SmarTone

White Paper

Version 1.0

The Rise of Ransomware : Will you be the next target ?

Table of Contents

1 Background

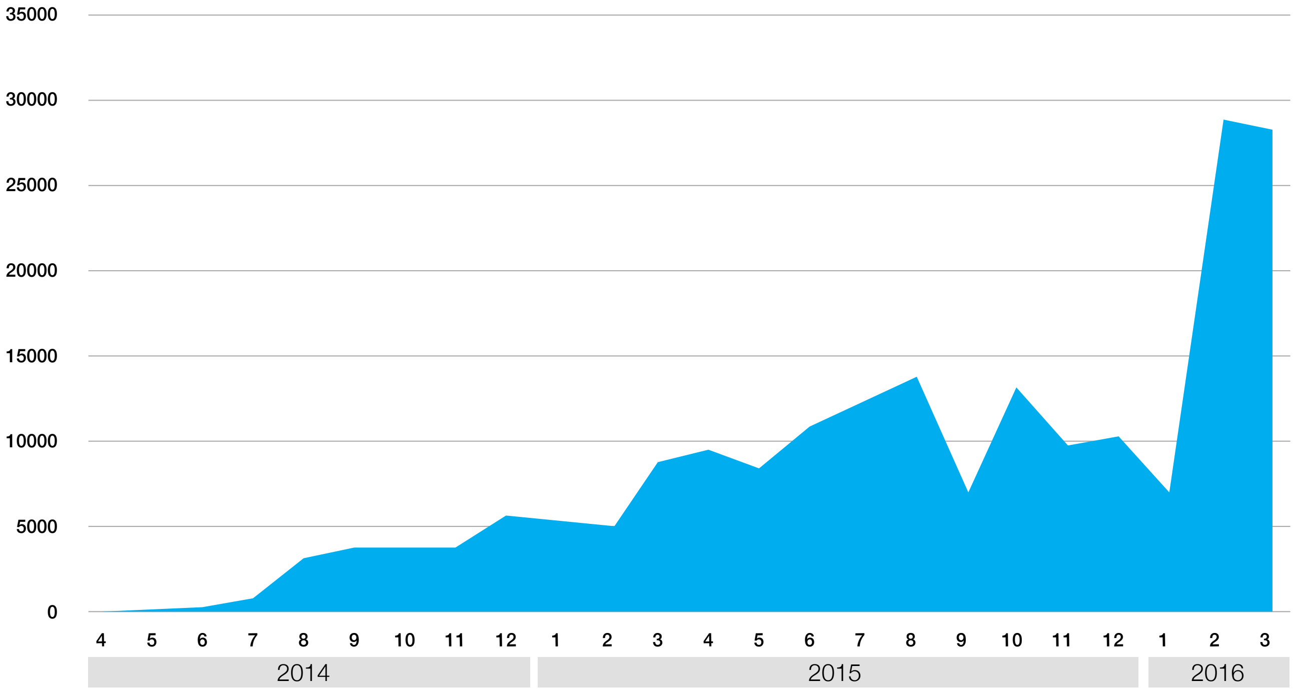
Ransomware is a type of malware that encrypts the victim's files without any consent, then demands a ransom in exchange for the decryption keys. This malware is aimed at making money from the victims. It is the most evil type of malware today as it can hardly be detected by traditional anti-virus programs. The white paper will explain what ransomware is, how it affects us, and solution available for us to ensure our data asset is under protection in the event of an infection.

In recent months, there have been a few high profile cases due to ransomware attack. For example in UK, Lincolnshire Country Council's computer systems were closed for four days in January 2016 after being hit by ransomware demanding a £1m ransom. Beside governmental department, healthcare industry is another target for attackers. In February 2016, a hospital in Los Angeles was attacked with $17,000 USD in Bitcoin demanded as ransom.

Ransomware is on a rising trend. Computer Security company Kaspersky Lab reported that the total number of users who encountered ransomware over the 12-month period from April 2015 to March 2016 grew by 17.7% in comparison to previous year: April 2014 to March 2015 – from 1,967,784 to 2,315,931 users around the world (Source: KSN Report: Ransomware in 2014 – 2016).

In Hong Kong, according to the statistics of the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), there were 172 ransomware incident reports in the first five months of 2016. The number is increasing, with a new monthly-high of 59 incidents of ransomware attacks in May 2016. Most of the victims were local home users, educational organizations and SMEs.

There are more than 50 ransomware families today, and with each composed of multiple variants. Ransomware not only appears in desktop computers, but also in mobile devices. The number of users attacked with mobile ransomware grew almost 4 times: from 35,413 users in 2014-2015 to 136,532 users in 2015-2016.



The number of users encountering mobile ransomware at least once in the period April 2014 to March 2016 (Source: KSN Report: Ransomware in 2014 – 2016)

Why there is a significant growth in ransomware? The answer is simple. Attackers could get good profit from creating and spreading it. According to CNN Money, cyber-criminals collected $209 million USD in the first three months of 2016 by extorting businesses and institutions to unlock computer servers. At that rate, ransomware is on pace to be a $1 billion a year crime by end of 2016!

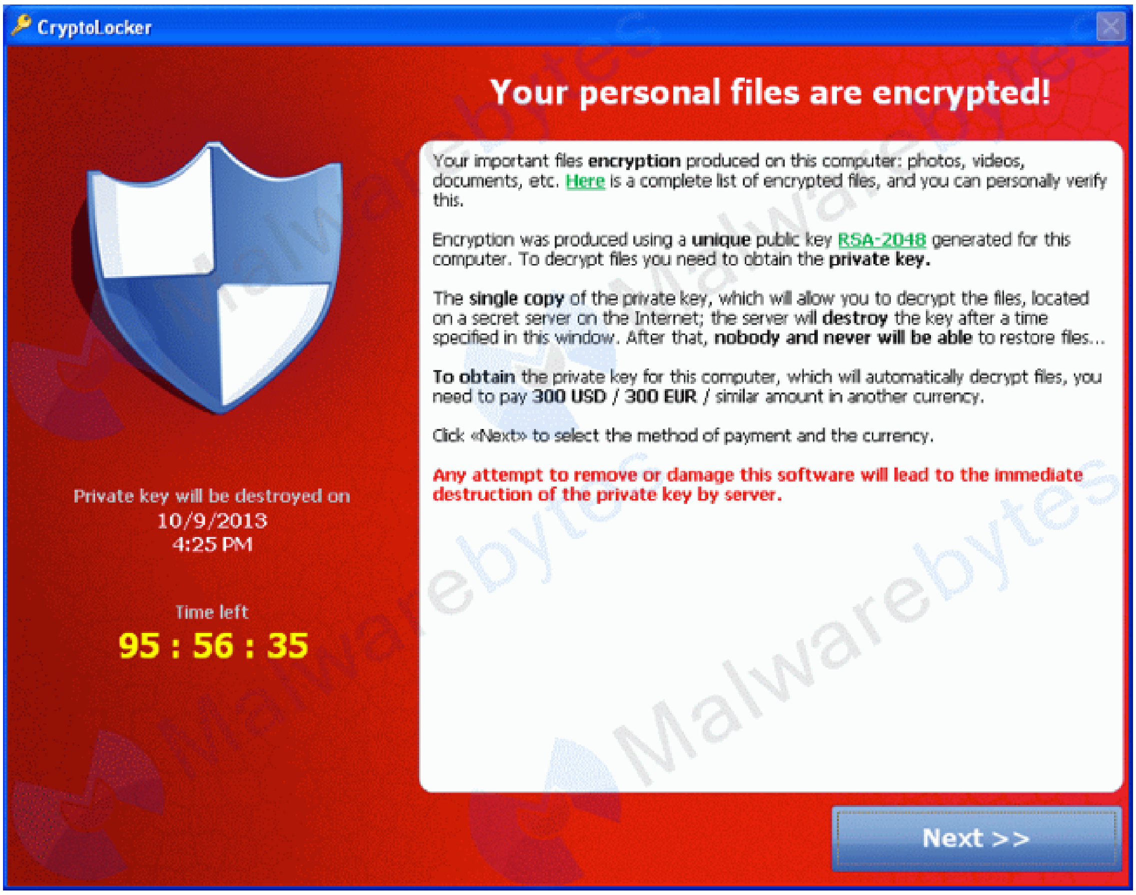
Although ransomware has been around for many years, it has risen dramatically over the last few years mainly due to the popularity of use in Bitcoin. Bitcoin is a digital currency that can be used to purchase things in the Internet world. Unlike conventional money, Bitcoin is not controlled by one central authority and it is totally anonymous. User can hold a bitcoin address which is not linked to a name or a physical address or other personally identifying information. Therefore, it is very difficult to trace for the source. Cyber criminals make use of Bitcoin to easily escape from legal liabilities. Nevertheless, buying Bitcoin is not as straight forward as you purchase something online with your credit card. Most people are unfamiliar with its buying process. Ransomware attackers try to make the payment process simple for victims by introducing some 3rd party stored-value card providers, like MoneyPak or Reloadit. Attackers first instruct victims to purchase a MoneyPak card (with any amount from $20 to $500 USD) with cash at a convenience store. Each MoneyPak card has a unique PIN code printed at the back. Attackers then request victims to give them the PIN code. With the PIN code, attackers can unlock the cards and exchange the money stored on the card to Bitcoin via some online trading platforms that offer a way for people to buy and sell Bitcoins with MoneyPak. Therefore, attackers can easily receive the demanded ransom from victims without leaving any trail while keeping the payment process simple to the victims.

Moreover, the emergence of Ransomware-as-a-Service (RaaS) model is a catalyst in making such growth. RaaS enables affiliates to obtain a piece of ransomware from the author and distribute it to victims. If the victim pays the ransom, the author would do a revenue sharing with the affiliate. Therefore, RaaS would let anyone without any knowledge of malware become a cybercriminal.

2 About Ransomware

Ransomware is typically delivered via infected attachments or web links in phishing email, or fake software update such as Adobe Acrobat or Java. After the ransomware is installed on victim's computer, the malware will start to encrypt files it can find on the machine itself with an encryption key. Files located in any mapped network drives or USB devices attached with the computer may also be encrypted. Once the process is completed, the files become inaccessible. The malware will place a pop-up screen like below with instruction for victim to pay in order to restore the files back.

Example of a typical ransomware pop-up message with time remaining of due payment



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

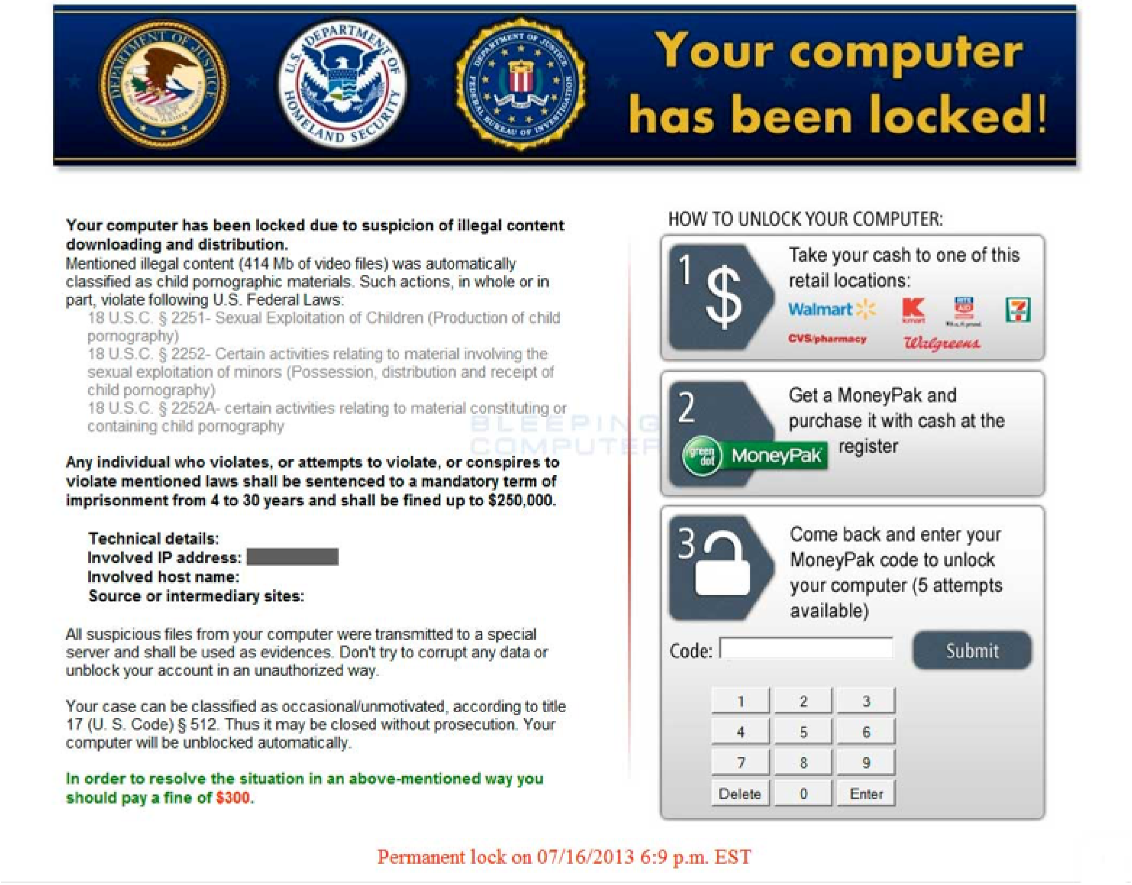
Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

The ransoms are typically a few hundred US dollars to one thousand, and you are often required to pay in Bitcoin. The pop-up message tells you if you do pay, you will get the decryption key to restore your files. The key is stored in the attacker's system. If you do not pay within a set deadline, the ransom may get doubled afterwards. If you still do not pay, the decryption key will be destroyed, and your files will be completely unrecoverable.

If you try to decrypt the infected files by yourself, it would be impossible as the key was generated by RSA-2048 encryption mechanism. This means in order to decrypt it on an average desktop computer, it would take million to trillion of years.

Few most recent variants of ransomware locks the computer display and does not allow the user to access any programs until the ransom is paid. The computer displays a pop-up message that claimed to be from the law enforcement. The message typically is about viewing some illicit materials, like child pornography. You need to pay a fine; otherwise, you will be arrested after the deadline of payment. An example with instructions on how to pay ransom in MoneyPak is showed below.



Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name:
Source or intermediary sites:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

Permanent lock on 07/16/2013 6:9 p.m. EST

Many individuals do pay up either because they would think it might be worth to pay in order to get their important files back or they believe the accrued message is true and become scared. We can see the attackers use some kind of psychological method to trick you and pressurize you in paying. If a victim really pays the ransom, this would give more incentive for the attacker to keep doing the ransomware business. Unfortunately, even if the user does pay the ransom, the attacker might often does not give you the decryption key. There is no way to stop the attacker to demand more money from you. Even worst, once you pay the ransom, you are helping to building up an ecosystem for the ransomware community. Your information which indicated "You are the person is willing to pay" will be placed in the marketplace for cyber criminals. You will have high chance to be attacked again by another ransomware or other malware in the future.

3 Solutions

Ransomware can be difficult to defeat. Prevention is the best cure. Here are a few advices to help you to protect from ransomware attack.

3.1 Avoid clicking on suspicious files

Since ransomware is transmitted via phishing email or advertisement on websites, you are strongly advised to avoid clicking on such advertisements, or to add Ad blocking tools to your system. You always need to think carefully before opening an email attachment or files from unknown sources. Ransomware often has hidden file extension (e.g. ".pdf.exe"). To easily identify suspicious files, you should enable your operating system to show hidden file extensions.

3.2 Frequently update your operating systems & applications

Software vendors release security patches on a regular basis. However, people are often running outdated software that has known vulnerabilities. It is a good practice to frequently update your operating system and applications to decrease the risk being attacked by ransomware, or any other malwares in general. If you can, enable automatic updates, or proactively visit software vendor's website to check for security updates.

3.3 Install a reputable anti-malware software

It is advised to always install an anti-malware software to help you detect malicious threats or suspicious behavior. However, for those newer ransomware variants that might not be detected by your anti-malware software, you may need to add a firewall protection to monitor the suspicious network traffic. It is because most malware relies on remote instructions by connecting with its Command and Control (C&C) server to receive instructions for encryption files.

3.4 Backup your data with versioning

All the above tips are only for prevention. You should always need to prepare the worst to come. What if my computer is compromised, how can I well prepare in advance? There is only one thing you can do is to backup all your files regularly in a way that would allow you to restore the files if your computer get inflected.

If you just backup your files to a hard drive that mapped to your computer for an easy access, this might not be a safe solution. Since the ransomware virus is so smart to go to all mapped drives to encrypt all the files, or even delete them. You might think of disconnecting the backup drive when you are not actually making a backup, then you have to remember to re-attach the drive in order to back up. The problem is that the backup is no longer automated. Thus, a local backup is not an appropriate solution, rather you may choose an online or remote backup solution.

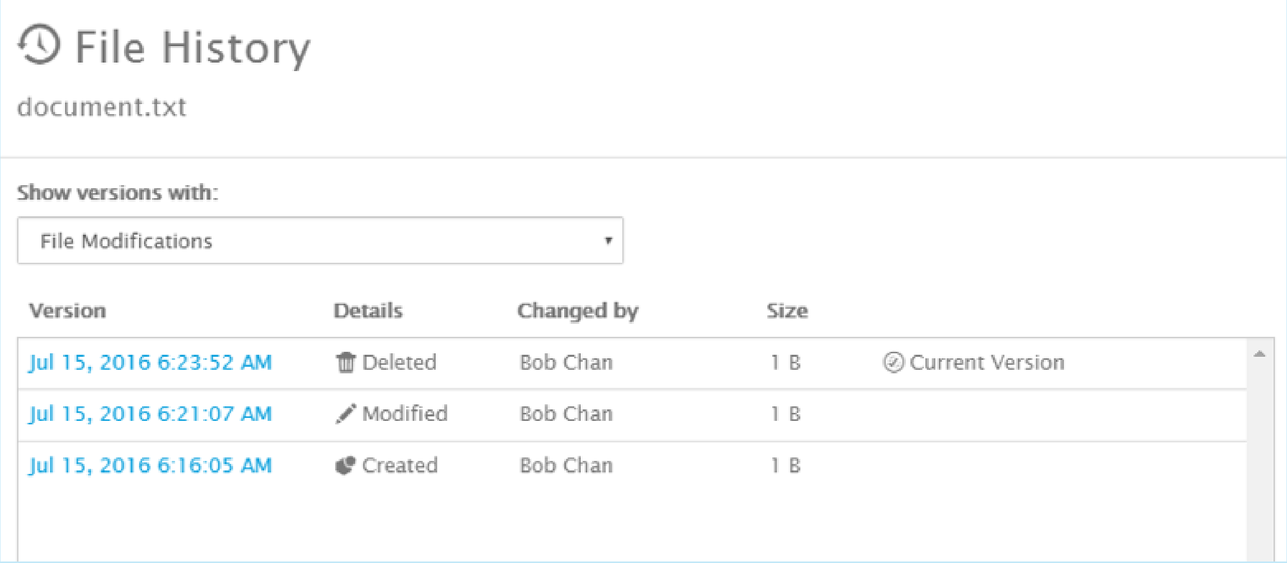
Most companies would normally backup their data in a daily basis, or in a more frequent schedule like once every 4 hours. However, this is not a 100% protection from ransomware attack. For example, say you are making some critical updates to a file; it is possible that your file could get encrypted or deleted by ransomware before the next backup job is run. You can only restore the last version from the backup storage, but without your latest updates. Thus, a periodic backup solution cannot fully address the problem created by a ransomware attack.

An alternative way is to adopt a solution that supports instant backup. Some instant backup solutions actually mirror files on one of your drives. However, this might not be a safe solution as the files will also get mirrored once they have been encrypted by ransomware. Your previously unencrypted backups will also be overwritten.

What you really need is an instant backup solution that supports versioning. Whenever a file is modified, a copy of the existing file stored in the backup storage is instantly and automatically created, with a version attached with it.

SmarTone Cloud backup solution

As part of the SmarTone Cloud backup solution portfolios, our Secure File Sync and Share (SFSS) solution supports instant backup with versioning. Your files on a local drive of your desktop are mirrored with one of a storage nodes in the SmarTone Cloud. Whenever a file is modified or even deleted, this file will get instantly synced to the cloud storage while a copy of the existing file already stored in the cloud will be created and be versioned. You can select which particular version to restore when needed. Versioning can also protect you from accidentally delete a backup file. Since SFSS automatically backups a version of your file every time you make an update; in case of a ransomware attack, you can always find a version of your file before it was encrypted/deleted.


File History

document.txt

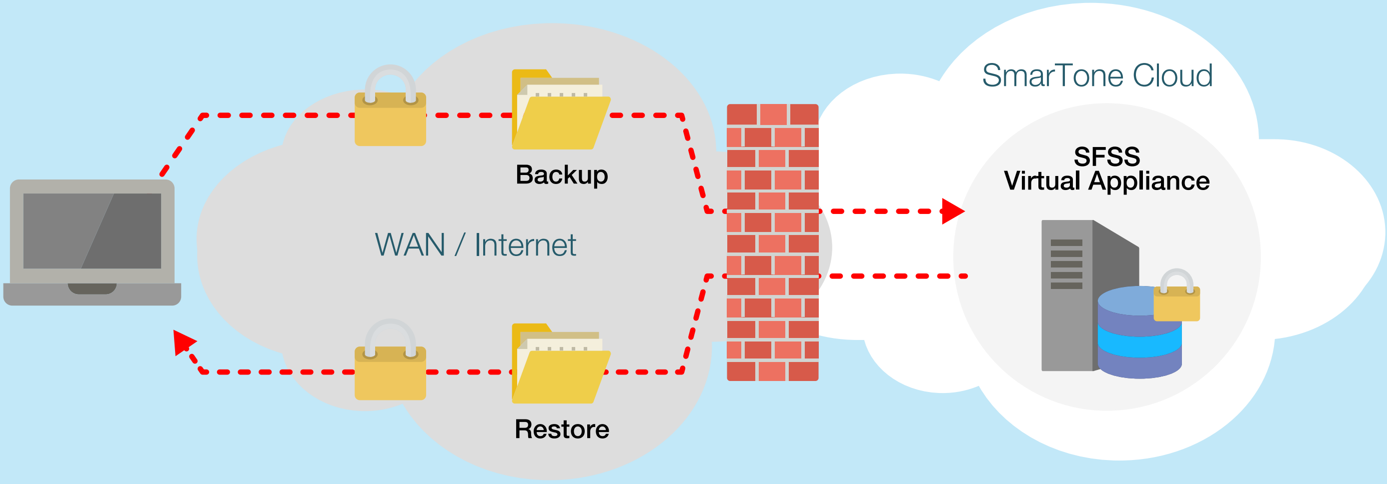
Show versions with:

File Modifications ▾

Version	Details	Changed by	Size	
Jul 15, 2016 6:23:52 AM	Deleted	Bob Chan	1 B	Current Version
Jul 15, 2016 6:21:07 AM	Modified	Bob Chan	1 B	
Jul 15, 2016 6:16:05 AM	Created	Bob Chan	1 B	

In the above example, I have a file called “document.txt” created and stored in my local mirrored drive with the cloud storage. After I modified this file, a backup copy of the original file is created and versioned. In case my “document.txt” on my local drive get deleted by a ransomware, I can still be able to find and restore a deleted version from the cloud storage.

You may probably be concerned about the data security and availability issues when moving your files to the cloud. Our SmarTone cloud infrastructure runs on solutions provided by Hitachi Data Systems (HDS) which has a worldwide leading position in enterprise-grade storage. Running in a Tier 3+ data center and with ISO 27001 ISMS certified, our cloud infrastructure can ensure your data is highly secured and well managed. To further strengthen the security level of our cloud, we have solutions like Next Generation firewall, Intrusion Prevention System (IPS) facilities, and 2 Factor Authentication. Through the use of our cloud platform, we ensure your get the highest availability and protection of your critical data.



You may ask if ransomware attacker would find way to destroy my backup files stored in the cloud. In order to strengthen the protection level of your data, our backup solution does not allow user to directly delete backup files from the cloud storage. Deletion can only be done by changing the backup policy (e.g. retention period, number of version allowed) via admin mode. Provided that you encounter a ransomware attack, the attacker must know the backup solution you are using and the admin credentials of the SFSS system, and be able to change the cloud backup policy behind it. With our high secure cloud infrastructure, the attacker can hardly be successful.

If you wanted your data to be more insured, you may consider to do a regular periodic backup in additional to SFSS. You may choose our cloud backup solution that supports backup of Windows and Linux server running on either physical server or virtual machine, application backup (e.g. MS SQL Server, Exchange, Active Directory), as well as desktop PC client backup.

You may be worried about performance issue when using cloud-based backup solution. The upload speed and restore time could be slow. You may adopt our cloud gateway solution. The cloud gateway is an on-premise appliance which can be simply treated as a local file server with both caching and cloud backup capabilities. Frequently used files, so called “hot data”, are always cached in the cloud gateway so that file access performance can be guaranteed. All data will automatically backed up to the SmarTone Cloud according to the backup policy configured on the cloud gateway. The shortest backup interval can be down to every 15 minutes. You might be wondered the required cloud storage would be growing very fast if backup is done so frequently. It is actually not the case. If there is no change on a file, only one copy of file content is stored in the cloud. A file shortcut, or called “stub”, is created in the cloud gateway that points to the file located in the cloud storage.

4 Conclusion

The growth of ransomware inflection is inevitable. It causes enterprises to loss of sensitive or proprietary information permanently. Disruption to both business activities and corporate reputation are so devastating. It becomes so costly to recover such loss. Making regular backup of your data is the only way to protect your data once you encounter a ransomware attack.

However not all cloud backup solutions are safe. Some solutions do not prevent the risk from deleting cloud-based backup files by ransomware. It is important to choose the right cloud solution provider. Running under a highly secured cloud infrastructure, SmarTone Cloud backup solution provides a complete data protection for your enterprise from ransomware attack.

Contact us

For more information, please contact your Account Manager

☎ 2281 8818
✉ business_markets@smartone.com
www.smartone.com/en/business_site/

SmarTone