doi:10.20396/revpibic262018870

XXVI Congresso de Iniciação Científica Unicamp
17 a 19 de outubro Campinas | Brasil

Monitoração de aplicações em ambientes Linux - Linux applications monitoring

Lucas B. Galante*, Marcus F. Botacin, Prof. Dr. Paulo L. de Geus.

Abstract
Linux applications are finding their role on important computer systems. At the same time these systems grow, they become target for malware. Therefore, understanding the security impacts of malware infections on them is essential to allow system hardening and countermeasures development. In this project, we developed tools and systems for evaluation of malicious ELF binaries to present a Linux malware landscape.

Key words:
Malware, Linux, Reverse Engineering

Introduction

Fighting malware is currently a major security task for incident response teams, as such kind of threat is responsible for a myriad of damages, from privacy leaks to financial losses [1]. To provide proper countermeasures, understanding samples behavior is essential.

Recently, Linux systems have grown their market share [2], being present as back-end of many services. At the same time it brings new, benign opportunities, it makes this environment target for malicious authors. Therefore, understanding the impact of Linux malware is essential to protect modern computer systems.

In this project, we proposed evaluating Linux malware to present a panorama of their behaviors. Our goal was to understand their impact over the system as a whole, thus allowing more precise and effective incident response.

Results and Discussion

To evaluate Linux malware, we developed a series of tools that allowed us to trace samples and observe their interactions with the operating system. By making use of static and dynamic analysis, we were able to inspect 5,680 Linux samples and draw a panorama of the threats targeting this environment.

Static analysis revealed samples link many distinct function calls. We classified them into categories, according [3], and identified a prevalence of network and evasion-related functions. When correlated to AV labels, we discover the network prevalence is related to a large number of *backdoor* malware samples.

The data retrieved through static analysis was considered as a lower bound for malicious behaviors, as many samples are distributed in obfuscated ways. We identified 4% were packed, for instance. To overcome obfuscated analysis limits, dynamic analysis procedures were deployed.

Dynamic analysis confirmed most results obtained through static analysis. We observed an increased use of network functions in x64 samples. In addition, it provided a fine-grained view on samples calls. For instance, we have discovered access to the */proc* directory correspond to 40% of all accessed directories. Samples use this directory to access the *passwd* and *shadow* files to retrieve login and credential information,

As most samples are network-powered (over 50% of connection attempts), we analyzed their network traffic to better understand attackers' project decisions. We discovered the samples which most perform connections were network scanners.
Given their presence, observe traffic towards varied Top Level Domains (TLDs), from .com and.net to .br.

Whereas focused on the Linux environment, we were able to compare our results to the ones from malware targeting other platforms, noticeably, to the ones from the Windows environment. Whereas distinct regarding operating system internals, they present comparable, significant potential to cause damage on their target machines.

Conclusions

The performed analysis procedures allowed us to draw a panorma of Linux threats. We discovered the most prevalent system calls, functions and their associated behaviors (*modularization and evasion*). We also performed network traffic analysis and discovered samples rely on the Internet to achieve their malicious goals.

Furthermore, we compared malware samples targeting the Linux O.S. to the ones targeting Windows. We discovered they can cause the same damage extent and present similar characteristics, including the use of anti-analysis tricks.

The presented landscape of Linux malware may contribute for enhancing incident response tools and procedures, as these can be driven on a more targetted way**.**

Acknowledgement

This work was supported by the Brazilian National Counsel of Technological and Scientific Development (CNPq) - PIBIC 2016/2018, process 800295/2016-1.

---

[1] TrendMicro (2017). Erebus linux ransomware: Impact to servers and countermeasures. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures.

[2] Itsfoss (2017). Desktop linux now has its highest market share ever. https://itsfoss.com/linux-market-share/.

[3] Grégio, A. R. A., Afonso, V. M., Filho, D. S. F., Geus, P. L. d., and Jino, M. (2015). Toward a taxonomy of malware behaviors. The Computer Journal, 58(10):2758–2777.