Ontrack®

Ransomware Data Recovery for the Enterprise

August 2019

Executive Summary

Ransomware incursions have reached epidemic proportions. According to some surveys, as many as 28% of organizations were hit with a ransomware attack last year. And the consequences can be dire: From being locked out of enterprise data for weeks, to deletion of entire databases and loss of customer trust.

The FBI received 1,493 complaints about ransomware in 2018 with victims incurring losses of $3,621,857. But that only counts the actual ransom payments, not the fallout. The City of Atlanta, for example, spent about $2.6 million on its recovery efforts from a ransomware demand for about $52,000.

According to Symantec, enterprise ransomware attacks are rising at 12% per year. This is a big reason for renewed emphasis on comprehensive and up-to-date backups. Oftentimes, however, backup files are incomplete, neglected or in some cases, infected with the same ransomware that attacked primary systems.

> According to Symantec, enterprise ransomware attacks are rising at **12%** per year.

If backups fail to provide adequate recovery, further response mechanisms include data recovery techniques such as decryption tools, recovery of logical data directly from storage media and sending media to a lab where technicians attempt to extract as much information as possible.

Unfortunately, the ransomware epidemic has given rise to some questionable practices in the data recovery field. Some companies falsely claim they possess special technology to recover data. They charge a large fee. But all they are really doing is paying the ransom. A few have even been found to have secret relationships with cybercriminals. They work together to infect organizational systems and then profit by "solving" the problem. This can put the whole subject of data recovery in a bad light.

Fortunately, there are reputable companies available such as Ontrack that provide real solutions when files have been encrypted by ransomware. Such companies adhere to FBI guidelines to never pay a ransom and harness workable data recovery technology. Depending on the situation, they can recover most of the lost data.

As the leader in enterprise data recovery, Ontrack should be your first call if backup and decryption tools fail to deal with an ongoing ransomware incursion.

Ransomware Epidemic

Ransomware is a kind of malware that encrypts or otherwise locks users out of their files. When users try to access data, they receive a notice demanding the payment of a ransom in order to regain use of their data.

According to cybersecurity and backup firm Datto, ransomware costs businesses about $75 billion a year. This includes the ransom itself, subsequent recovery efforts, organizational and IT initiatives to protect the organization from further attacks, as well downtime, forensic investigation, training costs, restoration, and loss of revenue/productivity.

More conservative estimates by Cybersecurity Ventures placed ransomware damage at more than $8 billion in 2018, with it predicted to reach $11.5 billion by the end of 2019. That's a startling rise from a modest $325 million four years ago. To put it another way, a business is now being subject to a ransomware attack every 14 seconds.

Whether the figure is $75 billion or $8 billion, the devastation is very real to those experiencing ransomware. In May of 2019, for example, the City of Baltimore was shut out of government systems for more than a month. Vital systems for vaccine production, ATMs, airports, and hospitals were all impacted. Although the ransomware demand was $76,000, the recovery price tag amounted to nearly $20 million. Lake City, Colorado paid $460,000 and Riviera Beach, Florida, paid $600,0000 to regain system access. By all indications, ransom demands are increasing.

Remedies to the ransomware scourge include sophisticated decryption tools that can rapidly crack some of the encryption methods used by this form of malware. However, the number of ransomware variants multiplies fast.

A couple of years ago, the virulent strains of ransomware were Locky, CryptoLocker and TorrentLocker. Now it's SamSam, CrypoFortress and TeslaCrypt. In a couple of months, new strains will emerge. As a result, ransomware mitigation vendors struggle to keep up with the volume of new variants emerging.

To make matters worse, an underground economy has grown up to support cybercriminals. Ransomware developers provide tech support and offer the latest ransomware over the Dark Web in exchange for a cut of the loot. This goes as far as Ransomware-as-a-Service (RaaS) that enables criminals to steal usernames and passwords without possessing sophisticated technical knowledge.

No wonder ransomware is on the rise. The United States FBI received 1,493 complaints about ransomware in 2018 with victims incurring losses of $3,621,857. That number, however, only takes into account the actual ransom payments, not the repercussions of the attack, the lost revenue or the PR fallout. Globally, the total number is much higher.

The enterprise sector, in particular, is under threat. The FBI, the U.S. Secret Service, and other law enforcement agencies have been warning U.S. firms for years that their computer files are being targeted by cyber spies and cyber thieves from countries such as China and Russia. The perpetrators behind the attacks are seeking information about mergers, patents, trade secrets, financial details and business plans.

One of the agonizing aspects of this problem is that it is typically brought about by gullible employees. Phishing emails continue to be effective in luring personnel into opening malicious attachments or websites. This weakness enables cyber criminals to gain credentials and either steal funds or initiate a ransomware infection.

The FBI received **1,493** complaints about ransomware in 2018 with victims incurring losses of $3,621,857.

Ransomware Prevention and Mitigation

Due to continued success of phishing, user training is very much a front-line defense against ransomware. Standard IT security practices and technologies such as anti-virus, anti-malware, intrusion detection/prevention, firewalls, network monitoring, and access controls must also be in place. Ports that do not need internet access should be closed, and those that do should be carefully watched and protected.

More recently, machine learning and heuristics programs have appeared on the market that can scan for ransomware behavior such as encryption by unauthorized programs. Backed up by threat intelligence and other safeguards, a vigilant IT department can limit the possibility of incursion.

In addition, further layers of protection must be in place such as regular backups. These backups must be comprehensive, must be easily recoverable and must be tested to verify accuracy. But ransomware constantly evolves and finds new ways to infect systems. Sometimes it attacks specific systems or databases. The malware often begins by using stolen administrator rights to disable online backups, especially on SANs. Then, the malware will delete NAS systems. At other times, it manages to infiltrate and encrypt backup files, too. Virtualized backup applications such as Veeam, for example, have been targeted as part of ransomware attacks. It isn't a case, then, of if it will strike, but when. Organizations need to be prepared. Tapes that remain in a tape library system have the potential to be overwritten, encrypted or otherwise corrupted by ransomware. Air gap backups eliminate the possibility of further infection, if the original backup was free from malware.

Certain best practices have evolved, detailing actions to initiate if ransomware strikes. A major principle is never to pay the ransom. The FBI is a firm advocate of non-payment. And the U.S. Conference of Mayors had all its members pledge to never pay a ransom to cybercriminals.

After all, those who satisfy ransom demands have no guarantee that their files will be decrypted. They may be extorted for more money, or they may find their files and systems now riddled with other types of malware.

Along with not paying the ransom, victims should immediately contact law enforcement. Impacted systems should be immediately shut down and disconnected from the network. Critical disks should be cloned before making any changes. No time should be lost once an attack is detected. Otherwise, the infection could spread to more users, systems and applications.

In addition, programs have been developed which decrypt certain strains of ransomware. IT personnel should contact providers or law enforcement to see if their infection can easily be decrypted. These days, there are over 100 decryption tools that can be used against more than 400 ransomware variants. Case in point: the FBI released the master decryption keys for the GandCrab ransomware to enable victims to decrypt files infected by GandCrab. Note, however, that cybercriminals endeavor to stay one step ahead. When one strain can be effectively decrypted, they begin developing an altered strain to make it unencryptable.

Once an infection is contained, backups are traditionally the best way to recover data.

Once an infection is contained, backups are traditionally the best way to recover data. Adequate backup files, whether from the cloud, backup applications or tape, permit the organization to get up and running rapidly. But care should be taken with backup files to ensure they were not subject to infection. Restoring files that contain ransomware will just lead to reinfection of IT systems. Further, backups are notorious for either being incomplete, out of date or even corrupted. In those cases, the best option is to contact a global data recovery provider with a proven record of recovery.

Recovery Options Beyond Backup

Even if decryption efforts fail and backups are missing or incomplete, data recovery may be possible depending on the type of storage and the kind of ransomware. Enterprise storage support may be available from copy-on-write systems such as NetApp WAFL or Oracle ZFS. Some of these systems allow a recovery engineer to walk back in time through the various copies available until they can find an unencrypted version.

That approach will enable the organization to restore their data, but some data loss is inevitable – if the uninfected copy is two weeks old, two weeks of data will potentially be lost. Early detection and intervention, therefore, is critical so that the ransomware encryption affects as few copies as possible, The more recent the recovery point, the better.

Further, there are a variety of techniques available that can recover data from hard drives, secondary storage, solid state drives, removable and other media. It is possible to use these techniques to restore deleted, inaccessible, corrupted, damaged or reformatted data when other methods have failed.

Software-based tools are the simplest approach. These can be used onsite or remotely to recover files that would otherwise be lost. Software recovery tools help resolve logical data loss issues such as accidental deletion and deleted partitions. Files can also be recovered from the recycle bin, from volume shadow copies and raw data recovery can be done using signature search.

If this doesn't resolve the issue, it is time to resort to in-lab data recovery. Even if the files are damaged, corrupted or partially encrypted, a reputable lab can have success in retrieving data. Failed drives can be examined to see what data can be extracted, whether due to physical or logical failures. Whether it's operating system upgrade failures, poor quality soldering, faulty components, manufacturer defects, as well as a range of damage scenarios due to disasters, drops, breaks, water, fire or power surges, in-lab services often do well in recovering data users thought might be gone forever. Even physical or mechanical failures such as head crashes, firmware failures and bad sectors can be resolved in the lab with a fair degree of success.

Be aware, however, that there are a few data recovery scams out there. You can generally tell them apart by the lavish promises of recovery. If they guarantee close to 100% data recovery, beware. Some of them pretend to have the secret sauce that will instantly unlock decrypted systems. What they actually do is pay the ransom and charge a hefty markup fee. A few are even colluding with the cybercriminals. Due diligence, then, is essential when selecting a firm to be trusted with enterprise data recovery.

The top data recovery labs have a deep understanding of virtualization, storage systems and on disk data structures. They can rebuild the RAID, file systems and block level data. In many cases, top labs can recover a surprisingly large quantity of information that was otherwise thought to be gone forever.

Ontrack Ransomware Data Recovery Services

Ontrack is the established market leader in data recovery. With a global presence that spans Europe, North America and APAC, Ontrack can recover data from virtually any physical media (HDD, SSD, tape, smart phone, RAID, SAN, server or Oracle and SQL database), as well as logical data loss and deleted files. Backed up by a suite of proprietary recovery tools and an experienced data recovery team, Ontrack has vast experience in dealing with data loss scenarios ranging from routine to extreme. This includes accidental deletion, media corruption, fire and water damage, dropped media, and more – onsite or remotely.

Over the years, Ontrack has developed partnerships with all major storage and media OEMs. This provides the company with in-depth knowledge of every type of file system, storage platform, media and firmware to be able to find whatever data may be recoverable and piece it all together.

Ontrack follows strict IT security protocols and is audited every year. Staff undergo background checks prior to being hired and facilities are secured with cameras and secured entryways based on SAS70 certification. Ontrack laboratories and data recovery staff are supported by a team of 200 R&D engineers. We have developed over 500 proprietary software and hardware tools for data recovery. With proprietary imaging software, for example, a drive can be imaged from the back to the front or from any point while avoiding damaged areas on platters. This process preserves the original drive while increasing the amount of data that can be recovered. In the case of RAID and SANs, engineers can image each drive and rebuild the RAID or striping of data to recover the data.

Media and devices can either be sent to the lab or On-Site Services Data Recovery can be performed at the user's location for the most critical and sensitive logical data loss situations. Remote recovery using advanced software recovery tools is another option.

A multinational Swiss chemical corporation experienced a ransomware attack that took over a NetApp system using administrator privileges obtained through phishing. The ransomware formatted all HDDs for 30% and created a new aggregate. Ontrack was able to rebuild the RAID, file system and restore the data for the customer.

Summary

Early detection and immediate action are the keys to mitigating the impact of ransomware. If ransomware gets through a network perimeter and a full backup is not available, data recovery may still be possible. Each scenario requires a different approach for data recovery. But only global vendors with a proven track record with enterprise systems should be trusted with recovery from ransomware attacks. Ontrack has extensive experience in recovering data from all major storage platforms and media. As a point of firm policy, Ontrack never pays ransoms. Instead, it endeavors to recover all possible data using advanced techniques. Ontrack has all the in-house expertise, facilities and tools required for comprehensive enterprise data recovery.

For more information visit www.ontrack.com or call 1-800-872-2599.