using modern hardware, your data can sometimes gets lost or corrupted. The important thing is to catch it immediately, report it, and fix it. Unity Active Archive's unique self-authenticating object replicator will not replicate corruption. Here's why: Approximately every 90 days, each Unity Active Archive node performs a thorough audit by checking serial numbers in sequence to ensure that all files are present, all match their previously stored hashes and all replication stores are exactly equal. This gives you positive assurance that all your files are there, and all are readable at all DR locations.

- A welcome side effect of Unity Active Archive's data authenticity and integrity features is that organizations are widely choosing to deploy Unity Active Archive for primary storage offload; that certainly makes sense, as it takes better care of files than the traditional server/backup paradigm.

When ransomware gets past your defenses, it obtains or generates a secret encryption key which is used to encrypt every file on your local device and any mounted (or possibly unmounted) network shares. Typically, those files are also renamed to something like "mydocument.doc.encrypted." But any of your files that have been protected by Unity Active Archive will remain safely untouched inside its archive.

Potentially new versions of files will start to be ingested by Unity Active Archive until the ransomware is detected and removed. Then recovery is extremely fast—Unity Active Archive gives you the option to use tiny shortcuts (sometimes called "stubs") that represent your undamaged files to restore them to your production servers. Unity Active Archive overwrites whatever garbage the ransomware has left on those servers, and does so at the rate of thousands of files per second. During the natural course of business, your most frequently-used files will re-inflate for faster access and the rest will remain as shortcuts. Unity Active Archive even gives you a unique, higher-performance option called "Virtual Shortcuts" which effectively requires zero time to recover files to your production servers.

Summing up, let's be clear: Unity Active Archive was architected from the beginning around the knowledge that attempts at corruption or deletion can come from anyone, anywhere and at any time. This includes from ransomware. That's why Unity Active Archive simply rejects every such attempt, regardless of whether it's from a virus, ransomware, spyware, user mistakes, software error - or a new threat that hasn't even been invented yet.

Nexsan 900 E. Hamilton Ave., Suite 230, Campbell, CA 95008 | 1.408.724.9809

=

HIGH-VALUE DATA
PROTECTION

IT'S YOUR MOVE

It's a simple fact that ransomware threats are getting more damaging and coming faster. If you diligently follow the preventive steps we discussed above you'll certainly cut the frequency of successful attacks, but the only true protection for your high-value data is to aggressively lock it down using a hardened storage solution like Nexsan Unity Active Archive. Considering the huge cost in time and money you'll face when dealing with a ransomware attack, we think deploying Unity Active Archive is the smartest move you can make.

ABOUT NEXSAN

Nexsan is a global leader in unified storage solutions that are focused on seamlessly and securely enabling a connected workforce. Its broad solution portfolio empowers enterprises to securely manage, protect and utilize valuable business data – while allowing users to sync, share and access files from any device, anywhere, anytime.

Nexsan 900 E. Hamilton Ave., Suite 230, Campbell, CA 95008 | 1.408.724.9809