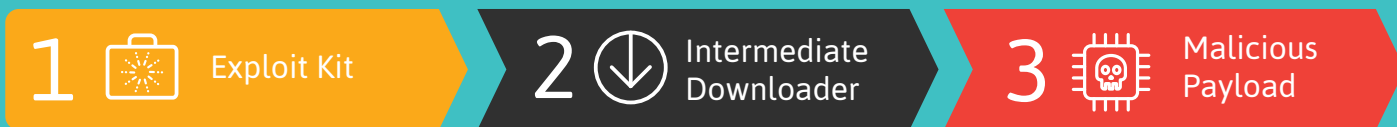


2017 - The Year Malware Went More Evasive

Evasion in Exploit Kits

Targets vulnerabilities in client-side software of website visitors

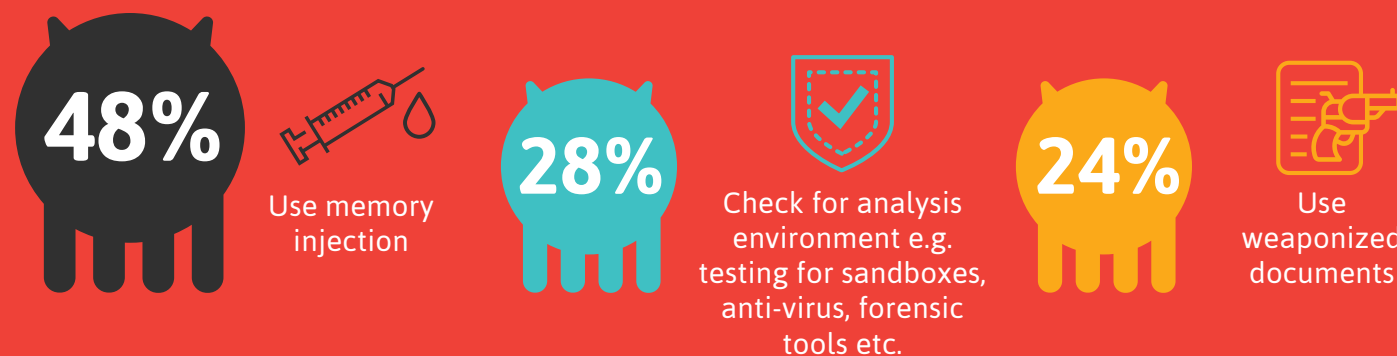
A typical infection path of an exploit kit:



99% of the campaigns tested were evasive either in the exploit kit or the payload phase

Evasive Ransomware

We tested 60 common ransomware families including, Locky, Spora, TeslaCrypt, Cryptomix, Jigsaw and others. Of those employing evasive techniques:



Did you know? Exploit kits were one of the most common ways to spread ransomware in 2017 with over **60%** applying evasive techniques!

The Shadow Brokers Leak Aftermath

First appearing in the summer of 2016, Shadow Brokers published several leaks containing hacking tools from the National Security Agency (NSA), including several zero-day exploits. Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus software, and Microsoft products. Their leaks were responsible for many campaigns, including:

Warning!

Shadow Brokers exploits are increasingly used by commodity malware for propagation.

WannaCry – damages worth **\$4B**



May 2017:

Shadow Brokers leak

ETERNALBLUE/DOUBLEPULSAR/ETERNALROMANCE

NotPetya – damages worth **\$300M** to Maersk, Merck and Fedex alone

Retefe – A Trojan targeting mostly European banking customers, delivered via massive phishing campaigns. It abuses proxy auto-config files to exfiltrate sensitive data.

Adylkuzz Cryptominer