Acronis Active Protection

Constant data availability in a changing threat landscape

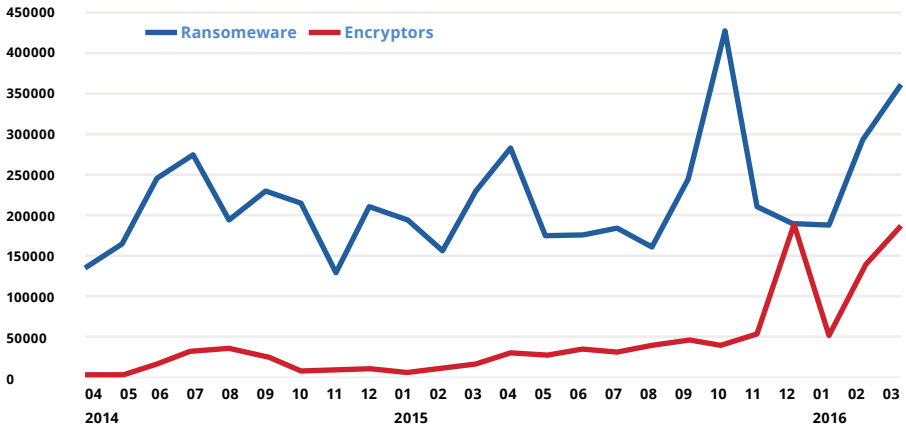
In 2015, online criminals used ransomware attacks to extort a mere $50M from victims. By the end of 2016, the FBI projects that ransomware gangsters will reap a cool billion dollars. The crooks are casting a wide net, targeting consumers and businesses alike.

In the future, perhaps ransomware will merely ask for money to prevent the bad guys from changing data in a random document to embarrass a person or compromise a legal request. Sounds like a nasty threat, but have you heard of it?

What is ransomware?

Ransomware is a type of malware that, upon infecting a device, blocks access to it or to some or all of the information stored on it. In order to unlock either the device or the data, the user is required to pay a ransom, usually in widely used e-currency. The term ransomware covers mainly two types of malware: so-called Windows blockers (they block the operating system or browser with a pop-up window) and encryption ransomware. The term also includes some of Trojan-Downloaders, namely those that tend to download encryption ransomware upon infection of machine. Nowadays, encryption ransomware is widely regarded as synonymous with ransomware.

In the graphs above, you can see that as ransomware grows in numbers, the anti-malware industry, including the FBI



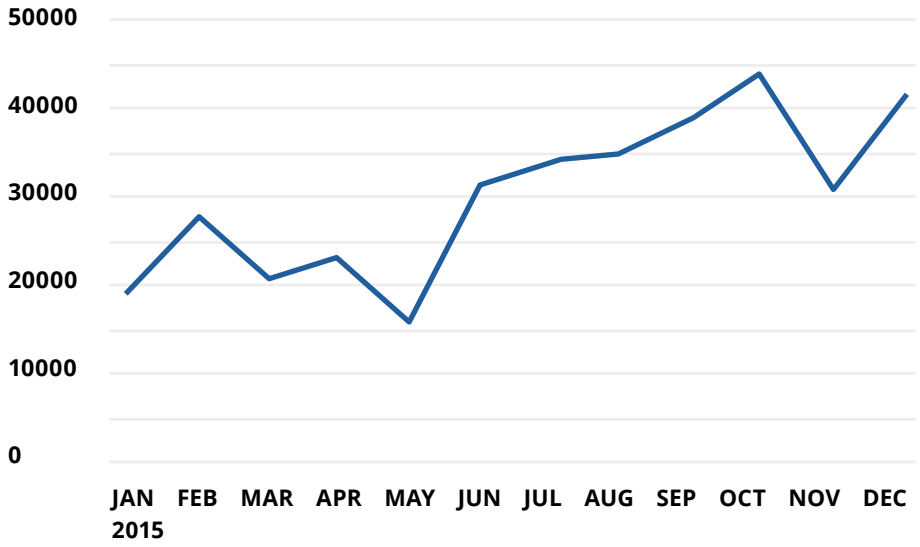
Data from Kaspersky Lab recent report (https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf)

A FEW THINGS TO REMEMBER

Acronis Active Protection is a new generation of data protection that provides:

- Real-time backup protection from ransomware for the Windows platform. There will be no time gap in restored versions of the files, so you do not have to lose any of your progress.
- It's future proof and can be enhanced even further when new threats emerge.
- It's completely transparent, user friendly, and works pretty much automatically.

As you can see, Acronis Active Protection adds an additional, and better, layer of data protection against today's ransomware and future variants.



Data from Symantec's recent report (https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf)

ACRONIS ACTIVE PROTECTION™: AN EFFECTIVE ANSWER TO RANSOMWARE THREAT

Acronis Active Protection is an advanced technology for Windows operating systems. Acronis has plans to expand it to cover Android and potentially other mobile and desktop operation systems in a similar way. However, at this point, the security industry sees most attacks on Windows machines as they are very widespread and ransomware has a long history of hitting Windows systems. This means cybercriminals need less research and efforts in order to create ransom-demanding malware.

Acronis Active Protection's patent-pending technology is also a foundation of a very solid data protection approach. It can be expanded in a variety of ways. But let's see the basics of how it works now.

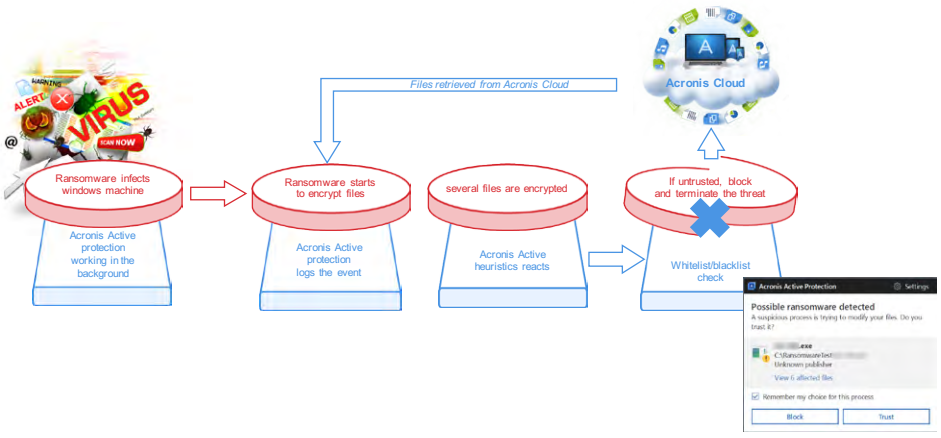
and similar organizations, agree that this threat will unfortunately grow more and more, especially in a corporate and smaller business space.

It is always better to stop a ransomware attack as early as possible. It should be stopped at the desktop, if possible before the ransomware has a chance to encrypt any files. So, it is important to understand the threat and use solutions that will enable a security team to respond quickly to a ransomware attack, without disrupting the workflow to the desktop and networking teams, as well as users on the network. This is applicable not only to corporate users, but consumer users as well.

Acronis has exactly the solution to fight ransomware effectively. It can be used as a part of Acronis consumer (and later on, corporate) products or you can pair these products with the anti-malware solution of your choice.

The heuristic detection approach

At the heart of Acronis Active Protection lies a heuristic approach that you may have heard of in relation to the anti-malware industry. The heuristic detection approach is much more modern and advanced than the signature one. One signature can detect only one sample, while heuristics can detect a few or even few hundreds of samples of files that belong to one



so-called family (usually similar in behavior or patterns of actions). The behavioral heuristics we are talking about are basically a chain of actions (file system events, to be precise) done by a program, which is then compared with a chain of events in a database of malicious behavior patterns.
Behavioral heuristics are accompanied by white and blacklists of various programs. Why do we need a whitelist check? Because heuristics are capable of detecting new threats, yet at the same time they operate on the basis of experience/behavior results and need to be controlled for false positives. That is why Acronis Active Protection products check any suspicious processes against the whitelist and blacklist. At the same time when user blocks the potential ransomware it goes into the blacklist and this does not let this malicious program to start on next reboot. This is very important because user do not have to repeat the process of blocking the ransomware all over again.
An obvious way for attackers to compromise the backup would be an attack to the Acronis True Image program. We implemented self-protection of the Acronis agent program. No process in the system except Acronis software can modify backup files, We have also implemented a robust self-defense mechanism that will eliminate any typical attack and not allow criminals to disrupt the work of the Acronis software or alter the content of backup files.
More than that, Acronis Active Protection also monitors the Master Boot Record of the user's Windows-based machine hard drive and will not allow any changes there for non-whitelisted legitimate utilities.

Does Acronis Active Protection work with any file?

Yes, it does. However, we must structure this in a way of constant, active data protection from three main threat vectors.

1. Ransomware attack on any file
A typical case can usually be solved by using previously backed-up files to restore compromised data. However, this is now easier to handle and most likely will never happen on a wider scale if you have an Acronis Active Protection-enabled product. Restoration of a few encrypted files is done automatically (after user confirmation) and to the latest version-- because the technology works in real-time. Imagine the situation when a backup is scheduled to be done at midnight but at 11 P.M., the machine is hit by ransomware. By simply recovering files from an online backup, 11 hours of work are lost. With constant monitoring of processes activity, as described above, no data is lost when a ransomware attack is initiated.

2. Ransomware attacking a local backup file
In this case, Acronis Active Protection actively monitors any 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, by using end-to-end strong encryption and restricting access to file modification activities only to signed and authorized Acronis agent software.

Ransomware attacks and how do we deal with them

Let's take a look on the table below where you can see techniques and

Behavior type	Explanation	Acronis Active Protection response
In-place overwrite	Ransomware opens and modifies data files in-place	Driver provides file access notifications to the service with heu-ristics data, per-forms copy-on-write of sus-picious activities. The ser-vice detects the case, sus-pends ransomware, the driv-er rolls back the file from its own 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, de-letes the original file.	The same pattern as above.
Master Boot Record overwriting	Ransomware opens Physi-calDrive, overwrites MBR, the sys-tem is rebooted, HDD/MFT is en-crypted on reboot (chkdsk dis-guised).	The driver watches WRITE/SCSI operations to MBR via RAW FS, notifies the service, the service veri-fies 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 does mali-cious actions as described above.	The driver provides injection attempts notifications to the service and the service in-structs the driver to start watching the process with-out doing copy-on-write. If suspicious patterns are no-ticed, a user can be instruct-ed to recover files from the cloud.

methods used by ransomware to perform its malicious actions.

Why is it better than antivirus plus any backup software?

That's actually simple: two separate products won't save your data from ransomware, as they do not know how to talk to each other. Any data impacted by a missed detection from an anti-malware solution in a traditional approach is gone, as no antimalware solution backs up files to the cloud and no backup solutions detect a malware presence. With Acronis Active Protection paired with Acronis Cloud via an Acronis endpoint agent, original data can be recovered from local caches, local backups, or cloud backups. This eliminates this most dangerous ransomware-related threat.

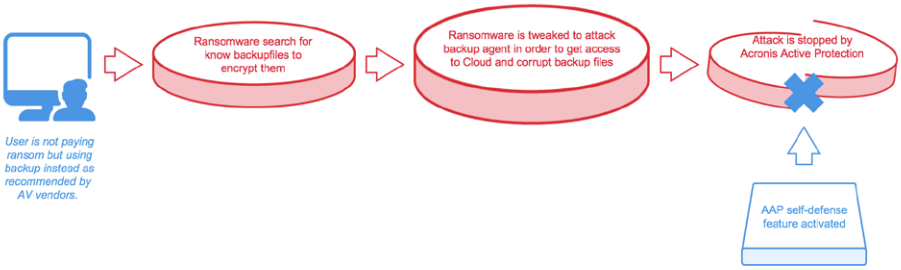
Anti-malware software can miss a ransom-demanding malware because this is actually what cybercriminals target. The bad guys research major, if not all, anti-malware solutions to find weaknesses in detection technologies or program architecture, in order to avoid detection. As we already mentioned, traditional signature detection is useless nowadays because cybercriminals just need to encrypt the malware in order to avoid detection. And many free anti-virus software packages still use this approach. So, this case is quite likely, that is why all anti-malware vendors recommend using backups, as we said earlier. At the same time, all cloud backup solutions protect against a simple attack vector – damage of data on a local machine. But no one protects against a targeted attack on a backup solution.

Acronis Active Protection protects against future threats

Why would cybercriminals attack backups? Because they will see a threat for their business/money income very soon. Projects like https://www.nomoreransom.org/prevention-advice.html motivate users to do two simple and very important things – backup and do not pay the ransom!

So, bad guys are already attacking backup files. However, this won't be enough in almost all cases, as many backup solutions have cloud storage. In order to compromise a cloud-based backup, they need to acquire credentials to access the cloud — and regular ransomware malware does not have these.

So bad guys will think: "How does data makes its way to the cloud?" Obviously, through an agent on the device. Technically there are many ways to inject the malicious code in the local agent and compromise backup data in the cloud. The only backup software that can stop this future attack is an Acronis product with Active Protection.



Acronis

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