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

Amla Wijerathne

(MS21908224)

Sri Lanka Institute of Information Technology

MSc. Cyber security 2021

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.

Problem Statement:

Since most of the organization interact with information technology resources, systems or networks in order to support their day to day business operation, technology has become the essential service in the world. Accordingly, cybercrime has been emerging and gradually increasing. Most of the security vulnerabilities can be prevented or detected through automated or manual solutions which will enable the organization to minimize the impact of cyber-attacks. However, the Zero-day vulnerability is an open risk in the world where there is no proper and preventive solution can be implemented till the vulnerability is publicly known.

In fact, the security risk of unknown vulnerabilities has been considered as something unmeasurable due to the less predictable nature of software flaws. This causes a major difficulty to security metrics, because a more secure configuration would be of little value if it were equally susceptible to zero-day attacks. With considering the gravity of this vulnerability, necessity of having in-depth study on the current context and available/possible solutions was impressive to develop this review paper on Zero-day attacks: asses security landscape and protect corporate network against unknown vulnerabilities

Objectives:

Purpose of this having this study is to demonstrate possible and practical solutions which will minimize the risk of zero-day attacks. The followings are the granular view of the review paper objectives;

- Understanding the gravity and current context of the zero-day vulnerability
- Review and identify world-wide zero-day attacks
- Analyze the root-courses and attack vectors
- Identify preventive, detective and corrective control measures

Preliminary Literature Review:

Few research papers were available on similar topics such as review paper on unknown security vulnerabilities, A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities etc. These articles and review papers were mostly discussed on the current context of zero-day attacks and safety measure. However, most of them were not focusing on how this vulnerability has already impacted on business world and mitigants that respective organization had taken and why those security control measures were failure.

Methodology:

The primary research method for this study is literature reviews and measuring the real-world examples and measurement of them. Study will further focus on why available solutions were ineffective in situations where zero-day attacks happened even though the control measures have been properly implemented. While demonstrating these effectiveness and ineffectiveness of such controls and most practical solutions will be reviewed throughout the paper.

References:

k-Zero Day Safety: Measuring the Security Risk of Networks Against Unknown Attacks Lingyu Wang, Sushil Jajodia, Anoop Singhal, Steven Noel

Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks Lingyu Wang, Meng Zhang, Sushil Jajodia, Anoop Singhal, M. Albanese

An Efficient Approach to Assessing the Risk of Zero Day Vulnerabilities- Massimiliano Albanese, Sushil Jajodia, Anoop Singhal, Lingyu Wang

Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero Day Attacks - Meng Zhang, Lingyu Wang, Sushil Jajodia, Anoop Singhal, M. Albanese