Acronis Active Protection™

Protect Data Against Loss to Ransomware

Constant Data Availability in a Changing Threat Landscape

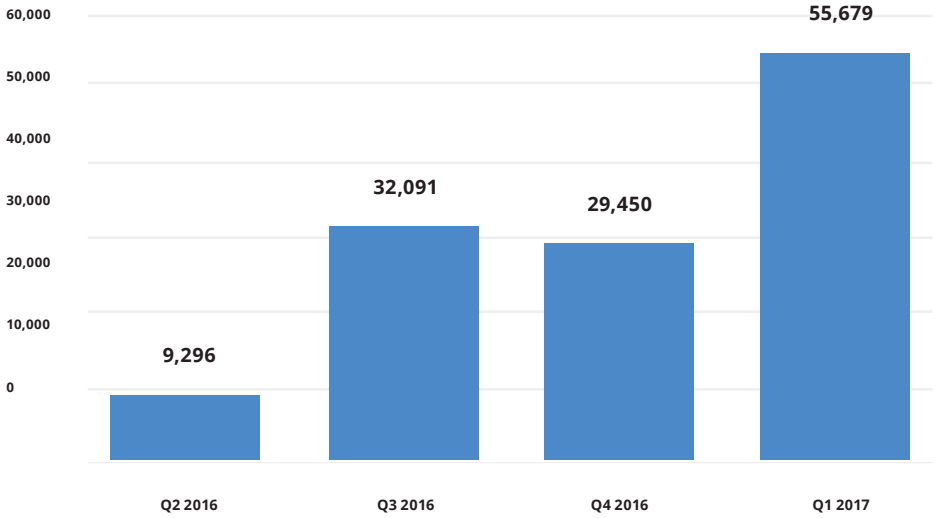
According to Osterman Research, 47 percent of companies have been attacked by ransomware and we can bet that the May 2017 "WannaCry" attacks across the globe have increased that number. Unfortunately, this is only the beginning for ransomware attacks, but not everyone understands the implications of this type of malware.

What is Ransomware?

Ransomware is a type of malware that blocks access to some or all information that is stored on a device. In order to unlock the device or the data, the user is required to pay a ransom, usually in widely used e-currency.

The term ransomware covers two types of malware: so-called Windows® blockers, which block the operating system or browser with a pop-up window, and encryption ransomware. Some Trojan Downloaders are also considered ransomware, namely those that download encryption ransomware upon infection of a machine.

Ransomware attacks have been growing at alarming rates as you can see in the tables below. Unfortunately, industry experts, including the FBI, predict that the number of ransomware attacks will continue to increase exponentially.



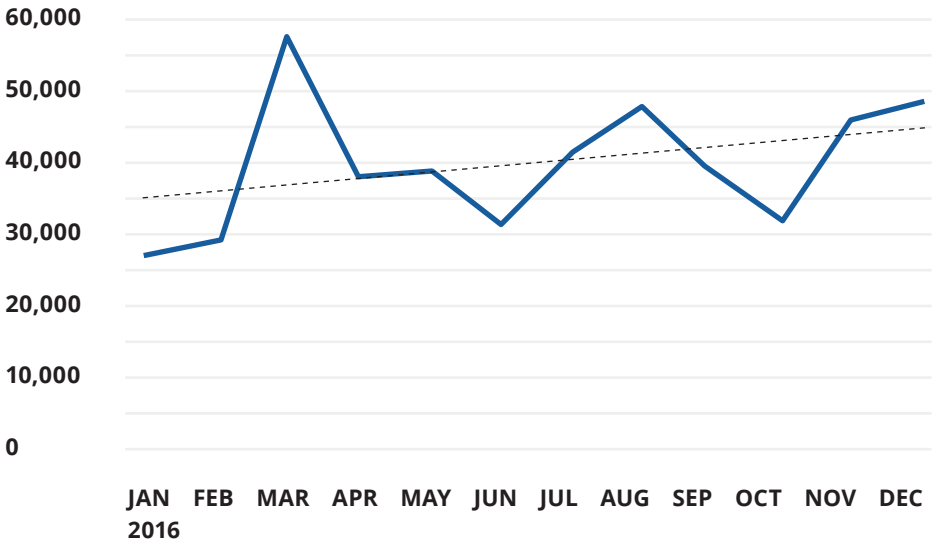
The number of newly created cryptor modifications, Q2 2016 – Q1 2017
Kaspersky Lab report, May 2017

KEY TAKEAWAYS

Acronis Active Protection is a new generation of data protection that incorporates Acronis' 14 years of experience protecting the data of over half a million organizations.

- It is real-time backup protection from ransomware. You don't lose data even if attacked.
- It protects your data, backup files, and the backup application itself, even if a ransomwarae variant is new or not yet identified.
- It is easy to use: it is user friendly, completely transparent, and provides automatic protection.

Acronis Active Protection adds an enhanced layer of data protection against today's ransomware and future variants.



Global ransomware detections by month
Symantec Corporation's Report, April 2017

ACRONIS ACTIVE PROTECTION: AN EFFECTIVE ANSWER TO RANSOMWARE THREATS

Acronis Active Protection is an advanced technology for Windows operating systems. Acronis has plans to expand it to cover Android® and other mobile and desktop operation systems in a similar way.

Acronis products and Acronis Active Protection patent-pending technology are the foundations of a very solid business continuity plan.

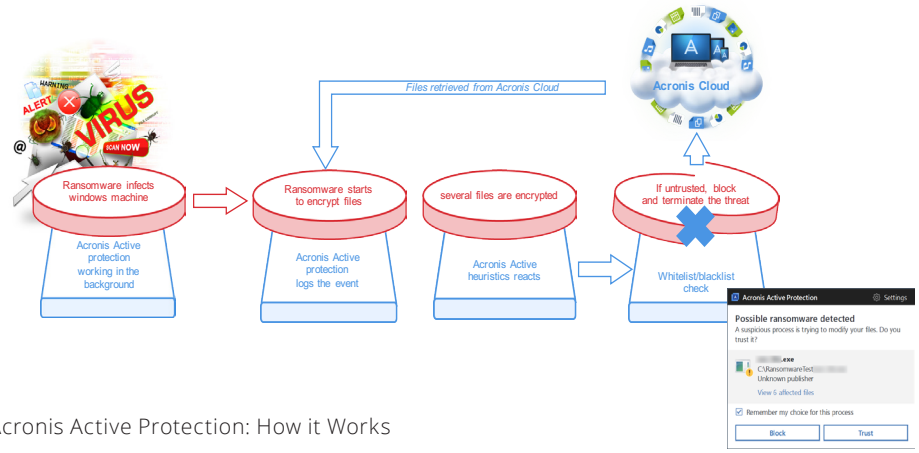
You always want to stop a ransomware attack as early as possible, preferably at the desktop before it can infect the network and other users. That is why you need a solution that identifies and stops the threat before it strikes.

Acronis offers the exact solutions to effectively fight ransomware attacks since all of their products include Acronis Active Protection. Organizations of all sizes and consumers can defeat ransomware by pairing Acronis products with the anti-malware solution of your choice.

The Heuristic Detection Approach

At the heart of Acronis Active Protection lies an heuristic approach, which is a modern and more advanced approach than detecting signatures alone. One signature can detect only one sample. However, heuristics can detect hundreds of files belonging to the same family by comparing a chain of file system events performed on the data to a database of malicious behavior patterns.

Acronis' behavioral heuristics are accompanied by white and black lists. While heuristics can detect new threats, they operate based on experience/ behavior results and need to be



Acronis Active Protection: How it Works

controlled for false positives. Therefore, Acronis Active Protection also checks suspicious processes against the whitelist and blacklist. When a user blocks a potential ransomware attack, it goes into the blacklist so that the malicious program does not start on the next reboot and the user does not need to repeatedly block the ransomware.

One way attackers try to compromise backups is to attack the backup software's agent. However, this won't happen with Acronis because Acronis Active Protection self-protects the Acronis agent program. No process in the system, except Acronis software, can modify backup files. In addition, Acronis Active Protection incorporates a robust self-defense mechanism that eliminates any typical attack so that cyber criminals cannot disrupt the work of the Acronis software or alter the content of backup files.

Lastly, Acronis Active Protection also monitors the Master Boot Record (MBR) of any user's Windows-based machine hard drive and does not allow any changes for non-whitelisted legitimate utilities.

Does Acronis Active Protection Work With Any File?

Yes, it does. Lets discuss the three ways how it protects any file.

1. Ransomware attack on any file

When a file is attacked, a user typically recovers by accessing previously backed-up files to restore compromised data. However, with Acronis Active Protection's real-time technology, encrypted files are restored automatically to the latest version after user confirmation. This feature is important particularly with scheduled backups. If you schedule a backup at midnight, but your machine is hit by a ransomware attacked at 11pm, you can lose more than 10 hours of work. When processes are constantly monitored, no data is lost when a ransomware attack occurs.

2. Ransomware attacking a local backup file

In this case, Acronis Active Protection actively monitors local drives and prevents backup files from being modified by malicious means.

3. Cloud backups are modified by malicious means

Files stored in Acronis Cloud Storage are exceptionally safe from direct modification by malicious code. Acronis Active Protection uses strong, end-to-end encryption and restricts access to file modification activities to signed and authorized Acronis agent software.

Ransomware Attacks and How Do We Deal With Them

The table below lists the ransomware attack techniques and the methods used by Acronis Active Protection to combat attacks.

Why is Acronis Active Protection Better than an Antivirus+Traditional Backup Software?

Two separate products cannot guarantee your data is safe from ransomware because they are not integrated. With the traditional approach, if your anti-malware software does not detect an attack on your data, your data is gone. Acronis Active Protection, strengthened by backups to local storage and secure Acronis Cloud Storage, recovers original data from local caches, local backups, or cloud backups.

Behavior Type	Explanation	Acronis Active Protection Response
In-place overwrite	Ransomware opens and modifies data files in-place.	The driver provides file access notifications to the service with heuristics data and performs copy-on-write of suspicious activities. The service detects the case, suspends the ransomware, and the driver rolls back the file from cache.
Via rename	Ransomware opens, renames, and modifies data files.	The same pattern as above.
Via new file	Ransomware creates a new file, copies original content, modifies a new file, deletes the original file.	The same pattern as above.
Master Boot Record overwriting	Ransomware attacks the physical drive, overwrites the MBR, the system is rebooted, HDD/MFT is encrypted on reboot (chkdsk disguised).	The driver watches WRITE/SCSI operations to the MBR via RAW FS and notifies the service. The service verifies the process and makes the decision.
In-place overwrite or rename or new file with injection into known good processes	Ransomware makes the injection into a well-known, good process and performs malicious actions as described above.	The driver provides injection attempt notifications to the service and the service instructs the driver to watch the process without performing copy-on-write. If suspicious patterns are detected, the user is instructed to recover files from the cloud.

Many times, anti-malware software misses a ransom-demanding malware because cybercriminals target the anti-malware itself by finding weaknesses in detection technologies or the program architecture.

This makes traditional approaches weak because cybercriminals only need to encrypt their malware to avoid detection.

This is why all anti-malware vendors recommend backing up your systems. At the same time, all cloud backup solutions protect against a simple attack vector – damage of data on a local machine. No one protects against a targeted attack on a backup solution.

Acronis Active Protection Protects Against Future Threats

Cybercriminals attack backups because their current business is threatened. Projects such as No More Ransom are educating users to do two simple and very important things – backup their systems and data and do not pay the ransom!

As a result, cybercriminals are now attacking backup files. However, with more predominate use of cloud backups, cybercriminals are getting even more creative. In order to compromise a cloud-based backup, the criminals need to acquire credentials to access the cloud — and regular ransomware malware does not have these credentials.

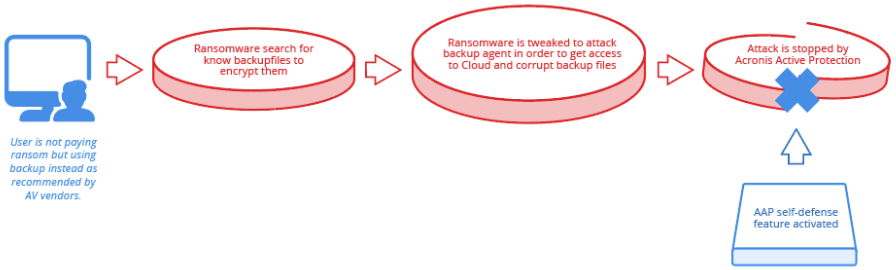
Instead, cybercriminals will attack the agent on the device that acts as a gateway to get data to the cloud. Technically, there are many ways to inject the malicious code in a local agent and compromise backup data in the cloud. Fortunately, there is one backup solution that can stop this — Acronis suite of products with Active Protection.

Independent Labs Agree

Independent lab AV-Test put four new programs onto the test bench and concluded, "The test clearly demonstrates that useful malware protection ought to include the deployment of backup software. [Acronis Active Protection technology] was the only backup solution in the test that was able to stop ransomware attacks."

Independent lab MRG Effitas came to the same conclusion. In the scope of their tests for Acronis, they stated, "No Vulnerability found."

See the Acronis Blog for more details about these third-party tests.



Acronis Active Protection: Stopping Future Attacks

Acronis

For additional information, please visit **www.acronis.com**