# Anomaly-Based Intrusion Detection for Web Servers

(Technical Report)

# Harboring Malware for Good: Government Purchase of Zero-Days

(STS Research Paper)

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

by

Roman Bohuk

May 7, 2020

# Preface

The proliferation of connected devices opens new attack surfaces and new threats. Despite public awareness of the dangers, cyberattacks are still the fastest-growing crime in the United States, and losses are increasing. How can they be prevented?

Web applications are ubiquitous. They store and process sensitive user data and serve as entry points to corporate networks. Vulnerabilities are still common, and the recent explosion of traffic volume necessitates automated means to stop attacks. Rule-based intrusion detection systems require large, up-to-date signature databases, and they are powerless against new attacks. A non-intrusive anomaly detection system for intercepting and classifying malicious HTTP traffic in real-time is proposed. The application creates a profile of benign traffic to flag suspicious requests and stop attacks that have not yet been observed.

Many states have secretly invested in the development of cyberweapons and capabilities, which inherently rely on zero-day exploits. These are vulnerabilities in popular software that are not disclosed to public or the maintainers of the code, putting every user of the software at risk. Governments therefore face a dilemma: do they release exploits or hide them for a later use? Retaining a zero-day compromises general cybersecurity of the nation, but disclosing information to vendors compromises criminal investigations and offensive cyberoperations. Vulnerabilities must therefore be examined on a case-by-case basis; transparency is also desirable to rebuild public trust.

**List of Contents**