Scalable Web Object Inspection and Malfease Collection

Charalampos Andrianakis

Paul Seymer

Angelos Stavrou

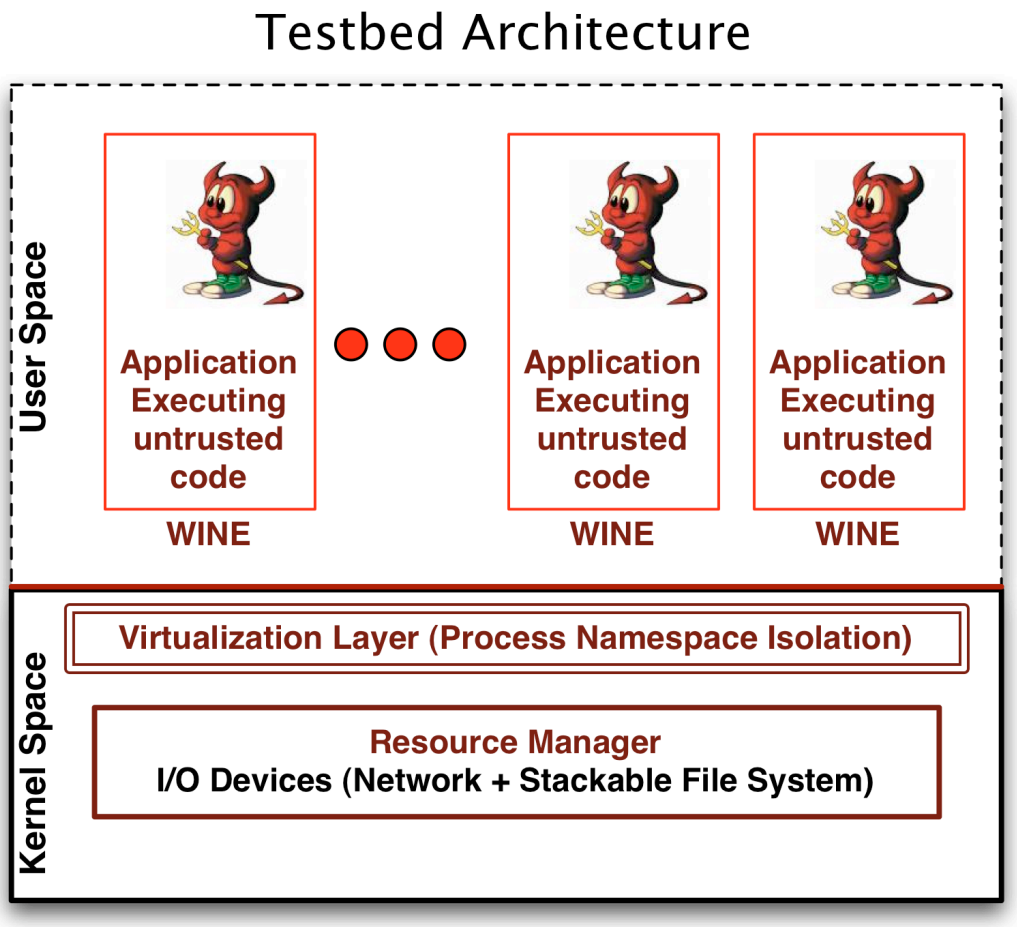
The Problem

- Drive-by download attacks infect thousands of computers daily
- Millions of URLs spread the attacks
- Current technologies based on full system virtualization can't scale

Our Solution

- A URL analysis framework using lightweight virtualization and a modified WINE engine
  - Scans thousands of URLs in parallel
  - Minimizes resource consumption (VM uses less than 300MB of disk, 3MB of memory)
  - Extracts the offending payload and use it for further analysis

Framework Architecture



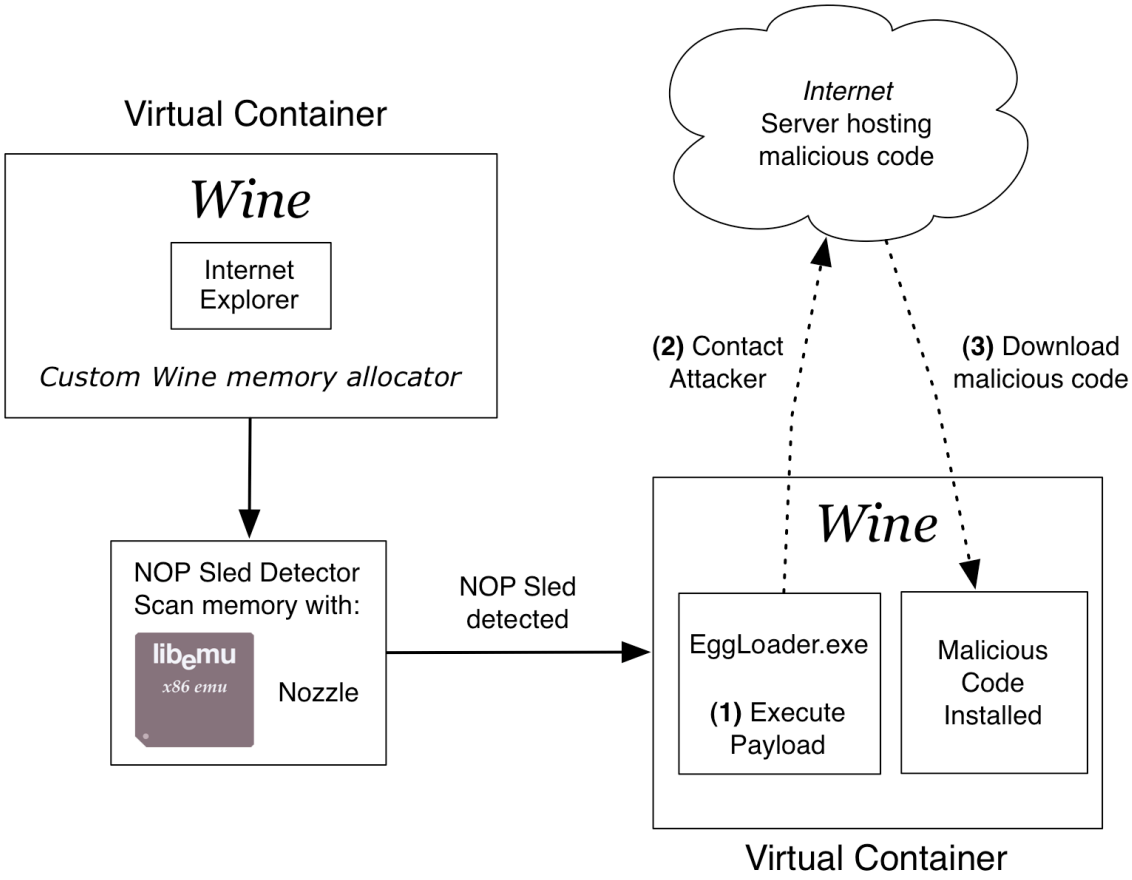
Framework Architecture

- OpenVZ containers with Debian Linux and WINE
- Execute Internet Explorer inside WINE and visit malicious URL
- NOP Sled detector inside WINE detects the attack (heap spray) and extracts the payload

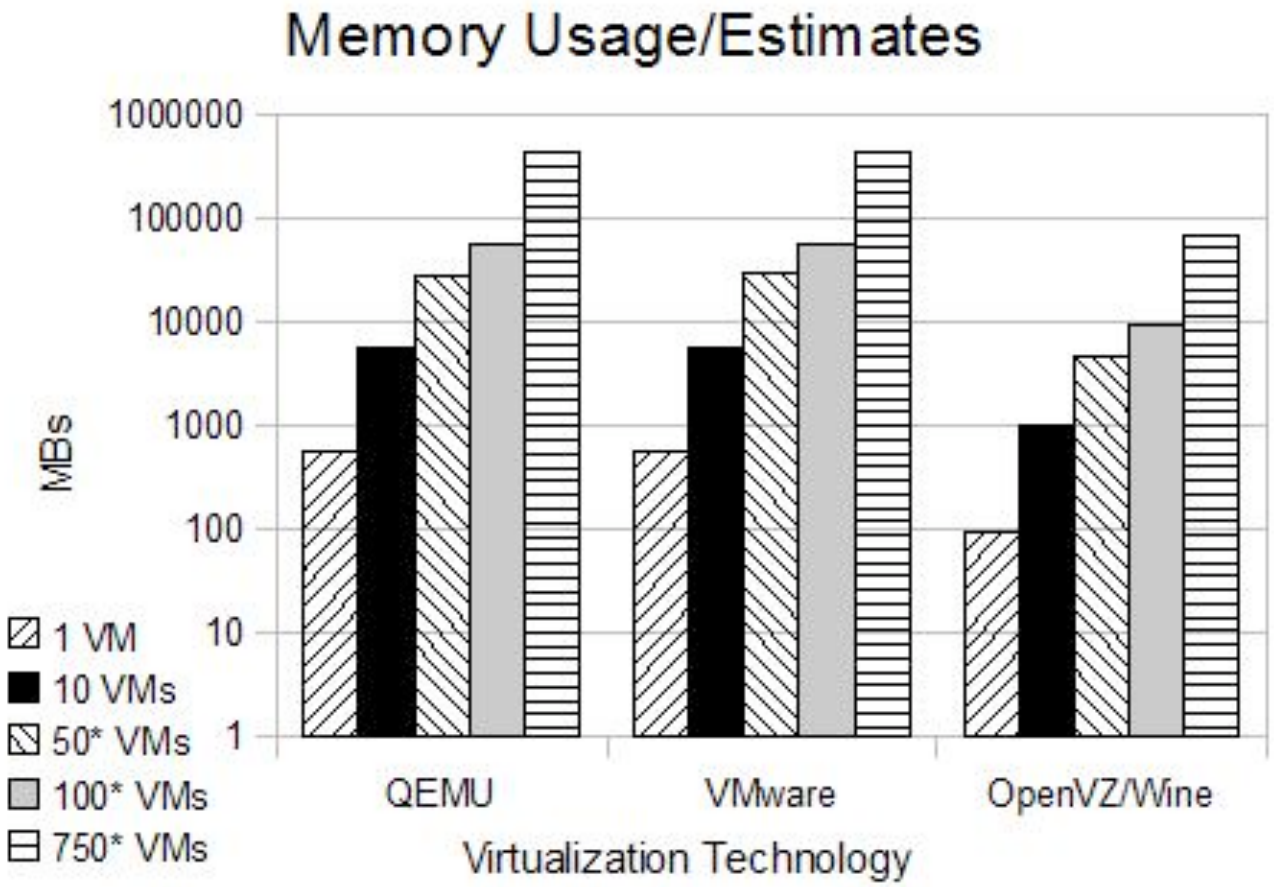
Framework Architecture

- The payload is executed inside WINE with the payload loader
- Malware contacts a remote server and downloads zero day malware binaries

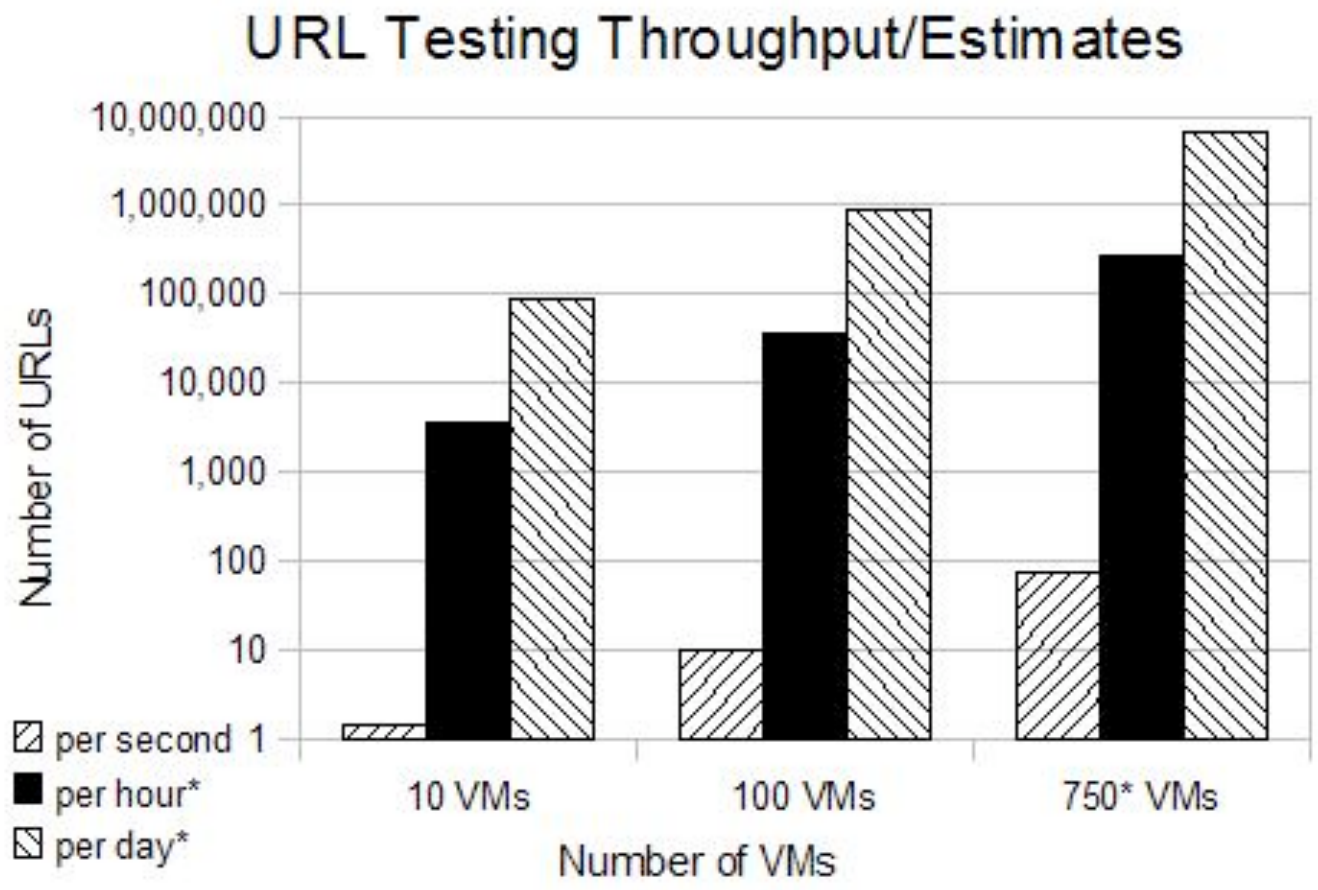
Framework Architecture



Scalability



Scalability



Limitations

- Our solution is limited to detecting heap spray attacks only

- If the offending payload references functions or data in the address space of the browser it can evade detection

Questions ?

Thank you!