Deep Secure: Spear-Phishing Protection

Anatomy of a Spear-Phishing Attack without Deep Secure protection:

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems. Following the social trail, he identifies other people the employee may know.

2. A fake but recognisable email address is created to impersonate a colleague or boss.

A personalised email is sent to the employee from the fake address with a link or attachment.

3. The email passes through the spam filter, AV scanning, sandbox, etc. and arrives at the employee's inbox. The email is opened because they 'know' the sender.

Spear-Phishing is an ever-growing business problem for one key reason: it works.

95% of all attacks on enterprise networks are the result of successful spear-phishing

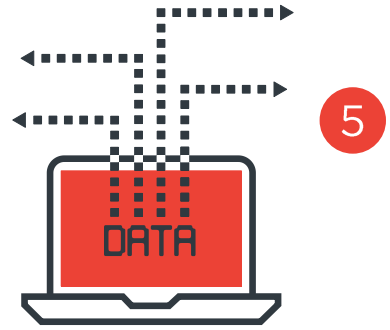
SANS Institute

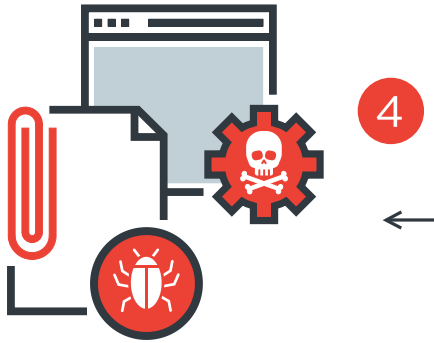
92% of malware is delivered via email

Verizon

70% of targeted attacks use spear-phishing emails

Symantec





5. COMPROMISED!

The hacker uses the compromised computer to infiltrate the corporate network to locate and covertly exfiltrate the target information.

4. A link is clicked, or attachment opened.

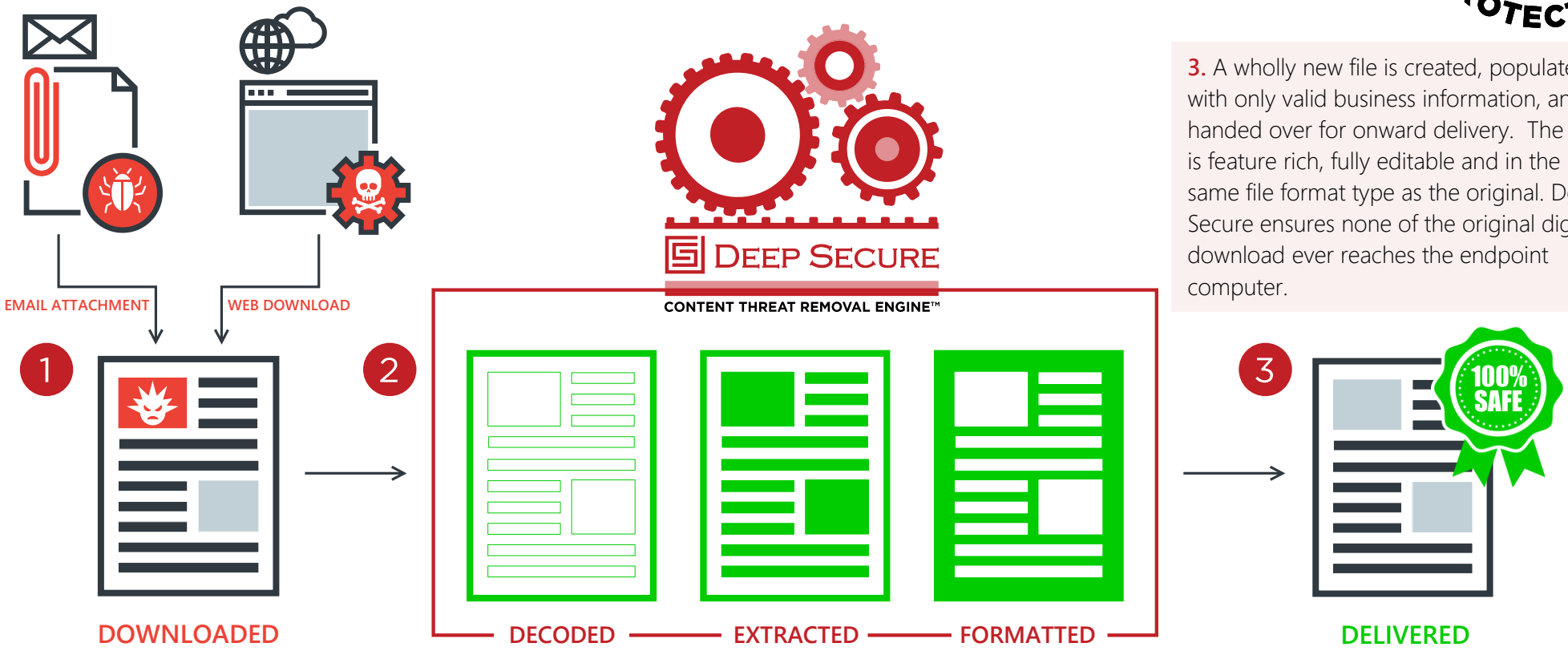
Clicked link causes a malicious document to be downloaded which infects computer/network.

Opened attachment causes malware to infect the computer/network.

Visit us at www.deep-secure.com or contact us e: info@deep-secure.com t: +44 (0) 203 950 5116

Deep Secure: Spear-Phishing Protection

Anatomy of a Spear-Phishing Attack with Deep Secure protection:



1. Deep Secure provides 100% effective protection against Spear-Phishing attacks by removing the threat from malicious email attachments and web document downloads.

Utilising a true zero trust security model, Deep Secure eliminates **all** malware from downloaded content.

2. Working with the existing web and/or email gateway, Deep Secure Content Threat Removal intercepts the downloaded digital content such as documents and images. This content is decoded and just the valid business information is extracted from it. The original file is then discarded, along with any encoding context, unnecessary metadata, active code or malware. Alternatively, the original download can be securely stored for forensic analysis. The extracted business information is then formatted to match the original.

3. A wholly new file is created, populated with only valid business information, and handed over for onward delivery. The file is feature rich, fully editable and in the same file format type as the original. Deep Secure ensures none of the original digital download ever reaches the endpoint computer.

4. PROTECTED!
The target employee's computer is safe.

Visit us at www.deep-secure.com or contact us e: info@deep-secure.com t: +44 (0) 203 950 5116