Adversarial Resilient Malware Detector Based on Randomization

Tech ID: 33803 / UC Case 2021-697-0

ABSTRACT

Researchers at the University of California, Davis have developed a machine learning (ML) malware detector based on a randomization technique to prevent cyberattacks on computer systems and networks.

FULL DESCRIPTION

Malware attacks on government and private sector computers, programmable devices, mobile devices, and networks continue to grow, costing trillions of dollars each year, with the sophistication of these malware attacks progressing at an alarming pace. Malware detectors are the primary defense to protect computer platforms from these malicious attacks and typically rely upon profiling benign applications using run-time data, including system calls and hardware performance counters.These types of malware detectors are termed static detectors. Though significant progress has been made in their development to increase their performance and capabilities, the static nature of these cybersecurity systems makes them vulnerable to adversarial cyber-attacks, which integrate ML practices designed to bypass such static ML-based detectors.

Researchers at UC Davis have developed a cost-effective, systems and methods including a random number generator coupled to a randomized machine learning-based malware detector configured for determining changes of settings and selections of parameters, candidate classifiers integrated with the randomized machine learning-based malware detector and configured to be initiated by a random number to avoid transferable learning, a set of feature combinations for random feature selection including monitoring granularity and detection prediction latency and a random number for identifying a set of feature combinations that minimize the overhead and maintain enough variance in data for baffling malware adversarial attacks. For example, the random number generator can reset any number of system operating parameters at millisecond intervals. This technique results in the creation of a moving target that makes it difficult for the malware attacker to penetrate through a constantly changing ML malware detector that is effectively impossible for the attacking malware to infer or train for.

APPLICATIONS

- Malware detection for programmable devices, computers, mobile devices, networks
- More effective cybersecurity protection

FEATURES/BENEFITS

- Improved malicious software detection as compared to current static detectors
- System can be used on multiple operating systems
- Use of a dynamic algorithm to prevent malware attacks
- Algorithm does not slow down computer performance

CONTACT

Andrew M. Van Court
amvancourt@ucdavis.edu
tel: .

INVENTORS

- Homayoun, Houman
- Mohapatra, Prasant
- Rafatirad, Setareh
- Wang, Han

OTHER INFORMATION

KEYWORDS

malware detection,

machine learning,

adversarial learning,

resilience

CATEGORIZED AS

- **Computer**
- Software

RELATED CASES

2021-697-0

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	11,822,651	11/21/2023	2021-697
Patent Cooperation Treaty	Published Application	WO 2023/049017	03/30/2023	2021-697

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Individual Identity Verified Through Device-Free, WiFi Based Framework
- Sensor-Assisted Facial Authentication System For Smartphones
- Energy Efficient Trigger Word Detection via Accelerometer Data

University of California, Davis
Technology Transfer Office
1 Shields Avenue, Mrak Hall 4th Floor,
Davis,CA 95616

Tel:
530.754.8649
techtransfer@ucdavis.edu
https://research.ucdavis.edu/technology-transfer/
Fax:
530.754.7620