HORNETSECURITY

Advanced Threat Protection

Detect and prevent highly complex and sophisticated attacks - effectively and in real time.

Use Hornetsecurity ATP to protect your business against individually targeted attacks starting from the first malicious email. Highly innovative forensic analysis engines ensure that the attacks are stopped immediately. At the same time the solution provides detailed information about the attacks on the company.

Protection against ransomware

Ransomware has increased sharply since the beginning of 2016: these are viruses that cripple the computer or an entire network by encrypting the locally stored files. It is only by paying a ransom - hence the name - that users have a chance to access their data again. Locky, Tesla, Petya and the like are polymorphic viruses that can be very difficult to detect. To do so, Hornetsecurity ATP uses, among other things, a sandbox engine to analyse the behaviour of attachments when being opened and filter out the email in the event of a positive find. Hornetsecurity also "freezes" suspicious emails in order, once the signatures of the filters have updated after a few minutes, to scan again.

Protection against blended attacks

Blended attacks combine different avenues of attack to be successful. The email can, for example, include a document that in turn can hide a link to a download page with malware. Hornetsecurity ATP combats these types of attacks by means of URL scanning and URL rewriting as well as sandboxing and freezing.

Protection against targeted attacks

High-ranking employees of companies are often the target of individual attacks, so-called spear phishing, whaling or CEO fraud. The attackers try to obtain passwords or credit card information, or convince the employees to transfer funds to a specific account. These attacks are virtually undetectable by conventional means. With Hornetsecurity ATP, the internal communication between particular persons in the company is specifically examined for such attacks in order to prevent abuse through identity spoofing.

Protection against digital espionage

According to a survey conducted by the IT industry association Bitkom, more than half of German companies have already been the victim of data theft, sabotage or espionage. The Hornetsecurity Spy-Out forensics system detects both known and completely new patterns for spying out information. This system reacts instantly and alerts you before information needing protection leaves the company.

Notification of attacks

The Hornetsecurity real time alerts notify you of acute attacks on your company and allow the rapid initiation of further internal measures and legal procedures. The notification system provides detailed analysis results for this purpose. The customer security team can also sensitise employees to identify additional avenues of attack, for example by telephone. If already delivered emails are later identified as potentially harmful, ex post alerting enables the IT security team to undertake an investigation into the accounts or systems affected.

HORNETSECURITY

Integration of Hornetsecurity ATP into email security management.

Hornetsecurity ATP integrates seamlessly into spam and virus filters. Emails that have passed this first test are subjected to further analysis by Hornetsecurity ATP. Among other thing, the service executes attachments and observes their behaviour in detail.

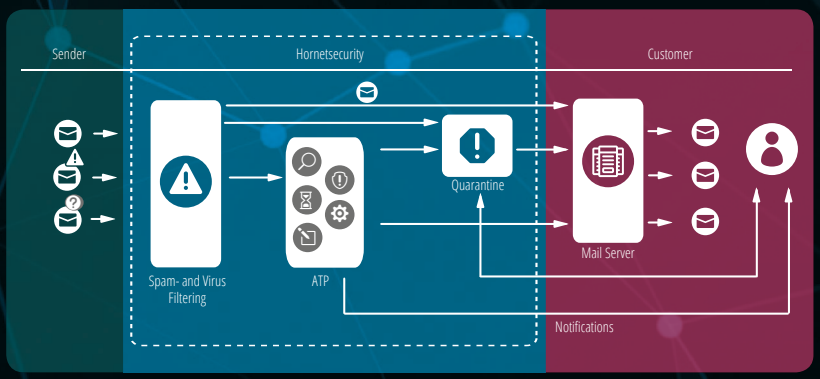
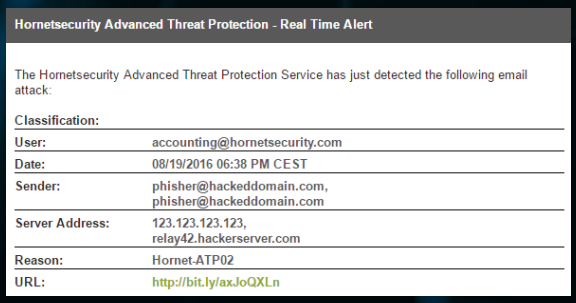


Fig: Spam and virus filter procedure with Hornetsecurity ATP



Hornetsecurity Advanced Threat Protection - Real Time Alert

The Hornetsecurity Advanced Threat Protection Service has just detected the following email attack:

Classification:	
User:	accounting@hornetsecurity.com
Date:	08/19/2016 06:38 PM CEST
Sender:	phisher@hackeddomain.com, phisher@hackeddomain.com
Server Address:	123.123.123.123, relay42.hackerserver.com
Reason:	Hornet-ATP02
URL:	http://bit.ly/axJoQXLn

Real-time notifications

As soon as Hornetsecurity ATP detects an attack, an alert is sent to the respective company's IT security team to inform it immediately about a possible threat. The person in charge is given various details on the nature and objective of the attack, the sender and why the email was intercepted.

Fig: Real-time notification by Hornetsecurity

Hornetsecurity ATP engines	Functioning and advantages
Sandbox engine	Attachments are executed in a variety of system environments and their behavior is analyzed. If it turns out to be malware, you are notified. Protects against ransomware and blended attacks.
URL rewriting	The URL rewriting engine secures all Internet calls from emails via the Hornetsecurity web filter. In the process, the sandbox engine also analyses downloads.
URL scanning	A document (such as PDF, Microsoft Office) attached to an email may contain links. However, these cannot be replaced, as this would violate the integrity of the document. The Hornetsecurity URL scanning engine leaves the document in its original form and only checks the target of such links.
Freezing	Emails that cannot immediately be clearly classified but look suspicious are retained for a short period by freezing. A further test is later performed with updated signatures. Protects against ransomware, blended attacks and phishing attacks.
Ex post alerting	If it later turns out that an already delivered email must after all be considered as potentially harmful, the respective company's IT security team is notified about the extent and possible countermeasures as soon as this is known. This permits rapid containment of a dangerous situation.
Targeted fraud forensics	Targeted fraud forensics detects targeted personalised attacks without malware or links. The following detection mechanisms are used for this: • Intention recognition system: alerting about content patterns that indicate malicious intent • Fraud attempt analysis: checks the authenticity and integrity of metadata and email content • Identity spoofing recognition: detection and blocking of forged sender identities • Spy-out detection: counter-espionage against attacks trying to obtain sensitive information • Feign facts identification: content analysis of messages based on provision of feigned facts • Targeted attack detection: detection of targeted attacks on individuals