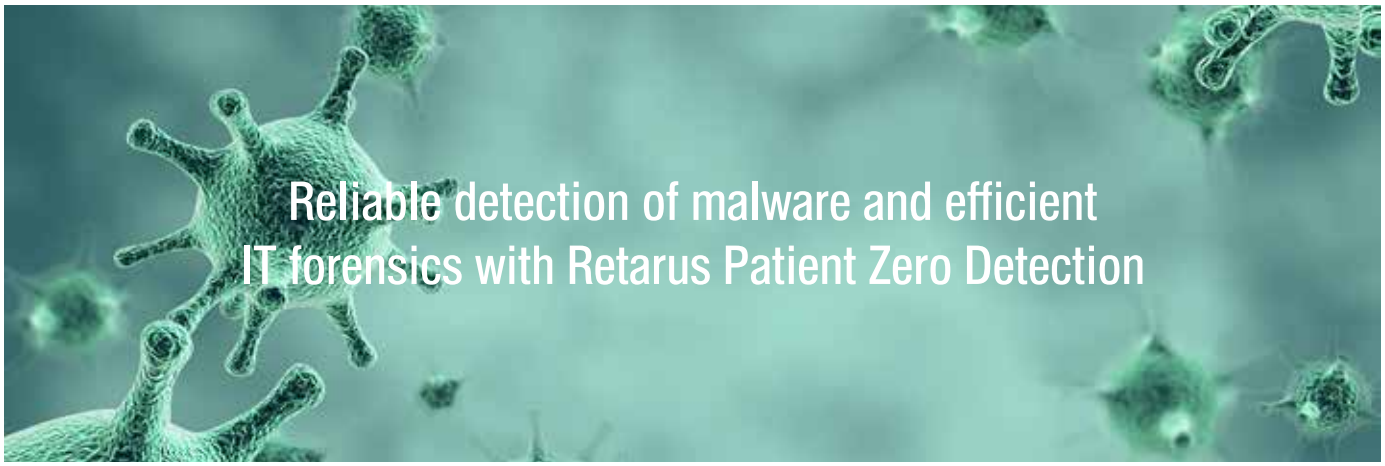
retarus



Reliable detection of malware and efficient IT forensics with Retarus Patient Zero Detection

The challenge

Simple protective measures have long been insufficient. The number of viruses attacking a company's infrastructure on a daily basis has grown too large. Once malware has entered the system, it becomes crucial to limit the damage it can cause. Only by identifying the recipients of infected messages, the so-called patient zeros, can timely measures be taken to prevent greater harm from being inflicted. At the same time, system settings have to be optimized continually to ensure comprehensive protection from future threats.

The background

Unfortunately, a large portion of electronic mail consists of spam, virus or targeted phishing attacks. Across the globe, more than 390,000 new instances of malicious software are registered daily. That means an average of 270 new computer viruses per minute. Email security programs are generally reliable at filtering out infected emails. However, no virus filter can offer 100 percent protection. When a specific virus first appears, even the best virus scanners are not familiar with its signature. That's why in addition to cloud services a lot of companies employ on-site virus scanners or elaborate sandboxing solutions. But in such cases administrators and recipients also often only learn about the existence of new types of viruses after it is already too late and the malware may have already had a chance to cause damage. The fact that the origin of the attack often remains unknown additionally complicates IT forensics enormously.

The solution

Retarus E-Mail Security safeguards reliably against malware attacks thanks to multi-level virus protection, intelligent spam and phishing filters as well as the Retarus Attachment Blocker. Retarus' proven fourfold virus scan, for instance, already ensures a very high level of protection by filtering out 35 percent more viruses than conventional virus protection services which rely on only two scanners. In combination with Retarus Patient Zero Detection, businesses can now protect their infrastructures even more securely against attacks and are moreover able to detect previously unknown malware.

Customer benefits

- Maximum protection for your IT infrastructure
- Quick response to attacks
- Simplified IT forensics
- Efficient business communication
- Sustainable optimization of system settings

Benefits at a glance

- Recipients of previously undetected malware reliably identified
- Instant alerting
- Email delivery without any delay
- Detailed reports and analyses
- Seamlessly integrates with Retarus Enterprise E-Mail Archive and Retarus E-Mail Encryption

Use Case

Retarus E-Mail Security makes use of multiple virus scanners with continually updating filter rules, which already provide an effective safeguard against the overwhelming majority of malicious messages.

Retarus' innovative Patient Zero Detection technology also identifies dangerous emails which have already been delivered. To this end, a digital fingerprint is generated for each attachment carried by incoming emails and stored in a database within the Retarus infrastructure. This does not result in any delay in delivery times. As soon as a virus scanner identifies malware in the same type of attachment at a later time, Retarus compares the fingerprint for the malicious attachment with the information saved in the database. The infected email is deleted immediately. If the signature matches one already stored in the database, the responsible administrators and, optionally, all previous recipients of the attachment are alerted immediately.

Thanks to the instant alert and details regarding the origin of the attack and the recipients, the impacted systems can be identified in no time and measures can be taken to prevent the virus from spreading throughout the company's network. The administrator can effortlessly check whether the email has already been forwarded. In this way, the infected email can often be deleted even before it has been opened.

Once an infected attachment has been opened, Retarus Patient Zero Detection simplifies the IT forensics. Detailed reports and analyses provide concrete points of reference about which files should be searched for viruses. In order to ensure better protection for the system in the future, the filter settings in Retarus E-Mail Security are continually optimized based on information obtained from Patient Zero Detection.

Did you know?

According to Kaspersky, $861,000 is the average cost resulting from a cyber attack against Enterprises.

Other scenarios

Secure encryption
Sensitive data should never be allowed to fall into the wrong hands. With Retarus E-Mail Encryption companies can safeguard the confidentiality of communications and implement applicable data privacy laws without any difficulty.

Intelligent email quarantine
Email digests provide businesses with a quick overview of all filtered virus and spam messages. Users can retrieve emails classified as spam directly from quarantine immediately, without requiring portal access. To ensure maximum protection, these messages are checked again for viruses when they are downloaded.

Attachment Blocker
With the Retarus Attachment Blocker companies can provide their infrastructures with even higher levels of security against malware attacks. This function prevents users from receiving all attachment formats which the administrator classifies as untrustworthy.