aramis
by aizoOn

Scientific Papers 2017-2023

A selection

ICCST 2017 (Spain) - Real-time behavioral DGA detection through machine learning

download paper

In this paper, we report on an effective DGA-detection algorithm based on network monitoring analysis. The proposed method first detects bots looking for the C&C and, then, analyzes resolved DNS requests in the same time interval. The linguistic and semantic features of the collected unresolved and resolved domains are then extracted in order to cluster them and identify specific bots. Finally, clusters are analyzed in order to reduce false positives.

ISC 2018 (UK) - Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic

download paper

In this paper, we report on an effective fast flux detection algorithm based on the passive analysis of the DNS traffic of a corporate network. The proposed method is based on the near-real-time identification of different metrics that measure a wide range of fast flux key features; the metrics are combined via a simple but effective mathematical and data mining approach.

MALCON 2019 (USA) - DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach

download paper

This paper proposes an effective covert channel detection method, based on the analysis of DNS network data passively extracted from a network, employing a machine learning module and the extraction of specific anomaly indicators able to describe the problem at hand.

ITASEC 2020 (Italy) - DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach

download paper

The paper proposes a technique for covert channel detection, based on the analysis of DNS data: the approach is based on a machine learning module and on specific anomaly indicators able to describe the problem at hand.

aramis
by aizoOn

Scientific Papers 2017-2023

A selection

ITASEC 2021 - Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic

download paper

The paper proposes an effective method for detection of fast flux attacks, based on the analysis of DNS traffic: the technique is based on the identification of different metrics able to describe the characteristics of this type of attack through the use of a data mining approach and statistics.

ITASEC 2021 - Towards an Automated Pipeline for Detecting and Classifying Malware through Machine Learning

download paper

The paper proposes an approach for classifying Windows Portable Executables (PEs); in particular, given a PE sample the proposed method involves first a classification phase between good and malicious and then it identifies the type of threat, the family and malware behaviour.

CISDA 2021 & ITASEC 2022 - Near-real-time Anomaly Detection in Encrypted Traffic using Machine Learning Techniques

download paper

The paper proposes an analytics monitoring encrypted traffic flows and extracting meaningful characteristics in order to identify possible attacks and anomalies, combining the use of machine learning with a statistical approach.

OL2A 2023 - PhishVision: a Deep Learning based Visual Brand Imperson-tion Detector for Identify-ing Phishing Attacks

download paper

The paper proposes a framework for visually detecting phishing websites, by identifying the main logo that characterizes web pages under analysis. PhishVision has been designed and implemented to provide Security Operation Center analysts with a phishing detection service that works in near real time.

JCP 2023 - Towards a Near-real-time Protocol Tunneling Detector based on Machine Learning Techniques

The paper proposes a protocol tunneling detector prototype which inspects, in near real time, a company's network traffic using machine learning techniques. The detector monitors unencrypted network flows and extracts features to detect possible occurring attacks and anomalies, by combining machine learning and deep learning.