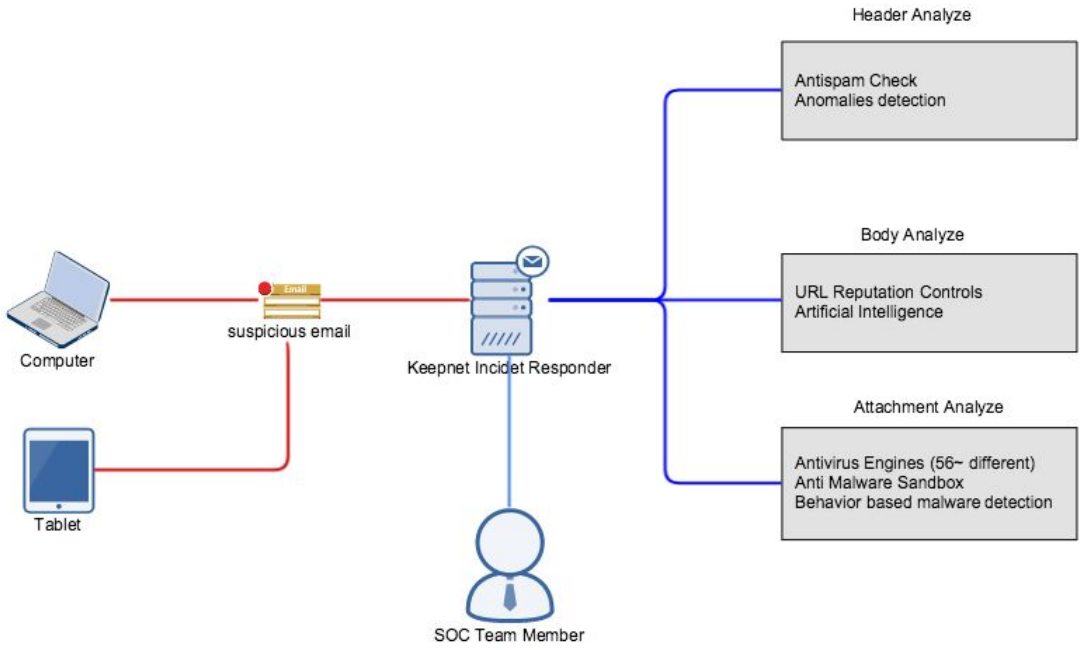
Next Generation Anti-Phishing Solution

About Keepnet Labs. Incident Responder

- *95 % of all attacks* *on enterprise networks are the result of successful spear phishing. (Source: SANS Institute)*
- *97% of people* *around the world cannot identify a sophisticated phishing email. (Source: Intel)*
- *Only 3% of targeted* *users report malicious emails to management. (Source: Verizon)*
- 66% of malware was installed via malicious email attachments. *(Source: Verizon)*
- 146 days globally, and a colossal 469 days for the EMEA region, which means early detection and alerts are as important as ever. (Source: Fireeye)

- How does your users report when they receive a suspicious email?
- What are you doing against the malware that passes your traditional security systems and reaches inbox?
- Are you able to invest hundreds of thousands of dollars to the most advanced threat analysis, sandbox, anti-exploitation solutions for analysis of emails and their attachments?
- When you perceive threats, you are too late to prevent it, do you realize it?
- This service analyzes suspicious e-mails (automatic or manual mode) reported from users' e-mail boxes with advanced integrated threat analysis modules. There is an active response feature to block traffic.

How Does It Work ?



1. Thanks to its plugin, Keepnet Phishing Reporter allows user to report suspicious e-mail with one click.

2. The Incident Responder service receives this email and analyses it with the following steps.

2.1. Header

2.1.1. Spam control with integrated antispam services

2.1.2. Anomaly detection

2.2. Body

2.2.1. URL reputation control

2.2.2. Malicious content detection

2.2.3. Detecting suspicious content with artificial intelligence

2.3. Attachment

2.3.1. Known malware control with Antivirus services

2.3.2. Detection of unknown malware with Anti Malware Sandbox technology

2.3.3. Detection 0-day file format exploits with Anti Exploit technology

3. According to malware result, it creates attack signatures in the following kinds for alarm generation or blocking active security devices;

3.1. Snort Rule

3.2. Yara Rule

3.3. Antispam Rule

3.4. ACL for Firewalls

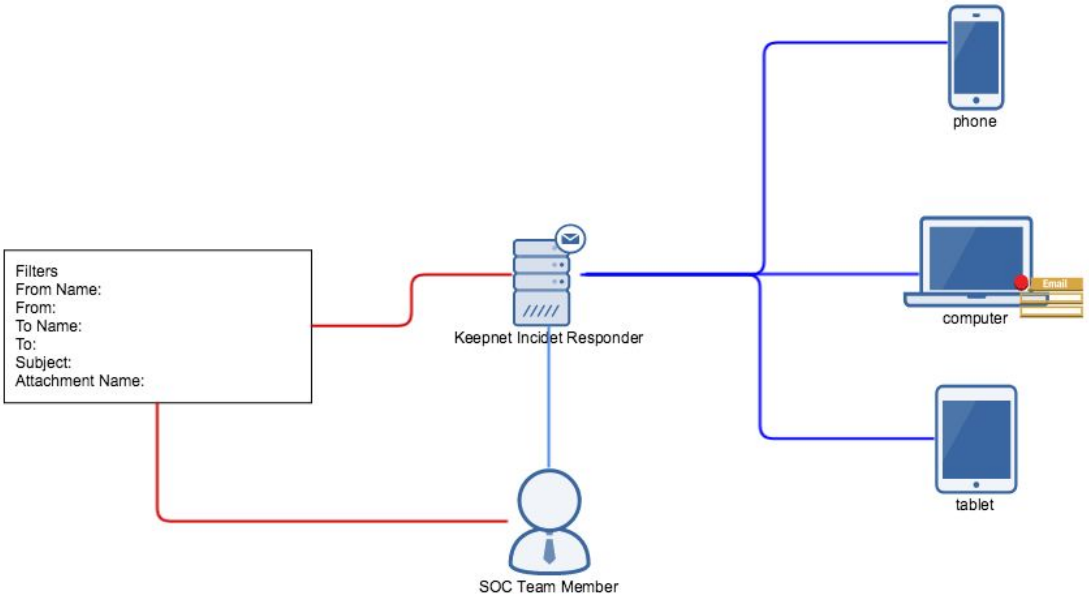
3.5. Logs for SIEM Solutions

Build-in Integrated Services

1. Virustotal: Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans by 56 different Antivirus Engines
2. Zemana Anti-Malware: Zemana is an effective malware, spyware, adware, ransomware, rootkits & bootkits detection service.
3. Trapmine: Trapmine is combination of malware detection and exploit prevention against both known and unknown (0day) threats.
4. Roksit DNS Firewall: Roksit DNS Firewall provides Active / Passive Botnet C&C, malware and phishing url detecting.

5. 3rd Party Services: If you have any threat analyze service like Fireeye, Bluecoat, Palo Alto that we can integrate them to autotomize this analysis actions and save your time.

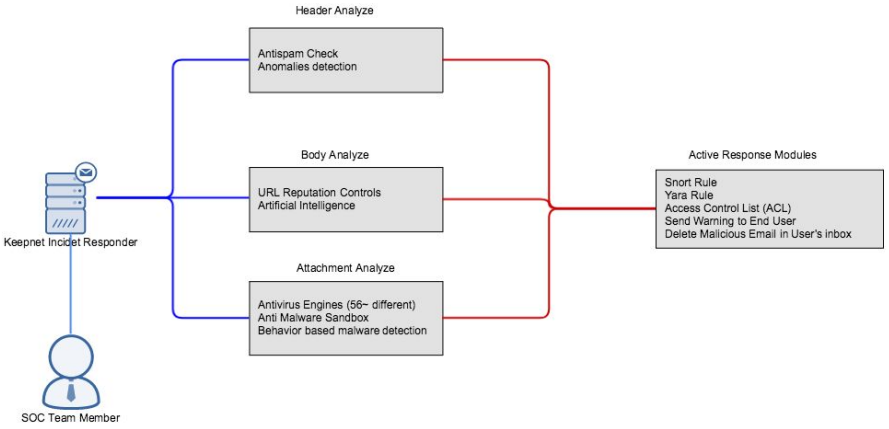
Incident Investigation



- You can search and detect which users the suspicious e-mail belongs to, and take preventive measures with just one click. The SOC / IR Team member can access malicious content and receive preventive measures with any filter that an e-mail can contain, by writing an advanced query, with phishing reporter installed in the e-mail reader.

Active Response

Phishing reporter provides you to destroy malicious e-mail with one click . But in order to detect and prevent the harmful activities that are anticipated in your network, you should pass the necessary rules to Antivirus, Antispam, IPS, SIEM, DLP, Sandboxing products. This subject, which requires serious expertise and consumes hours, is resolved with phishing reporter in seconds with one click, and it allows you to orchestrate with your security solutions.



To help you take precautions, if the email you analyse is suspicious;

Rules	**Description**
Snort Rule	Generate Snort rules that you can use this rules with best-known IPS (intrusion prevention system) to block malicious activity.
Yara Rules	Yara is a tool designed to help malware researchers identify and classify malware samples. It's been called the pattern-matching Swiss Army knife for security researchers (and everyone else). Many of cyber threat prevention tools or services compatible with Yara rules.

Reverse Engineering Support

We provide expert support with our professional phishing and malware analysis team and with the power of other SOC companies around the world that we have agreement. In various SLA time, you have opportunity to get an in-depth analysis of phishing e-mails and malware from a specialized team.

We offer sophisticated malicious software analysis support with SOC teams based UK, USA, Estonia, Bosnia ve Turkey.

Benefits

The traditional protection methods are inadequate. However, this technology offers the most effective cyber attack detection and defense services with multiple alternatives, to protect you against ransomware, spear phishing and 0-day exploitation attacks targeting your email.

Benefits to the security operation center (SOC):

- Cost-Effective: With built-in integrated services, you do not need to invest in any other anti-malware sandbox and anti-exploitation solutions.
- It will reduce the effort that you spend to analyse malicious e-mails for hours.
- Unwanted e-mails can be deleted from the user's e-mail box with information received from the command center.
- It reports which e-mail message is in an e-mail box of users.
- If the existing security measures are inadequate for analysis, detection and prevention, it gives the occasion to benefit from Keepnet's analysis service.

- It provides more effective security measures with integration with third party systems (SIEM, Firewall, DLP etc.)

Direct benefit to email user:

- Employees report aggressive attacks with a single click.
- Early "Phishing" warnings are taken from users and a "sensor" network is created.
- The user is notified of this correct action when he/she clicks the **"Report Phishing"**[1] button in a simulated phishing security test.
- It allows the user to send a suspicious e-mail to analysis services and get a risk score.
- Institution’s security culture strengthens.
- Employees receive immediate feedback that enhances their training.

[1] It is a way of proactively involving users to protect institution's security, where suspicious e-mails are reported by employees. In this way, a culture of awareness constantly evolves against phishing attacks. This service also provides an easy way for end users to report to their IT department and statistical follow up.