transactions in the basic blockchain, the price of each of the L2 transactions decreases proportionally. This solution is called a rollup, and they mainly differ from each other in the method of forming proof of validity and verification.

Leading today are rollups formed with the help of zero-knowledge proof. This is a field of mathematics, not a specific technology, so there could be countless implementations of it, but primarily it is zkSNARK and zkSTARK.

The main idea is that you can prove something to someone without revealing that "something", declaring only that "something" is true. For example, you can prove that there is a certain amount of money on your bank account without revealing your balance. Or you can prove that there is a penguin in the picture, without revealing where exactly it is.

Retrospectively, zkSNARK and zkSTARK did not aim for broad implementation of zk-proofs, zero disclosure was obtained by them unintentionally, as an addition to succinctness or transparency respectively. However, despite this, they gave an impuls to the development of a new, advanced branch of computer science.

For this reason, I urge not to be prejudiced against any technology, because progress and innovations can not be criminal, only people and their application of the products of progress can be.

References

1. Governing Carbon Markets with Distributed Ledger Technology – Michael Mehling
2. Proofs, Arguments, and Zero-Knowledge - J Thaler

ANTI-VIRUS TOOLS: DETECTING AND PREVENTING MALWARE

Miedviediev A. O., student,
Suknov M.P., PhD, Associate Professor,
Kharkiv National University of Radio Electronics

As cyber threats and malware continue to evolve, the need for effective anti-virus tools becomes crucial. This article provides an overview of various anti-virus tools and their underlying detection and prevention techniques. By understanding the

strengths and limitations of different anti-virus tools, users can make informed decisions in safeguarding their digital assets against malicious software.

Malicious software, known as malware, is a big problem for computer security. To tackle this issue, anti-virus tools have been created to protect people and companies.

Signature-based detection is one of the traditional and widely used techniques in anti-virus tools. It involves comparing the digital signatures of files or code snippets with a database of known malware signatures. This method is effective in detecting known and well-established malware variants. However, it may struggle to detect new and evolving malware strains.

Researchers, including Mihai Christodorescu (2005) and colleagues, have conducted studies to see how well signature-based detection works [1]. In one study, they suggested a new approach called semantics-aware malware detection. This approach improves upon traditional signature-based techniques by also considering the meaning and behavior of malware. The researchers tested their method and found that it improved the detection rates compared to the usual signature-based methods that only rely on specific signatures.

Heuristic-based detection finds new and unknown malware by analyzing file characteristics and behaviors. It looks for patterns and behaviors associated with malware using rules and algorithms. This method is effective for identifying new threats, including zero-day attacks. However, strict rules can result in false positives, misidentifying legitimate files as malware.

Studies have investigated the effectiveness of heuristic-based detection approaches. For instance, Rieck et al. (2008) proposed an approach that combines heuristic rules with machine learning to classify malware behavior [3]. Their work demonstrated the efficacy of combining heuristic rules with machine learning techniques, achieving high detection rates and low false positive rates.

Behavioral analysis observes software behavior to identify suspicious activities that may indicate malware, without relying on signatures or rules. It detects both known and unknown malware, but may require significant computer resources and careful fine-tuning to minimize false positives.

Researchers, Robertson and Vigna (2010), conducted a study to understand more about behavioral analysis [4]. They specifically focused on the structural properties of malware families. By examining the behaviors of different malware samples, they found common patterns and characteristics that can be useful for detecting and categorizing malware. Their study provided valuable insights into understanding the behaviors of malware and improving detection methods.

Machine learning algorithms accurately detect and classify malware by learning from known examples. They offer high detection rates but require powerful computing resources and can be susceptible to advanced malware techniques.

Several studies have explored machine learning-based approaches for malware detection. Kolbitsch et al. (2009) proposed an effective and efficient malware detection approach at the end host using machine learning techniques [2]. Their work demonstrated the feasibility of using machine learning to detect malware with high accuracy and minimal false positives.

Anti-virus tools play a vital role in safeguarding computer systems and data against malware attacks. Signature-based detection, heuristic-based detection, behavioral analysis, and machine learning-based detection are among the techniques employed by these tools. Each approach has its strengths and limitations, and a combination of multiple techniques is often employed to provide comprehensive protection. Ongoing research and development are necessary to enhance the effectiveness of anti-virus tools in combating new and emerging threats.

References

1. Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2005). Semantics-aware malware detection. In Proceedings of the 2005 IEEE Symposium on Security and Privacy (pp. 32-46). IEEE.

2. Kolbitsch, C., Comparetti, P. M., Kruegel, C., Kirda, E., Zhou, X., & Wang, X. (2009). Effective and efficient malware detection at the end host. In Proceedings of the 18th USENIX Security Symposium (pp. 351-366).

3. Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Learning and classification of malware behavior. Journal in Computer Virology, 4(4), 251-261.

4. Robertson, W., & Vigna, G. (2010). An empirical study of the structural properties of malware families. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 626-638).

OVERVIEW OF ML-BASED BOT DETECTION APPROACHES BASED ON SERVER LOG DATA

Holoborodko B.Y., student,
Suknov M.P., PhD, Associate Professor,
Kharkiv National University of Radio Electronics

A significant portion of the Internet traffic on modern websites is generated by bots, which pose a threat to the security, privacy and performance of websites. To develop effective methods for detecting bots and establishing reliable patterns of real user behavior, it is necessary to be able to distinguish and classify traffic. The complexity of this issue lies in the fact that not all bot traffic is bad. Many systems, such as Google or Bing, crawl and index a website with a good purpose - to understand what is on the web page and show it to interested visitors.

We will look at modern methods of detecting bots on websites, and highlight their advantages and disadvantages. We will only consider server-based models that use HTTP request logs, IP addresses, user agents, and user sessions for training and evaluation. That is, we only consider models and approaches based on server-side information, without analyzing mouse or keyboard keystrokes. In addition, we do not consider models based on information collected via JavaScript, as a large number of users use various ad blockers and other applications, which makes it impossible to combine data from the server and the client's browser.

To begin with, let's focus on an approach based on unsupervised learning. The approach proposed in 2020 [2] is based on the use of unsupervised learning (k-means and graduated probabilistic c-means) followed by supervised cluster labeling. The effectiveness of the method proposed by the authors is evaluated using experiments on real e-commerce data under realistic conditions and compared with the effectiveness of