

Research @ Botacin's Lab

Marcus Botacin¹

¹Texas A&M University (TAMU)
botacin@tamu.edu

Topics

1 Research Projects

- Offensive Security

- Offensive-Defensive Security
- Defensive Security

Topics

1

Research Projects

● Offensive Security

- Offensive-Defensive Security
- Defensive Security

Automated Attack Generation Using LLM models

GPThreats-3: Is Automatic Malware Generation a Threat?

Marcus Botacin
Texas A&M University
botacin@tamu.edu

Abstract—Recent research advances introduced large textual models, of which GPT-3 is state-of-the-art. They enable many applications, such as generating text and code. Whereas the model's capabilities might be explored for good, they might also cause some negative impact: The model's code generation capabilities might be used by attackers to assist in malware creation, a phenomenon that must be understood. In this work, our goal is to answer the question: Can current large textual models (represented by GPT-3) already be

attackers could use the models [10]. To contribute to this debate, we present an evaluation of the model's capabilities from the attacker's perspective. We explore how the models could assist attackers in many tasks, from the entire malware creation to the addition of anti-analysis techniques to existing code, and the automatic creation of malware variants via a scriptable procedure.

We investigated model capabilities by creating custom queries that were performed via OpenAI's public

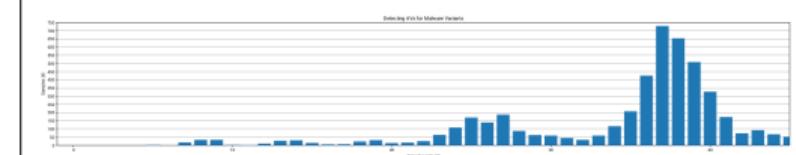


Figure 1:

Malware variants detection rates vary according to the functions used to implement the same behaviors.

Topics

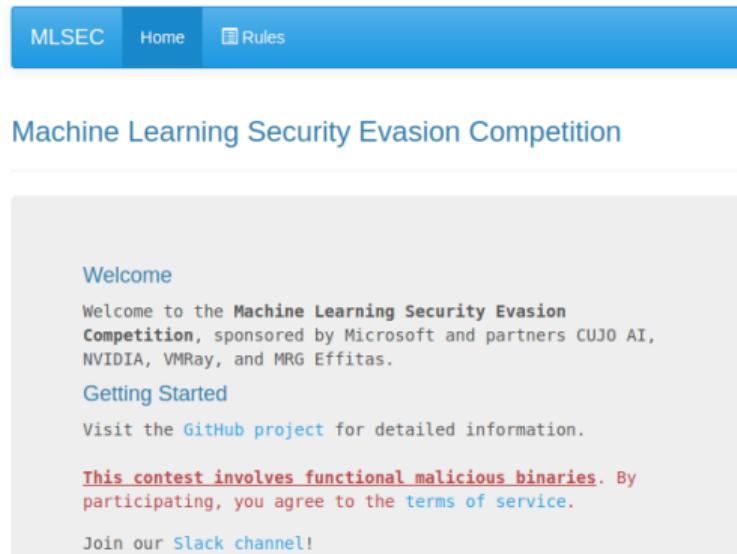
1

Research Projects

- Offensive Security

- Offensive-Defensive Security
- Defensive Security

Adversarial ML in Practice



MLSEC Home Rules

Machine Learning Security Evasion Competition

Welcome

Welcome to the Machine Learning Security Evasion Competition, sponsored by Microsoft and partners CUJO AI, NVIDIA, VMRay, and MRG Effitas.

Getting Started

Visit the [GitHub project](#) for detailed information.

[This contest involves functional malicious binaries](#). By participating, you agree to the [terms of service](#).

Join our [Slack channel](#)!

Figure: mlsec.io



CUJO AI CYBERSECURITY FOR NETWORK OPERATORS

Luckily, everyone understood this mistake and accepted the new results.

Analysis of the winning solutions

Please check out all the great write-ups from the participants.

First place in the attacker track and second at the defender track

<https://secret.inf.ufpr.br/2020/09/29/adversarial-malware-in-machine-learning-detectors-our-mlsec-2020-secrets/>

The previous one, but white-paper format, defender track only

<https://ieeexplore.ieee.org/document/8636415>

Figure: <https://cujo.com/machine-learning-security-evasion-competition-2020-results-and-behind-the-scenes/>

Topics

1

Research Projects

- Offensive Security

- Offensive-Defensive Security
- **Defensive Security**

Hardware-Assisted Attack Detectors



The screenshot shows the NSF website's award search results. The main content area displays the following details for an award:

NSF Org:	CNS Division Of Computer and Network Systems
Recipient:	TEXAS A&M ENGINEERING EXPERIMENT STATION
Initial Amendment Date:	July 18, 2023
Latest Amendment Date:	July 18, 2023
Award Number:	2327427
Award Instrument:	Continuing Grant

On the left sidebar, there are links for 'Awards', 'Search Awards', 'Recent Awards', 'Presidential and Honorary Awards', 'About Awards', 'How to Manage Your Award', 'Grant General Conditions', and 'Cooperative Agreement Conditions'.

Source: https://www.nsf.gov/awardssearch/showAward?AWD_ID=2327427



The screenshot shows the Texas A&M University Engineering website. The main content area features a news article with the following details:

Home | **News** | Innovative Approach: Detecting Malware Through Hardware-integrated Protection

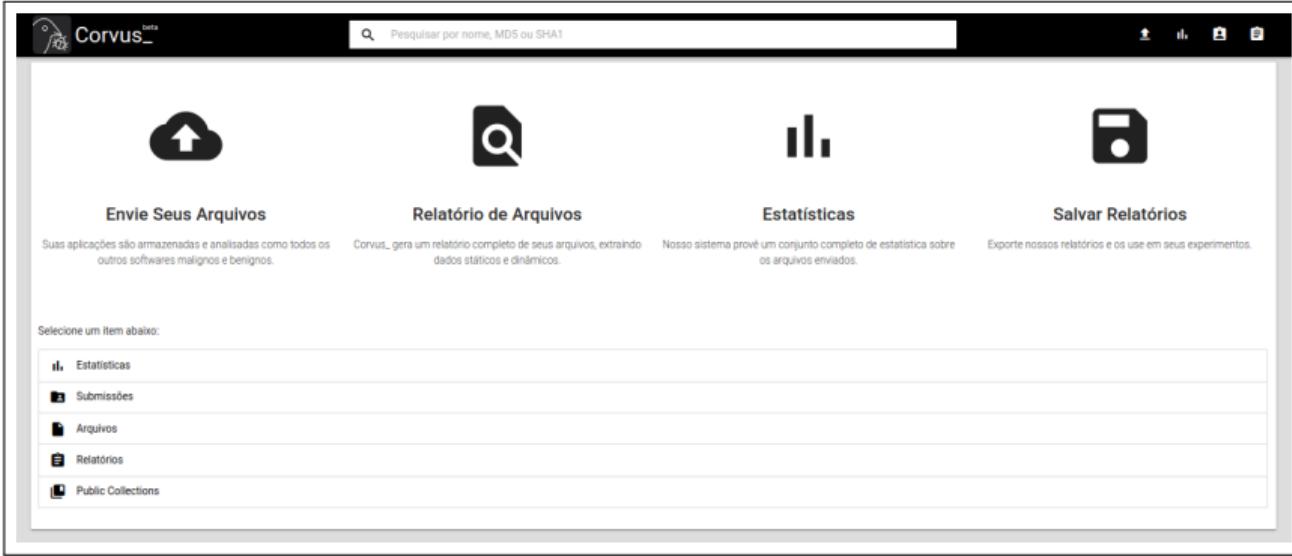
Innovative Approach: Detecting Malware Through Hardware-integrated Protection

August 14, 2023 | By Justin Agan

Computer Science and Engineering | Research

Source: tx.ag/ft0dCdj

Threat Intelligence Platforms



The screenshot shows the Corvus_ beta web interface. At the top, there is a logo of a raven, a search bar with the placeholder "Pesquisar por nome, MD5 ou SHA1", and a user menu with icons for profile, settings, and help. Below the header, there are four main sections: "Envie Seus Arquivos" (Upload Your Files) with a cloud icon, "Relatório de Arquivos" (File Report) with a magnifying glass icon, "Estatísticas" (Statistics) with a bar chart icon, and "Salvar Relatórios" (Save Reports) with a file icon. Each section has a brief description. Below these sections is a sidebar titled "Selecione um item abaixo:" (Select an item below:) containing a list of items with icons: "Estatísticas", "Submissões", "Arquivos", "Relatórios", and "Public Collections".

Corvus_

Pesquisar por nome, MD5 ou SHA1

Envie Seus Arquivos

Relatório de Arquivos

Estatísticas

Salvar Relatórios

Selecione um item abaixo:

- Estatísticas
- Submissões
- Arquivos
- Relatórios
- Public Collections

Thanks!

botacin@tamu.edu