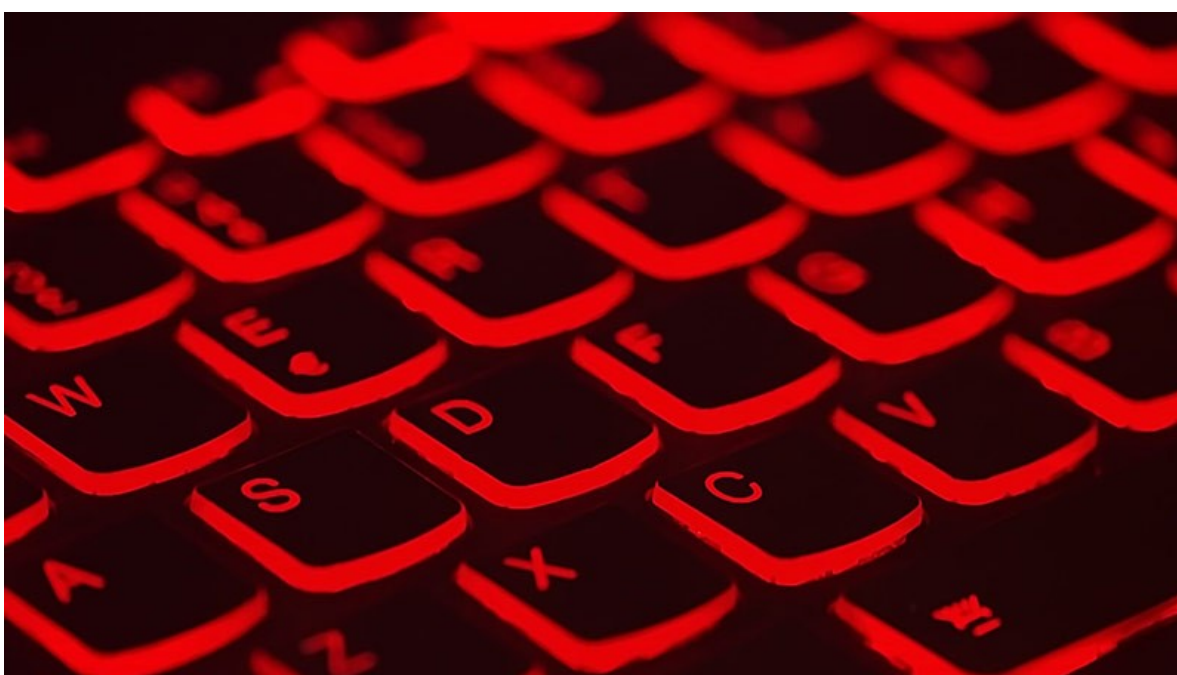


blogs.unb.ca

Cybersecurity research project releases new dataset

3-4 minutes



A new dataset to support the development of real-time cyberattack detectors has been released by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick.

The cybersecurity dataset, named [CICDDoS2019](#), will be used to benchmark Distributed Denial of Service (DDoS) attack detectors.

The dataset has been created by a CIC team and led by Dr. Arash Habibi Lashkari, CIC's research coordinator and assistant professor at UNB's Fredericton faculty of computer science.

"DDoS attacks are a menace to network security," says Dr.

Lashkari. “They aim to exhaust the target networks with malicious traffic. Whilst many statistical methods have already been designed for DDoS attack detection, developing a real-time detector with low computational overhead is still one of the major challenges faced by cybersecurity researchers.”

The existence of well-designed datasets is a vital part of the ongoing evaluation of new detection algorithms and techniques. The latest dataset contains up-to-date, benign versions of common DDoS attacks, allowing researchers and developers to test their solutions.

Since joining UNB five years ago, Dr. Lashkari has been involved in the generation of several datasets such as VPN Traffic (ISCX-VPN-2016), Malicious and Obfuscated URLs (ISCX-URL-2016), Tor Traffic (ISCX-Tor-2017), Android Adware (ISCX-AAGM-2017), Android Malware (CIC-AndMal-2017), and Intrusion Detection and Prevention (CIC-IDS-2017 and CSE-CIC-IDS-2018). These datasets have been used by more than 300 researchers and practitioners in their work.

“This labelled dataset allows cybersecurity researchers to test and evaluate the accuracy and detection rate of their proposed techniques, specifically machine learning-based methods with separate training and testing days,” he explains.

“One of the most critical issues for businesses in the cybersecurity market is the lack of datasets to test their products before they launch,” says Dr. Ali Ghorbani, director of CIC. “CIC’s datasets are widely used by industry as well as universities and researchers from around the globe in testing their security products by creating real-life attack scenarios, capturing malware behaviour patterns,

and monitoring encrypted traffic nature.

“In a simple Google search of ‘cybersecurity datasets’, CIC appears on the top of the results - which demonstrates that CIC meets a pressing need for the cybersecurity market players by making this critical tool available to the private industry.”

Media contact: [Fiona Hendrie](#)