uc3m | Universidad Carlos III de Madrid

Bachelor Degree in Computer Science and Engineering
2019-2020

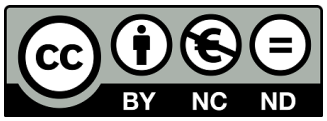
Bachelor Thesis

"ScrambleSuit: A Tool for Evading Malware Analysis Sandboxes using PoW-based Timing Side Channels"

Daniel Aceituno Gómez

Tutored by Antonio Nappa

Leganés, 2020



ABSTRACT

One of the strongest assets used by cybersecurity companies and manufacturers for malware analysis systems are sandboxes, which provide an instrumented and isolated environment to test run unknowns artefacts in the system to detect any potential malicious intent. Malware itself has been evolving due to this by hardening analysis and developing evasion techniques, which are triggered once the environment is detected to be a potential sandbox through environment monitoring. Some of this monitoring techniques are based on fingerprinting, such as red-pills, which look for specific CPU instructions that are known to be poorly emulated while others look for parallel running processes that are known to be present on typical Virtual Machine vendor environments. Due to this detection methods, sandboxes themselves attempt to mitigate possible detection by different means.

In this document a new evasion system is proposed based on Proof-of-Work (PoW) algorithms, which show an asymptotic behaviour with regards to computational cost on different hardware platforms. For this purpose ScrambleSuit is developed, a tool capable of automating the inclusion of virtualized environment detection using PoW for analysis evasion into a malware sample.

A malware sample with the properties added by ScrambleSuit is uploaded to three different public and a locally run sandbox environment, which detected the sample as clean, with the malicious behaviour being hidden by the evasion mechanism, thus demonstrating the validity of Proof-of-Work algorithms as a mechanism for sandbox detection using their execution as a timing side-channel.

Keywords: analysis evasion, Proof-of-Work, side channel attacks, virtual environments, malware, sandboxing