zupyak.com

Arash Habibi Lashkari – Amplifying Cybersecurity Research Impact: The Role of Knowledge Mobilization | Zupyak

Patrick-John2

6–7 minutes

“My mother said I must always be intolerant of ignorance but understanding of illiteracy. That some people, unable to go to school, were more educated and more intelligent than college professors.”

- Maya Angelou

Modern times have witnessed a significant rise in malware outbreaks targeting mobile phone users through app stores. These attacks have raised serious apprehensions about the security of these digital marketplaces and the possible risks faced by smartphone users. Many CEOs and executives of major software firms have expressed their growing concern based on this trend. Their observance says that a paramount hike has been witnessed, and hackers seem to be paving a pathway through app stores.

The after-effects of these malware attacks can be overwhelming. Malicious software can snip sensitive personal data, as well as banking information and contact details, which are then either retailed on the dark web or oppressed by attackers. In other cases, ransomware is used to encode the data on a victim's phone, demanding payment for its release.

One of the foremost matters contributing to this flow of malware is the lack of rigorous security checks directed by most app stores. According to Arash Habibi Lashkari, a professor focusing on malware studies at the Canadian Institute for Cybersecurity at the University of New Brunswick, app stores need to reassess their security policies. He highlighted the need for change, stating:

"They need to change their strategy."

Lashkari is among the highly cited researchers in cybersecurity. He is well-recognized for his research in Malware Analysis and in several fields of cyber security, including Intrusion Detection Systems (IDS), Network Traffic, and dark web analysis.

Lashkari's research in 2015 highlighted the vulnerabilities in app stores. Initially, he downloaded 5,000 apps from Google Play and found them all to be legitimate. However, when he repeated the process in 2017, he discovered that over 200 of these apps had been negotiated and turned into malware. This validates how attackers are endlessly finding ways to bypass security measures.

For Encrypted traffic analysis and characterization, Lashari has contributed significantly. He created three datasets: VPN-NonVPN-2015, Tor-NonTor-2016, and Darknet-2020. These datasets laid the foundation for his pioneering work on detecting and characterizing Darknet traffic using Deep Image Learning, which he termed DIDarknet. This modern approach signified a leap forward in understanding and combating threats lurking in the shadows of the internet.

In 2021, he expanded his contributions by acquiring a robust staking ensemble model for darknet traffic classification and characterization. This advanced model promised to augment the accuracy of recognizing malicious activities on the darknet.

Lashkari’s passion to combat cybersecurity threats did not stop with Darknet analysis. In 2016, he ventured into the kingdom of malicious URL detection and categorization, addressing threats like Spam, Phishing, Malware, and Defacement. His work resulted in the creation of the ISCX-URL-2016 dataset, which became a valuable resource for researchers worldwide.

In 2020, he took on another challenge by designing the first-ever DoH (DNS over HTTPS) tunnel analyzer using Time-series classification. This pioneering work resulted in the CIRA-CIC-DoHBrow-2020 dataset, funded by the Canadian Internet Registration Authority. It provided an understanding of the evolving landscape of DNS security and privacy.

In 2021, Lashkari collaborated with Bell Canada to propose a lightweight hybrid data exfiltration and malicious DNS traffic analysis solution. This collaborative effort emphasized the importance of industry partnerships in addressing developing cybersecurity threats effectively.

From 2017 to 2020, Lashari turned his attention to Android malware analysis. Leveraging Machine Learning (ML) and Deep Learning (DL) algorithms, he designed and developed three different Android malware analysis systems. His systematic approach led to the creation of four datasets: AAGM-2017, CIC-AndMal-2017, CIC-InvesAndMal-2019, and CCCS-CIC-AndMal-2020.

Also, in collaboration with the Canadian Centre for Cyber Security (CCCS), he familiarized two novel Deep Learning-based Android malware characterization resolutions—DIDroid and Entroplyzer. These solutions assured to improve the detection and understanding of Android-based threats.

Lashkari's promise to advance cybersecurity prolonged to intrusion detection and characterization systems. He proposed a fast and robust ML-based intrusion detection system, resulting in the CIC-IDS-2017 dataset. Building on this foundation, he extended the project with support from AWS, producing the first and only IDS datasets for Amazon—CSE-CIC-IDS-2018. These datasets have been instrumental in developing effective intrusion detection solutions.

Furthermore, he played an essential role in pointing out the universal issue of Distributed Denial of Service (DDoS) attacks. His contribution, the CIC-DDoS-2019 dataset, covers 12 common DDoS attack types, offering researchers a complete resource to study and mitigate these threats.

In the fastidious sphere of cybersecurity, knowledge mobilization and research impact are supreme. Lashkari’s contributions, from generating invaluable datasets to proposing innovative solutions, have enlarged the field's ability to combat cyber threats. As we move forward, the collaboration between academia, industry, and government entities remains vital in securing our digital world.