WHITE PAPER

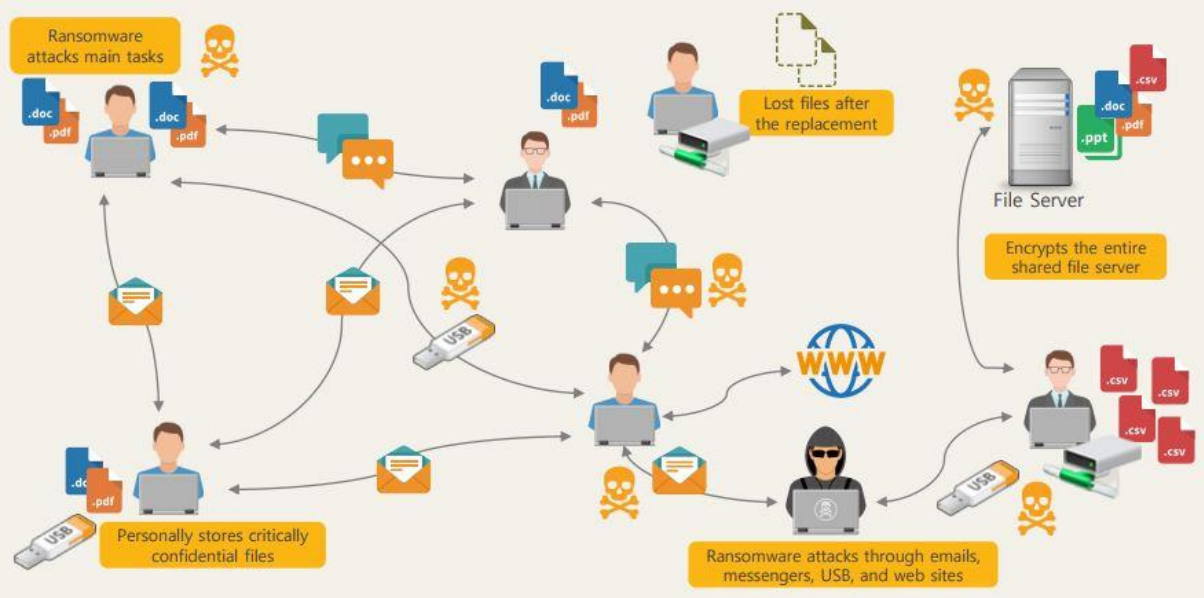
WHAT IS A RANSOMWARE PREVENTION FILE SERVER
AND HOW DOES IT PREVENT RANSOMWARE 100%?

VERSION: 1.2
Dated: Sep 15, 2017

Prepared by:
John Woo
Kevin Kim
www.filingcloud.com

1. What is ransomware?

Ransomware is a new type of hacking method that encrypts the files within an infected PC and demands a “ransom” of money for their recovery. More than 250 countries around the globe are experiencing the harmful spread of ransomware on a daily basis. Hospitals and corporations especially, where data is practically synonymous with survival itself, are being targeted.



2. Understanding the existing methods for preventing ransomware attacks and their limitations

The most well-known methods of preventing ransomware attacks is by either installing a vaccine software (which is known as an endpoint protection method) or backing up your PC’s data. Vaccine software and pattern detection-based anti-virus software are both only good for detecting attacks from existing ransomware and malicious codes. The fatal problem with this method however, is the fact that once a new version of ransomware is present in the system, no existing vaccine software or endpoint protection in the world can prevent it from encrypting the PC’s data and files, since they can only detect existing malware with familiar patterns.

Another precautionary measure is data backup. Basically, the user prepares for the worst case scenario (in this case, the encryption of one’s data due to an inevitable breach of ransomware) by constantly backing up one’s files and restoring them onto the PC or server after an attack. However, backup restoration is NOT a preventive technology, but rather, a mere recovery. If an attack occurs, interruption of business is inevitable, and even after a backup restoration, data loss between backups and operations is bound to occur. You need 100% guaranteed preventive technology to prepare for such an attack, not an incomplete form of recovery.

3. FilingBox, a file server 100% guaranteed to prevent ransomware attacks

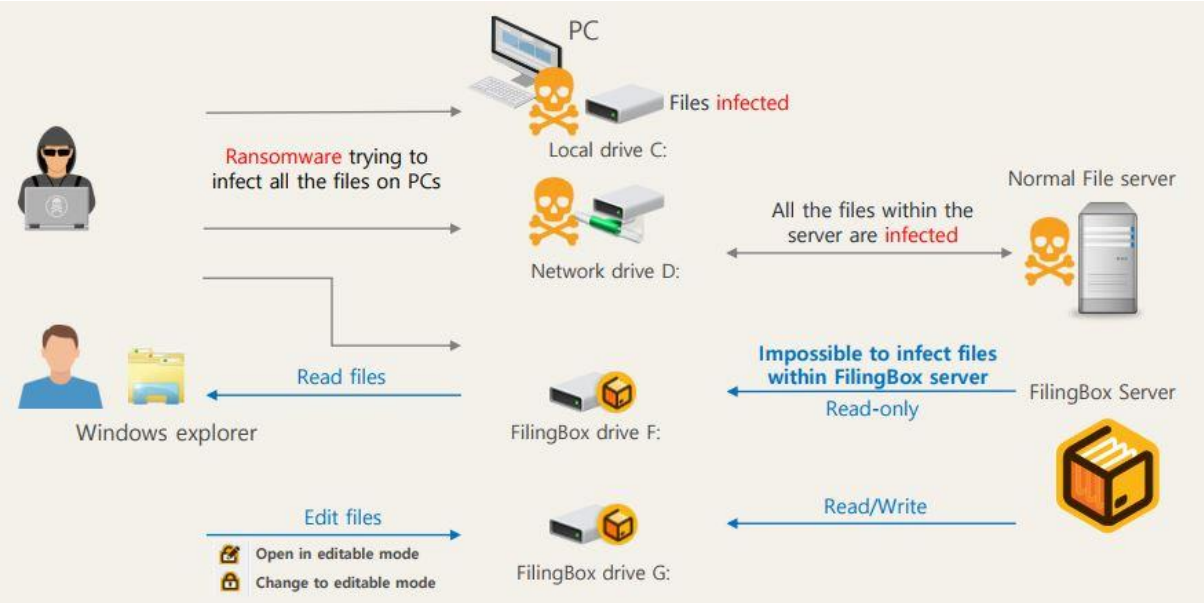
While FilingBox will require an installation onto a server apart from the PC due to it being a file server, the stored data within the file server however will be 100% safe from ransomware attacks originating from within the PC.

The reason FilingBox can guarantee data safety with such confidence is because it is equipped with the technology to check the program on the PC that is attempting to interact with the files within the file server, and only allows the program(s) that is known and trusted as a work program.

Existing Windows or Linux file servers only checks the user of the connected PC, and does not check whether or not the program attempting to interact with the stored files is legitimate. Through this vulnerability, all data within the file server will inevitably be encrypted in the event of a ransomware attack.

Basically, FilingBox itself takes absolute charge of approving the programs and only allows trusted work programs to interact with your critical files, and doesn't leave that responsibility to the connected PC, leaving no room for vulnerabilities or security breaches.

Another interesting aspect of FilingBox that differentiates itself from its competition, is the fact that it only allows interactions between files and legitimate programs on the PC through a whitelist method; whereas other existing solutions limits their security through a blacklist method that can only filter out and prevent existing malwares through familiar pattern detection, which obviously cannot detect nor prevent attacks from new versions of ransomware with never before seen patterns and actions.



We can confidently say that FilingBox is the only technology on the market that can prevent ransomware 100%, with a patent pending on the global scale including the US. FilingBox has recently been awarded the top grade GS certification by the Software Testing & Certification Laboratory, and it has received favorable reviews from major organizations and agencies such as Nonghyup Investment & Securities, Kookmin Card and the Police Department within the last year.

4. The difference between whitelist-based program access control when running on a PC and on a ransomware prevention file server

Among the endpoint protection technologies installed on the PC, there is a white list-based prevention method that permits access only to programs specified in a specific folder or drive, rather than a blacklist method that blocks malicious programs from running.

Ransomware will not be able to access the folder or drive because it can only access the folder or drive that you specified in advance, but it will not be able to prevent ransomware attacks in the end.

Ransomware includes a Full Disk Encryption (FDE) attack that encrypts the file system under the Windows operating system at the drive level, so that even if you control a program accessing a specific folder from the top of the OS, you cannot stop the attack.

Also, in order to prevent FDE attacks, all normal programs running on the PC are registered on the whitelist. However, whenever a large number of programs are newly upgraded or added, the user or the administrator has to register the programs in the whitelist each time. The frequency of occurrence is too frequent to prevent ransomware.

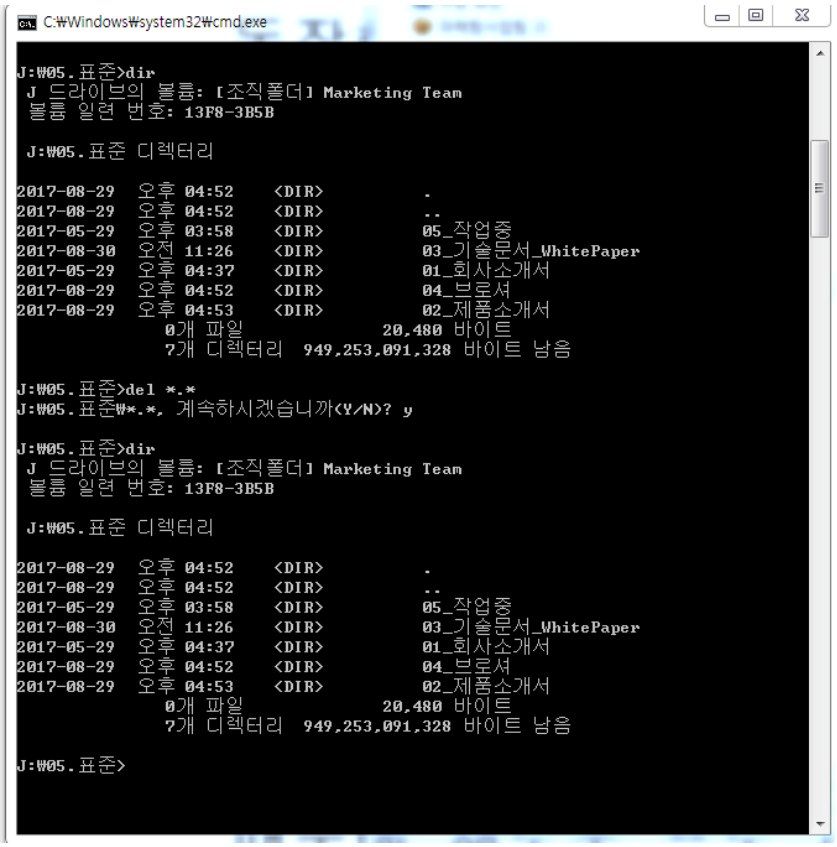
For example, if you want to work with a specific program on a PC but it is not a whitelist target program, if it is intercepted, you have to find an administrator so that you can run it. It becomes a pesky situation of giving up management of the whitelist program list.

Therefore, it is more difficult for a PC to check whether a program accessing a file is a legitimate program. However, the situation is 100% different if it is an anti-malware file server, not a PC, where the program is checked and verified on whether or not it is legitimate for file access.

Ransomware protection for PC data protection file servers are 100% protected against any kind of ransomware attacks without the hassle of setting up white programs for users or administrators.

A ransomware prevention file server provides files with read-only properties for accessing files of all other programs running on PC, in addition to file browsing by the PC's Windows Explorer.

For example, it is possible to delete a file by Windows Explorer on a network drive connected to a ransomware prevention file server. When a file is deleted using a DOS command, the file server accepts the delete command. However, since the DOS command is not a program designated in advance, it does not delete the files. In addition, the ransomware prevention file server does not support file format or encryption attacks at the drive level, such as FDE. (In fact, attempting to format the drive associated with the ransomware prevention file server will stop the PC from functioning.)



Therefore, no matter what type of firmware the PC runs on, the files in the ransomware prevention file server are safe.

Also, from the management side of the whitelist, it is necessary to set all the programs to be executed when comparing the list on the PC, but the ransomware prevention file server allows only the file access by Window Explorer, so you do not need a separate setup every time a new program is added.

Technically, when you open a file in a network drive that is associated with a ransomware prevention file server in a particular program, the file is provided as read-only. (Of course, even if the file was opened as read-only, the user can always save the document under a new name.)

However, if you need to directly edit the files in the ransomware prevention file server, you

can edit and save the documents directly by opening the edit window provided in Windows Explorer.

In addition, whenever the document is opened through edit mode, the ransomware prevention file server automatically creates a new version of the document.

Therefore, if white list based data access management is performed on the ransomware prevention file server rather than on the PC, it is possible to prepare against all kinds of ransomware attacks and a major advantage is that users and administrators do not have to frequently update the whitelist.

5. FilingBox Demo

FilingBox Demo:
https://www.youtube.com/watch?v=m7jva0N8HZ4&list=PLtQ3XkjWXMf4KmKj07k_kj-jSqBSi_0vN

FilingBox Introduction:
https://www.youtube.com/watch?v=KtrW3oU7fk4&list=PLtQ3XkjWXMf7u8-2UoHe7xXb5NEhGaRvi

Homepage: http://www.filingcloud.com

For more information, contact:

- **ByungJae Kim**
  Boston Office
  kbyungjae@mdainus.com
  Framingham, MA, USA

- **John Woo**
  CEO
  jhwoo@filingcloud.com
  Seoul, Korea

- **Kevin Kim**
  Marketing
  kevin@filingcloud.com
  Seoul, Korea