Proposal for a Review paper on Zero-day attacks: asses security landscape and protect corporate network against unknown vulnerabilities

Introduction:

In today’s digital marketplace, there is hardly an organization that does not depend on software or “the internet”. This dependence brings with it a degree of vulnerability. Businesses today are far more likely to have their operations interrupted by cybercriminals than malicious actors in the real world. Zero-day attacks are especially feared because they give hackers a unique opportunity to bypass typical cybersecurity defenses.

A zero-day attack is when hackers release malware before developers have an opportunity to release a fix for the vulnerability—hence zero-day. Zero-day refers to a newly discovered vulnerability in the software. As developers are just finding out about the flaw, patches or security update to resolve the issue, have not been released. In zero-day attacks, software vendors are reactive, not proactive. They can only respond when problems emerge.

This paper describes a contextual misuse approach combined with an anomaly detection technique to detect zero-day cyber-attacks. The contextual misuse detection utilizes similarity with attack context profiles, and the anomaly detection technique identifies new types of attacks using the One Class Nearest Neighbor (1-NN) algorithm. Experimental results on the NSL-KDD intrusion detection dataset have shown that the proposed approach is quite effective in detecting zero-day attacks.

Prevent Zero-day attacks

To keep your computer and data safe, it’s smart to take proactive and reactive security measures.

Your first line of defense is to be proactive by using comprehensive security software, like Norton Security, that protects against both known and unknown threats.

Your second line of defense is to be reactive and immediately install new software updates when they become available from the manufacturer to help reduce the risk of malware infection.

Software updates allow you to install necessary revisions to the software or operating system. These might include adding new features, removing outdated features, updating drivers, delivering bug fixes, and most important, fixing security holes that have been discovered.

Follow this security checklist to be sure you are doing everything you can to help keep your information protected from the security risks associated with zero-day vulnerabilities:

* Keep software and security patches up to date by downloading the latest software releases and updates. Installing security patches fixes bugs that the previous version may have missed.
* Establish safe and effective personal online security habits.
* Configure security settings for your operating system, internet browser, and security software.
* Install a proactive and comprehensive security software to help block known and unknown threats to vulnerabilities.