Vilniaus universitetas

VEIKLOS ATASKAITA

Mašininiu mokymusi grindžiami metodai apgaulingoms ir obfuskuotoms kenkėjiškoms programoms generuoti stiprinant kibernetinį saugumą.

Doktorantūros pradžios/pabaigos metai: 2023-2027
Studijų metai: 2023/2024 pirmas pusmetis

Doktorantas: Juozas Dautartas
Vadovas: Doc. Dr. Viktor Medvedev

Studijų planas ir jo vykdymo suvestinė

Vilniaus universitetas

Studijų metai	Egzaminai [1]	
	Planas	Įvykdyta
I (2023/2024)	**3**	**1**
II (2024/2025)	1	
III (2025/2026)		
IV (2026/2027)		
Iš viso:	4	1

Studijų metai	Dalyvavimas konferencijose				Publikacijos					
	Tarptautinėse [2]		Nacionalinėse [3]		Su citav. rodikliu [4]			Be citav. rodiklio [5]		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta [6]	Būklė [7]	Planas	Įvykdyta [6]	Būklė [7]
I (2023/2024)				**1**						
II (2024/2025)			1							
III (2025/2026)	1				1			1		
IV (2026/2027)	1				1					
Iš viso:	2		1	1	2			1		

Ataskaitinio pusmečio darbo planas ir jo vykdymo suvestinė

Vilniaus universitetas

Egzaminai 2023/2024 (I pusmetis)		
Planas	**Įvykdyta**	**Būklė**
Mašininis mokymasis, I ketv.	Mašininis mokymasis 2024 m. kovo 7 d.	Išlaikytas

Dalyvavimas konferencijose 2023/2024 (I pusmetis)		
Planas	**Įvykdyta**	**Konferencijos tipas**
DAMSS: 14th conference on data analysis methods for software systems, Druskininkai, Lietuva, Lapkričio 30 - Gruodžio 2, 2023	**Obfuscation and evasion techniques for red team assessments** 2023 m. lapkričio 30 – gruodžio 2 d., Lietuva Autoriai: Dautartas, Juozas; Budžys, Arnoldas; Medvedev, Viktor.	Nacionalinė

Publikacijos 2023/2024 (I pusmetis)			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos tipas**

Tyrimų objektas

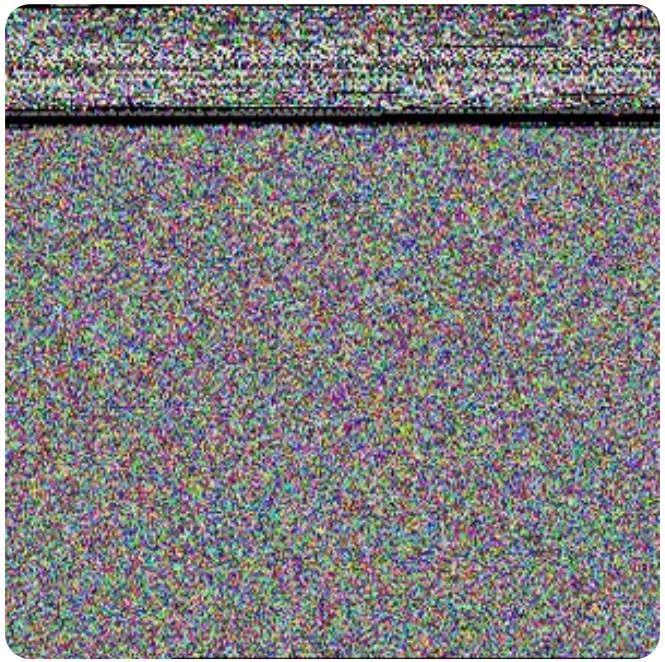
Mašininio mokymosi algoritmai C2 sistemų agentams (kenkėjiškoms programoms) generuoti ir obfuskuoti.

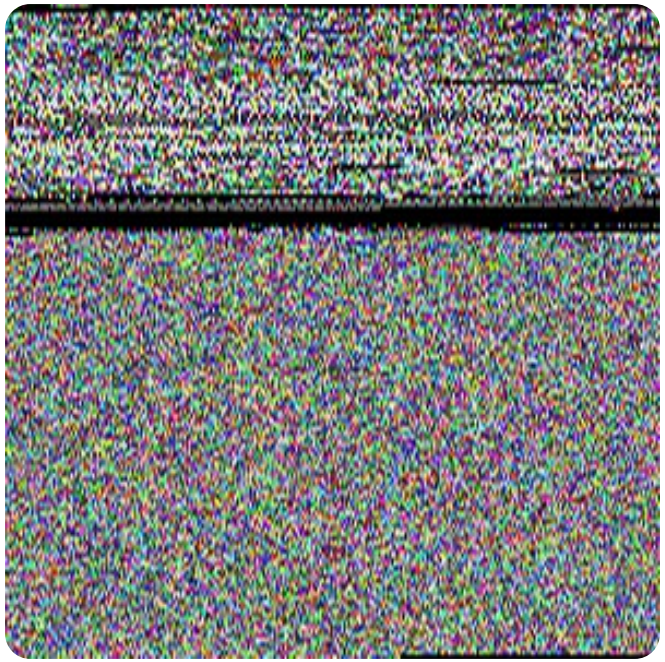
Tikslas

Pasiūlyti ir ištirti naują kenkėjiškos programinės įrangos generavimo metodą, skirtą veiksmingai išnaudoti mašininiu mokymusi pagrįstų kenkėjiškų programų aptikimo sistemų pažeidžiamumą, siekiant padidinti kibernetinių grėsmių atsparumą ir pagerinti bendrą jų aptikimo tikslumą ir patikimumą.

Uždaviniai

- Atlikti išsamią analitinės literatūros apžvalgą, siekiant nustatyti esamus mašininio mokymosi metodus ir būdus, skirtus kenkėjiškoms programoms aptikti, klasifikuoti ir generuoti kenkėjiškas programas.
- Analizuoti antivirusinių ir galinių įrenginių aptikimo ir reagavimo (angl. Endpoint Detection and Responce, EDR) sistemų kenkėjiškos programinės įrangos aptikimo mechanizmus, siekiant suprasti kenkėjiškos programinės įrangos klasifikavimo ypatybes.
- Įvertinti ir išskirti pagrindinius kenkėjiškos programinės įrangos požymius, turinčius įtakos jų aptikimui, siekiant pagerinti kenksmingų programų klasifikavimo tikslumą.
- Sukurti naują arba modifikuoti esamą kenkėjiškų programų (angl. Command and Control framework agents) generavimo metodą, kuriuo siekiama sukurti klaidinančius ir sunkiai aptinkamus C2 sistemų agentų pavyzdžius, galinčius klaidinti mašininiu mokymusi pagrįstus kenkėjiškų programų aptikimo modelius.
- Įvertinti sugeneruotus kenkėjiškų programų pavyzdžius, naudojant įvairius kenkėjiškų programų aptikimo sprendimus ir mašininiu mokymusi grindžiamas kibernetinio saugumo sistemas.
- Ištirti esamas ir pasiūlyti naują strategiją, kaip padidinti mašininio mokymosi modelių atsparumą priešiškoms atakoms.





Per pusmetį gauti rezultatai

- Išanalizuoti kenkėjiškos programinės įrangos statiniai ir dinaminiai aptikimo metodai.
- Dalyvauta įvairiuose tarptautiniuose renginiuose ir kibernetinio saugumo pratybose, kur įgauta ir surinkta daug naudingų žinių ateityje vygdomiems tyrimams.
- Išbandyti klasikiniai mašininio mokymosi algoritmai (Random forests ir CNN) kenksmingo programinio kodo aptikimui.

Kito pusmečio darbo planas

- Išlaikyti du egzaminus: Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika ir Gilieji neuroniniai tinklai.
- Atlikti mašininio mokymosi metodų, skirtų kenkėjiškų programų aptikimui, klasifikavimui ir obfuskavimui (maskavimui), analitinę apžvalgą.
- Identifikuoti (nustatyti) mokslines problemas, susijusias su kenkėjiškos programines įrangos generavimu, aptikimu ir klasifikavimu kibernetinio saugumo kontekste taikant mašininio mokymosi metodus.

KLAUSIMAI

Juozas Dautartas
juozas.dautartas@mif.stud.vu.lt