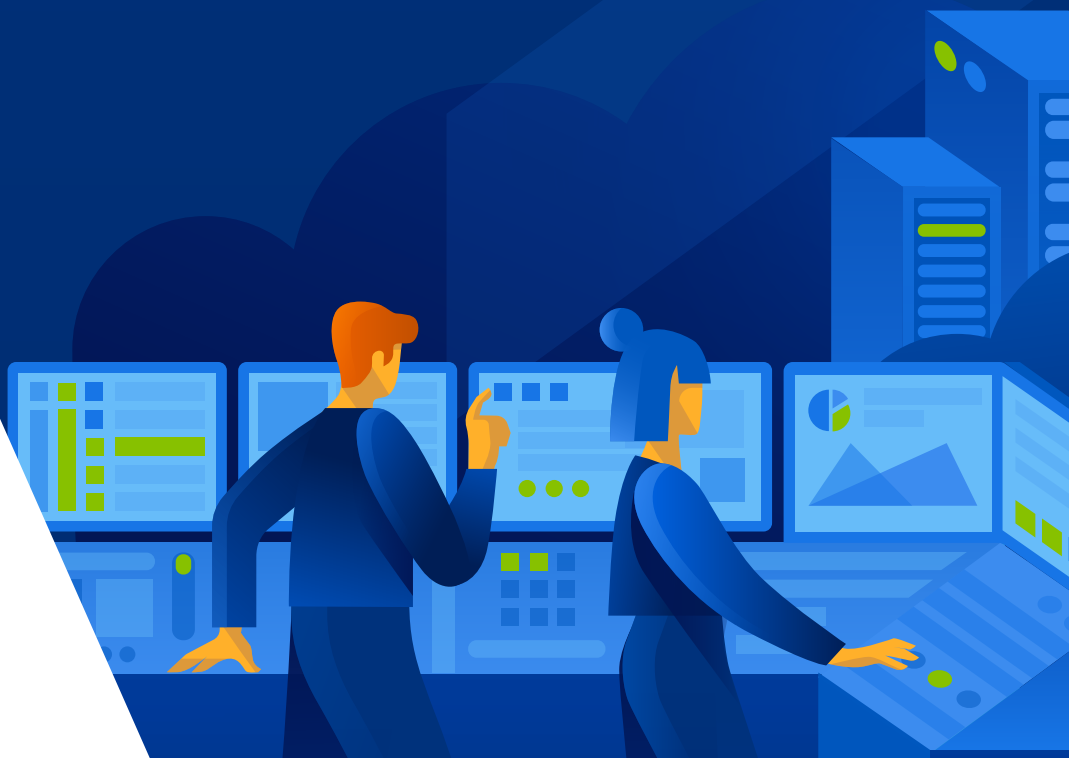
Acronis



WHITE PAPER

Acronis Active Protection: Constant data availability in a changing threat landscape

AI-based defense for your critical data

Ransomware attacks, which pose a direct threat to user data, continue to grow in frequency and complexity. You may have heard of 2017 global epidemics such as WannaCry and exPetr, which hit hundreds of companies around the globe. Good news: We have Acronis Active Protection to keep your data safe and secure.

Cryptors, a form of ransomware that encrypts files, are becoming more popular. In 2020, AV-Test reported 137.51 million new malware attacks, only slightly less than the year before, and a 50% increase in ransomware attacks worldwide.

Acronis security experts see signs of growing competition between ransomware distributors. Attackers are starting to probe previously unreached countries, where users may not be prepared for fighting ransomware and where competition among criminals is lower. Ransomware-as-a-Service is becoming more and more popular, with amateur cybercriminals trying to earn easy money.

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. Another growing threat is so-called wiper malware. This looks like a ransomware cryptor that encrypts your data, but its goal is simply to destroy the data. There is no way to restore the data and no ransom to pay. One example is the exPetr wiper, which you can read about on our blog. Another example is Industroyer, which we also covered.

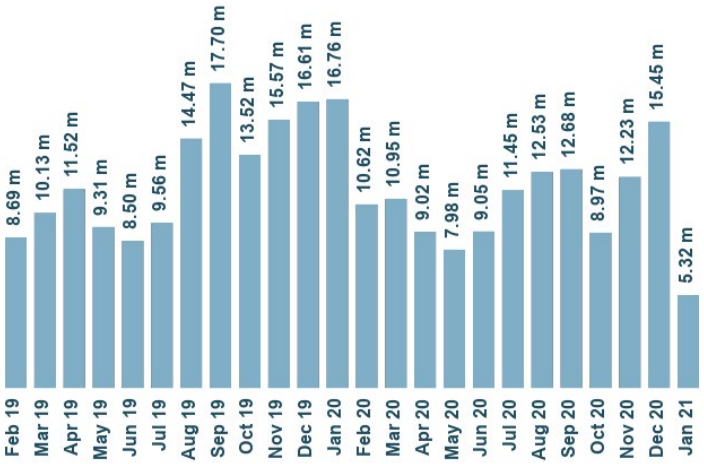
We call these types of threats "data infringing malware." Let's take a closer look.

WHAT IS RANSOMWARE, CRYPTORS, AND WIPERS?

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 has to pay a ransom, usually in a widely used e-currency like bitcoin.

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 (cryptors). But it also includes some trojan-downloaders, namely those that tend to download encryption ransomware upon the infection of a machine.

Today, encryption ransomware is synonymous with ransomware and is the most popular type out there. If the cryptor does not have data restore functionality, it is called a wiper. In the chart below, you can see the recent growth in ransomware. Security experts, the FBI, and other organizations agree that ransomware attacks will continue to take place more frequently, especially in corporate and small business environments.



Source: AV-Test
https://www.av-test.org/en/statistics/malware/

It is always best to stop a ransomware attack as early as possible – 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 infection without disrupting the workflow to the desktop and users on the network. This is applicable not only to corporate users, but home users as well.

ACRONIS ACTIVE PROTECTION: AN EFFECTIVE ANSWER TO RANSOMWARE

Acronis has exactly the solution to fight ransomware effectively: Acronis Active Protection, which is included in many Acronis Cyber Protection solutions. Acronis Active Protection is an advanced technology that uses sophisticated analysis and artificial intelligence to monitor your system for any erratic behavior and quickly stop it. If ransomware somehow manages to get through the first line of defense and start encrypting

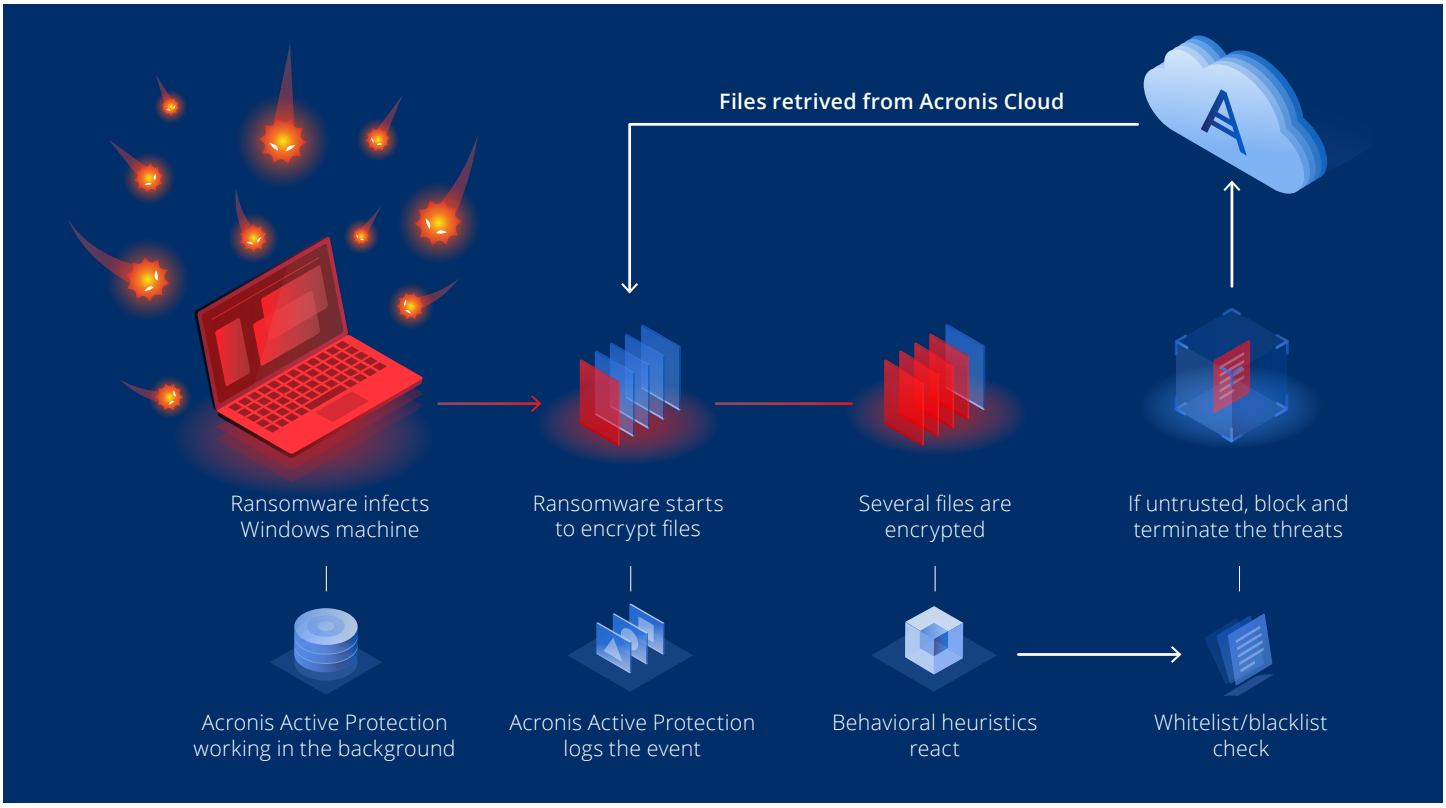
files, Acronis Active Protection will quickly detect the encryption and halt it – automatically restoring the files to the most recently backed up version.

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 take a closer look at how it works.

THE HEURISTIC DETECTION APPROACH

At the heart of Acronis Active Protection lies a heuristic approach to malware detection that is much more advanced than the traditional, signature-based approach. While one signature can detect only one sample, heuristics analysis can detect hundreds of samples of files that belong to one so-called family (usually similar in behavior or patterns of actions). Acronis' behavioral heuristics are basically a chain of actions (file system events, to be precise) done by a program that is then compared with a chain of events in a database of malicious behavior patterns.

Acronis Active Protection checks any suspicious processes that it detects against the whitelist and blacklist. Potential ransomware is stopped and placed on the blacklist, which prevents it from starting again on the next reboot. This is important because the user does not have to repeat the process of blocking the ransomware all over again next time they start the machine. In addition, Acronis Active Protection monitors the Master Boot Record of the user's hard drive and will not allow any changes there by software that isn't legitimate and included on the whitelist.



ACTIVE PROTECTION ENHANCED BY MACHINE LEARNING

Acronis introduced Active Protection in January 2017. While performing well in independent testing and earning accolades from the media, Acronis has worked diligently to make it even better. The result is an improved version that incorporates machine learning and artificial intelligence technologies.

How does it work? The first step is a stack trace analysis. A stack trace is a report that provides information about program subroutines. It is commonly used for certain kinds of debugging, where a stack trace can help

software engineers figure out where a problem lies or how various subroutines work together during execution.

Put simply, it is possible to detect code injections from ransomware using process stack trace analysis based on a machine learning approach.

Why is the ability to detect code injections important? Because injection into legitimate processes (e.g., explorer.exe, regsvr32.exe, svchost.exe, etc.) is a high-end technique used by sophisticated black hat developers to hide ransomware's traces in a system and avoid detection. With code injection, attackers do not need to use custom processes that can be easily detected. If Acronis Active Protection notices something strange is going on with a legitimate process, it takes a stack trace and sends it to our machine learning module, where the behavior is compared with existing models of clean and infected stack traces to determine if it's a threat or not. If the behavior is confirmed to be malicious, the user gets an alert suggesting that they should block the ransomware-like process. As a result, machine learning not only raises the detection level but also reduces any potential false positives as it acts like second authority for heuristics to make the final decision.

IMPROVED AGAIN IN 2019

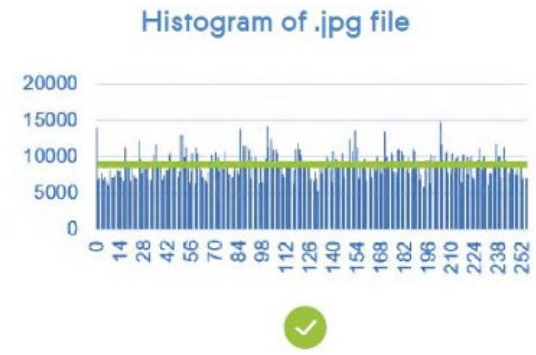
Since its introduction in 2017, Acronis Active Protection has continuously been enhanced and improved. In 2019, self-defense was improved even further to prevent illicit termination of processes. If ransomware tries to stop Windows processes affecting work on Acronis Active Protection, we will prevent this. Secondly, we improved multi-process injection detection, a technique used by some sophisticated ransomware families. Thirdly, core behavioral heuristics were updated to make ransomware detection even more effective. Last but not least, we did a lot in terms of performance, in some cases speeding up detection by 30% and optimizing the whole process of communication with our Acronis Cloud Brain.

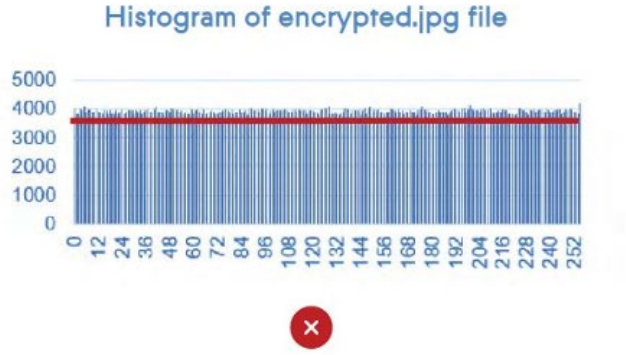
In terms of AI in Acronis Active Protection – the stack trace detection model was reduced in size even further, which means faster reaction times. As a result, processing is accelerated and model training takes minutes instead of hours.

OTHER TECHNIQUES USED BY ACRONIS ACTIVE PROTECTION TO SAFEGUARD DATA

Analysis of statistical distribution can also be used to fight ransomware. Acronis Active Protection can create a histogram by inspecting individual bytes of the data before and after a ransomware attack. Due to the nature of encryption, the histogram of the data after encryption is distinct and easily recognizable. After that, a statistical distribution test is performed on the data. If the histogram closely resembles that of an encrypted file, it will be flagged as suspicious and result in a ransomware alert in end-user interface.

Another technology that is now a part of Acronis Active Protection: specially crafted honey pots that are used to find and disarm ransomware. Like a bee is drawn to honey, ransomware is often looking for certain kinds of files. If you place these kinds of files into controlled directories, you can catch and isolate the ransomware. Because Acronis Active Protection controls these directories, the infection can't spread. This technique is totally safe and secure. Users won't see these files because they are hidden in the system and take up very little space on a hard drive, so this additional layer of security doesn't create any inconveniences.





NEW LEVEL OF ANTI-RANSOMWARE DEFENSE

With machine learning leading the way, all of these technologies bring Acronis Active Protection to a whole new level, especially when it comes to zero-day threats. It creates a model of which processes are legitimate, so even if bad guys find a new vulnerability or way to infiltrate the system, machine learning will detect the ransomware's processes and put a stop to them.

Acronis' machine learning infrastructure is built so that new anonymized user data will be uploaded regularly for analysis. But new behavior models will be ready much faster and updates to product heuristics will be sent in a matter of seconds to further boost security.

ACRONIS ACTIVE PROTECTION ALSO PROTECTS BACKUP FILES

Why would cybercriminals attack backups? Because regular backups are a key defense against ransomware. If the data on your machine is backed up and stored out of reach from hackers, ransomware is little more than nuisance. Projects like www.nomoreransom.org motivate users to do two simple and very important things – back up and don't pay the ransom!

So, bad guys have started attacking backup files. The only anti-ransomware that can stop this kind of attack is Acronis Active Protection, which prevents any process in the system other than Acronis software from modifying backup files.

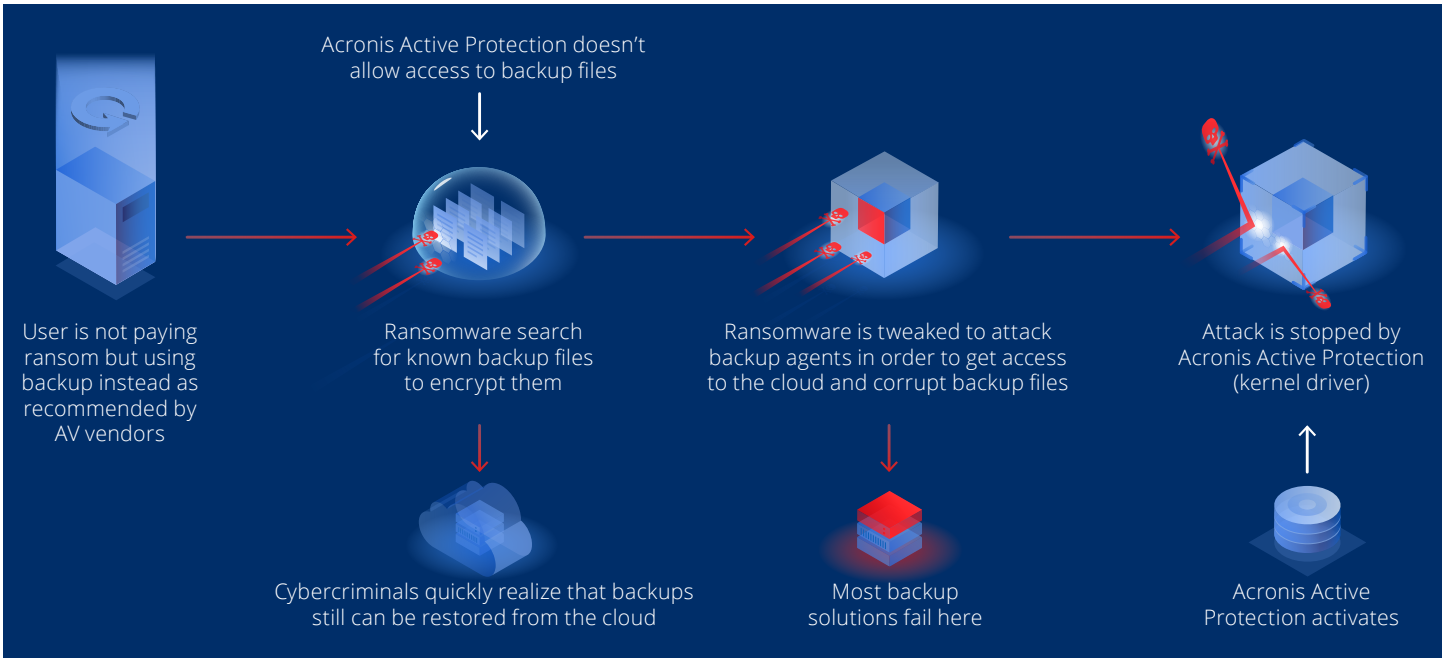
We have also implemented a robust self-defense mechanism that eliminates any typical attack and does not allow criminals to disrupt the work of the Acronis software or alter the content of backup files.

A FEW THINGS TO REMEMBER

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

- **Real time protection from ransomware. There will be no time gap in restored versions of the files, so you do not have to lose any of your progress.**
- **Future-proof protection that is enhanced further whenever new threats emerge.**
- **Transparent, user friendly protection that works automatically.**

As you can see, machine learning and new heuristics algorithms make Acronis Active Protection an even better layer of data protection against today's ransomware and future variants.



Acronis

Learn more at
www.acronis.com