HORNETSECURITY

FACT SHEET

ADVANCED THREAT PROTECTION

Counter modern threats with the most advanced defense mechanisms

The risk of a targeted cyberattack with ransomware, CEO fraud and Trojans is increasing dramatically.
Protect your business from devastating malware attacks with Advanced Threat Protection.

Protection from:

- ransomware
- blended attacks
- targeted attacks
- business email compromise

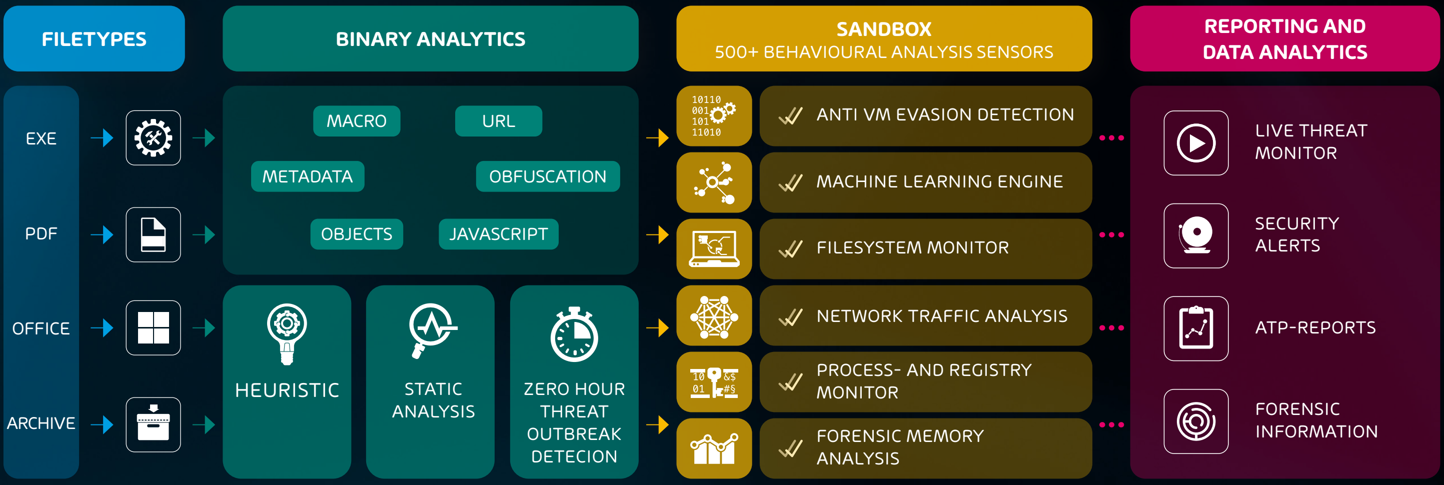
Fraud protection mechanisms

- Analysis of fraud emails on **content and meta level**
- Analysis of **SMTP transport** data in context with the management structure of a company
- Requests for funds/critical information permitted only from internal company sources
- External emails – with senders pretending to be managers – are blocked

Ransomware protection mechanisms

- **ATP sandbox accesses threat intelligence databases when scanning email attachments**
- Stored **indicators of compromise (IoC)** are classified using over 50 anti-virus engines available on the market
- Enrichment of the analyses with information on already known hash sums (e.g. of defective attachments or IP addresses that are in context with malicious instances)
- **Only about 5% of the IoCs for new ransomware campaigns in 2018 were evaluated negatively by conventional anti-virus engines at the first appearance of a ransomware**
- **Real time alarm: Real-time notification of IT security teams about acute attacks on the company. Contains detailed information about the type and scope of the attack.**

Fig.: Advanced Threat Protection Sandbox vs. Ransomware & Polymorphic viruses



FILETYPES

EXE

PDF

OFFICE

ARCHIVE

BINARY ANALYTICS

MACRO

URL

METADATA

OBFUSCATION

OBJECTS

JAVASCRIPT

HEURISTIC

STATIC ANALYSIS

ZERO HOUR THREAT OUTBREAK DETECION

SANDBOX
500+ BEHAVIOURAL ANALYSIS SENSORS

ANTI VM EVASION DETECTION

MACHINE LEARNING ENGINE

FILESYSTEM MONITOR

NETWORK TRAFFIC ANALYSIS

PROCESS- AND REGISTRY MONITOR

FORENSIC MEMORY ANALYSIS

REPORTING AND DATA ANALYTICS

LIVE THREAT MONITOR

SECURITY ALERTS

ATP-REPORTS

FORENSIC INFORMATION

www.hornetsecurity.com | info@hornetsecurity.com

HORNETSECURITY

FACT
SHEET

ATP-Engines	Functionality and advantages
Sandbox Engine	Email attachments are scanned for possible malicious codes by running the suspicious file in a virtual test environment and identifying potentially dangerous effects. If the document sent with the email is found to be malware, the email is moved directly to quarantine.
Secure Links	Secure Links protects users from malicious links in emails. It replaces the original link with a rewritten version that goes through Hornetsecurity's secure web gateway. If a user clicks on a link, a deep web scan is initiated: The service recursively scans the target site and follows links to look for malicious web resources. The system blocks access to malicious sites and prevents hackers and cybercriminals from being able to access the user's confidential data or infecting their computer with malware.
URL Scanning	Leaves the document attached to an email in its original form and only checks the target of links contained in it.
Freezing	Emails that are not able to be clearly classified immediately are held back for a short period of time. The emails are then subjected to a further check with updated signatures.
Malicious Document Decryption	Encrypted email attachments are decrypted using appropriate text modules within an email. The decrypted document is then subjected to an in-depth virus scan.
Targeted Fraud Forensics	**Fraud attempt analysis:** Checks the authenticity and integrity of metadata and mail content. **Identity spoofing recognition:** Detection and blocking of forged sender identities. **Intention recognition system:** Alerting to content patterns that suggest malicious intent. **Spy-out detection:** Defense against espionage attacks to obtain sensitive information. **Feign facts identification:** Identity-independent content analysis of news on the basis of falsified facts. **Targeted attack detection:** Detection of targeted attacks on individuals who are particularly at risk.
QR Code Analyzer	To be one step ahead of threat actors, Hornetsecurity developed a feature which is able to do more than simply scanning QR codes. The QR Code Analyzer also detects QR codes embedded in other images – Attackers may start using this trick to circumvent simple QR code scanning apps. The QR Code Analyzer can detect QR codes at light speed and can analyze different types, including URLs and texts. It supports all common image types such as GIF, JPEG, PNG and BMP.