Extension of Malware Dynamic Analysis System Alkanet for Windows Pico Process

Takatsugu Nakayama
Ritsumeikan University
Ibaraki, Osaka, JP
tnakayama@asl.cs.ritsumei.ac.jp

Shoichi Saito
Nagoya Institute of Technology
Nagoya, Aichi, JP
shoichi@nitech.ac.jp

Koichi Mouri
Ritsumeikan University
Ibaraki, Osaka, JP
mouri@cs.ritsumei.ac.jp

ACM Reference Format:
Takatsugu Nakayama, Shoichi Saito, and Koichi Mouri. 2024. Extension of Malware Dynamic Analysis System Alkanet for Windows Pico Process. In . ACM, Kyoto, Japan, 1 page.

1 Introduction

In recent years, Windows has become a major target for malware due to its large user base. In 2016, Microsoft released the Windows Subsystem for Linux (WSL)[2], a subsystem that allows Linux environments to run on Windows. Since WSL is implemented as a Windows subsystem, it offers the advantage of easy integration with Windows, compared to Linux environments created using third-party virtualization software. As WSL can execute Linux binaries (ELF) directly on Windows without conversion, Linux malware can also run on WSL. Given the close relationship between WSL and Windows, malware running on WSL can potentially attack Windows. It has been reported that Bashware, a type of malware running on WSL, can bypass Windows security software[1]. Although dynamic analysis is crucial for understanding malware behavior, there is currently no dynamic analysis system capable of analyzing malware that runs on WSL.

There are two versions of WSL: WSL1 and WSL2. WSL1 runs as a small Windows process called a pico process. The pico process invokes Linux system calls on Windows. These Linux system calls are executed through a different pathway than the system calls (Windows system calls) invoked by the NT process of Windows. Therefore, Alkanet[3], which targets Windows system calls, cannot trace Linux system calls. Figure 1 illustrates the configuration of Alkanet. Alkanet employs two machines to trace system calls: an execution machine and a logging machine.

To enable Alkanet to trace Linux system calls, it is necessary to set hook points at appropriate positions obtain arguments, and return values according to the system calls being traced. To make Alkanet capable of analyzing malware running on WSL1, we enable the tracing of Linux system calls and demonstrate its capability to analyze malware running on WSL1.

2 Tracing WSL1

Because the Windows NT kernel cannot execute Linux system calls, the LXCORE kernel driver is utilized to perform these executions.

Workshop'24, July 2024, Kyoto, Japan

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM

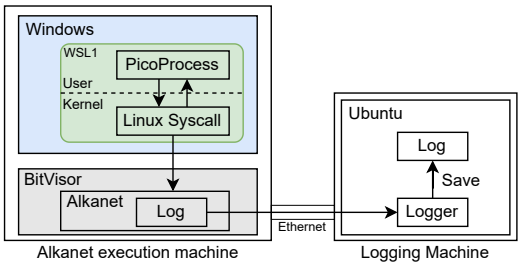

Figure 1: Overview of Alkanet for WSL1

Approximately 300 Linux system calls are implemented within LXCORE, and the pico process executes these calls. Alkanet traces the pico process by setting hook points in LXCORE from the hypervisor. To establish these hook points, it is necessary to avoid the randomization of LXCORE locations by ASLR.

Alkanet can acquire the address of ntdll.dll from the LSTAR MSR, but the address of LXCORE remains unknown. Consequently, hook points are set in ntdll.dll just before the pico process executes a Linux system call. Given that the transition from ntdll.dll to LXCORE occurs immediately before the execution of a Linux system call, Alkanet can ascertain the address of LXCORE at that juncture. This allows Alkanet to set hook points in LXCORE, circumventing ASLR, and thus trace Linux system calls.

3 RESULTS

To demonstrate that malware running on WSL1 can be dynamically analyzed using Alkanet, the operation was verified with a test sample. It acts as a loader, executing scripts by downloading them from a simulated C&C server. Specifically, it was confirmed that system calls such as bind and connect for network communication, openat for file access, and clone and execve for process creation can be traced by Alkanet. Since these system calls are essential to understanding the malware's behavior, their tracing enables dynamic analysis of the malware. The behavior of the test sample was observed with Alkanet, confirming that its behavior can be logged. The behavior of the test sample loading and executing the scripts was monitored with Alkanet. The behavior observed using Alkanet aligned with the behavior of the test sample.

References

[1] Check Point Software Technologies LTD. 2017. Beware of the Bashware: A New Method for Any Malware to Bypass Security Solutions. https://research.checkpoint.com/2017/beware-bashware-new-method-malware-bypass-security-solutions/.
[2] Microsoft. 2022. Windows Subsystem for Linux Documentation. https://learn.microsoft.com/en-us/windows/wsl/.
[3] OTSUKI YUTO, TAKIMOTO EIJI, SAITO SHOICHI, and MOURI KOICHI. 2014. System Call Tracer based on Virtual Machine Monitor for Malware Analysis. *Transactions of Information Processing Society of Japan* 55, 9 (9 2014), 2034–2046.