Research @ Botacin's Lab

Marcus Botacin[1]

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

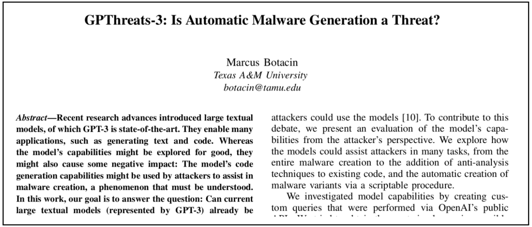
Topics

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

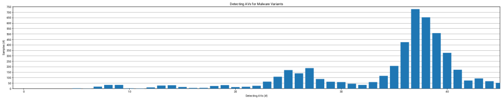


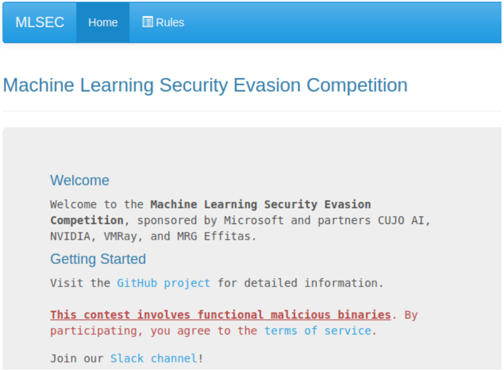
Figure 1: **Malware variants detection rates** vary according to the functions used to implement the same behaviors.

Source: `https://ieeexplore.ieee.org/document/10188649`
GANs: `https://www.youtube.com/watch?v=1wzeHzUG3l4`
CoPilot: `https://www.youtube.com/watch?v=6P92ayn2qt0`
Integration: `https://www.youtube.com/watch?v=p85EbQPREWk`

Topics

1. Research Projects
   - Offensive Security
   - Offensive-Defensive Security
   - Defensive Security

Adversarial ML in Practice



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.

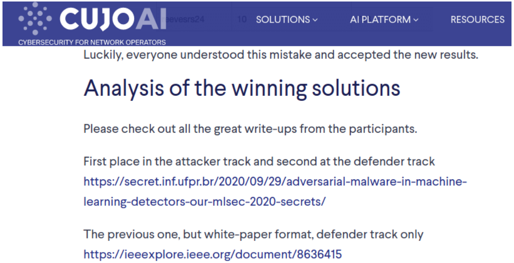
Getting Started

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`



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

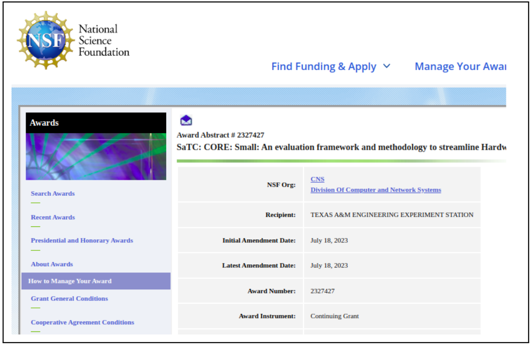
Figure: `https://cujo.com/machine-learning-security-evasion-competition-2020-results-and-behind-the-scenes/`

Framework: `https://www.youtube.com/watch?v=p2gubquZbDE`

Topics

1. Research Projects
   - Offensive Security
   - Offensive-Defensive Security
   - Defensive Security

Hardware-Assisted Attack Detectors

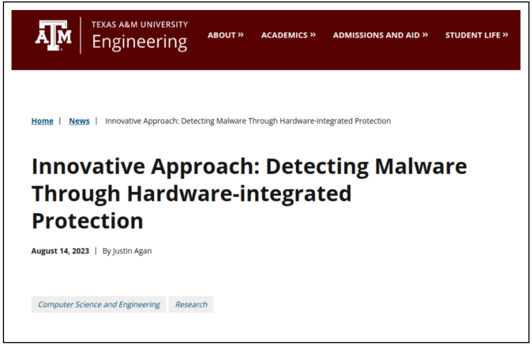


Award Abstract # 2327427

SaTC: CORE: Small: An evaluation framework and methodology to streamline Hardw

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

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


TEXAS A&M UNIVERSITY
Engineering
ABOUT »
ACADEMICS »
ADMISSIONS AND AID »
STUDENT LIFE »
Home | News | Innovative Approach: Detecting Malware Through Hardware-integrated Protection

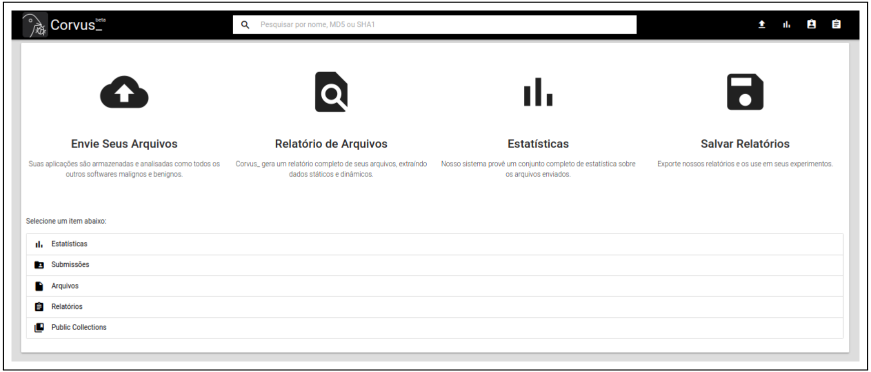
Innovative Approach: Detecting Malware Through Hardware-integrated Protection

August 14, 2023 | By Justin Agan

Computer Science and Engineering Research

Source: `tx.ag/ft0dCdj`

Threat Intelligence Platforms



Corvus_ beta

Pesquisar por nome, MD5 ou SHA1

Envie Seus Arquivos

Suas aplicações são armazenadas e analisadas como todos os outros softwares malignos e benignos.

Relatório de Arquivos

Corvus_ gera um relatório completo de seus arquivos, extraindo dados státicos e dinâmicos.

Estatísticas

Nosso sistema provê um conjunto completo de estatística sobre os arquivos enviados.

Salvar Relatórios

Exporte nossos relatórios e os use em seus experimentos.

Selecione um item abaixo:

- Estatísticas
- Submissões
- Arquivos
- Relatórios
- Public Collections

Sandbox: `https://www.youtube.com/watch?v=C2-6Xg44ge4`

Thanks!

botacin@tamu.edu