ČESKÉ
VYSOKÉ
UČENÍ
TECHNICKÉ
V PRAZE

Stratosphere Lab

Arming Malware with GANs

•••

Maria Rigaki
maria.rigaki@aic.fel.cvut.cz
🐦 @mrigaki

Background Information

- PhD student at CVUT in Prague (advisor: Sebastian Garcia)
- Member of the Stratosphere Lab
- Machine Learning and Security
- Background in Software Development and Systems Engineering

What is this talk about?

- It is NOT about guns!

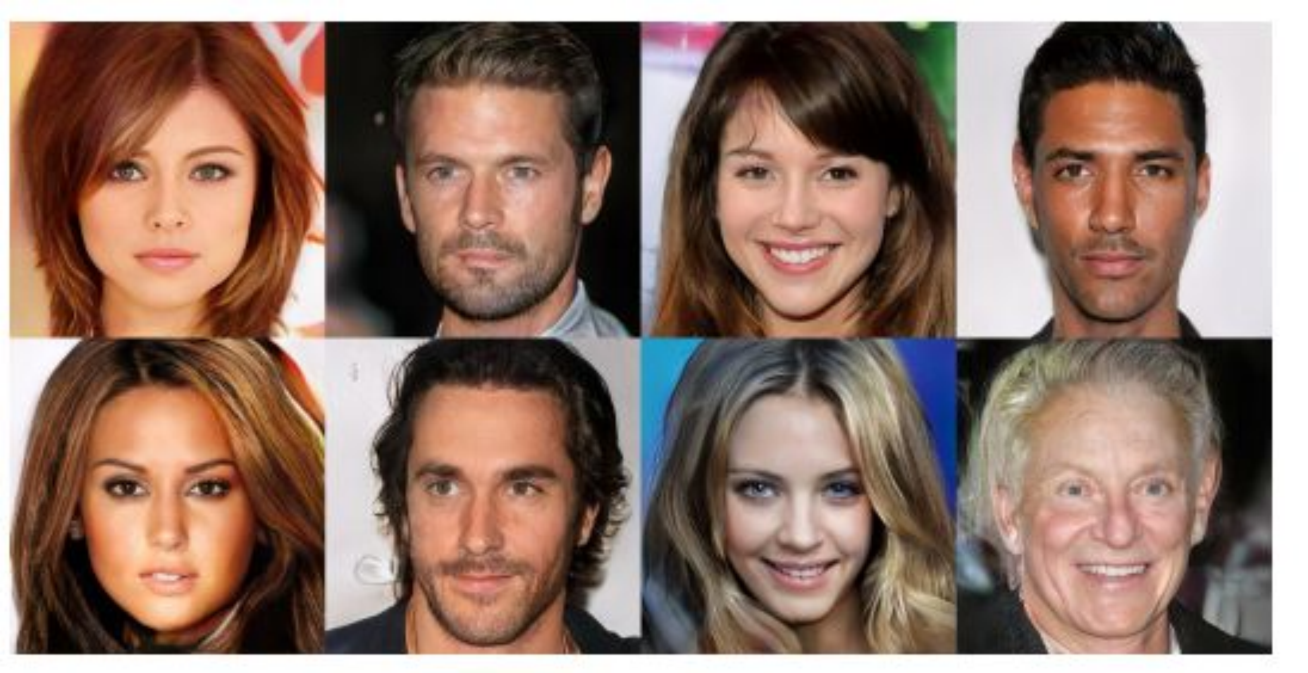
- Work based on our paper: “Rigaki M., Garcia S., *Bringing a GAN to a knife-fight: Adapting Malware Communication to Avoid Detection*”

- High level view of Generative Adversarial Networks
- An example of using GANs in a Network Security application

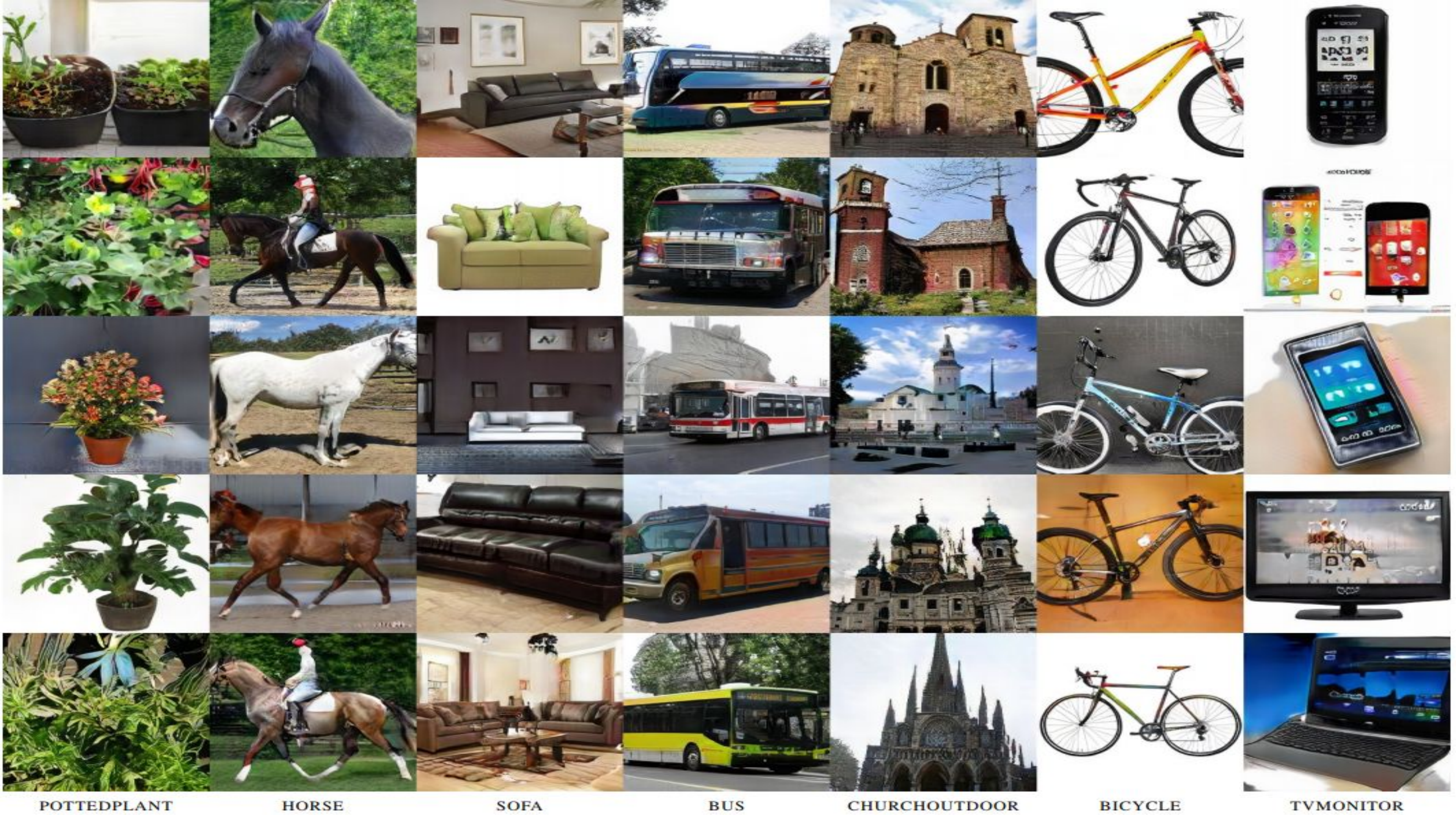
What are we trying to do?

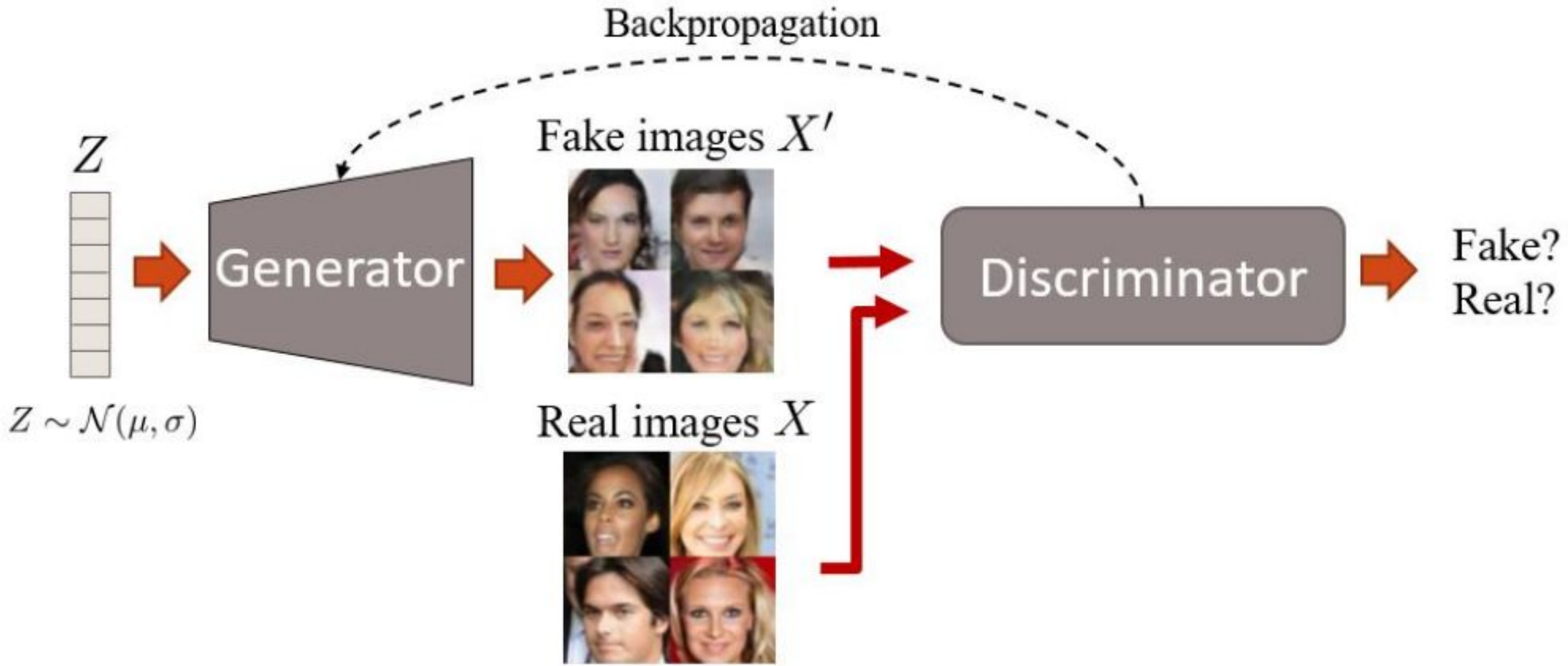
Can we use GANs to modify malware C&C traffic to mimic normal network traffic, in order to evade detectors while the communication channel remains effective?

Generative Adversarial Networks (GANs)



Karras, T., Aila, T., Laine, S., & Lehtinen, J. (2017). Progressive growing of gans for improved quality, stability, and variation. arXiv preprint arXiv:1710.10196.


POTTEDPLANT
HORSE
SOFA
BUS
CHURCHOUTDOOR
BICYCLE
TVMONITOR



http://guimperarnau.com/blog/2017/03/Fantastic-GANs-and-where-to-find-them

Dataset

- Network captures of two Facebook users chatting for a day
- Extracted the Facebook related netflows
- Features: ***duration***, ***byte size*** and ***time between consecutive flows***
- Treated the data as time series
- Detector behavioral model

Malware

- RAT: https://github.com/fluproject/flu
- Client in C#, web server in php
- Client C&C periodic actions:
  a. checks if server is online,
  b. connects to the server & registers,
  c. downloads a list of commands to execute
- HTTP GET requests
- Adapted ***duration***, ***byte size*** and ***time between consecutive flows***

Flu Project
fluproject

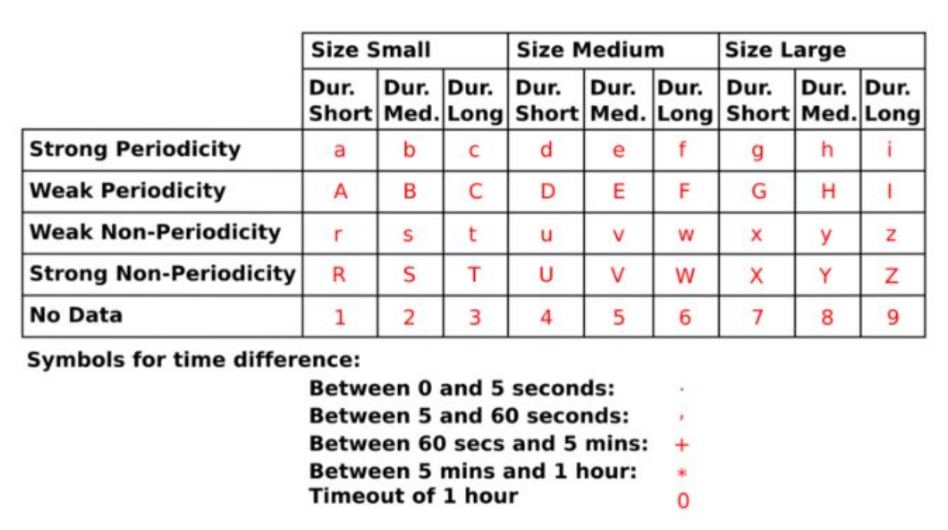
Flu Project es una comunidad hacker ética gestionada por Pablo Gonzalez y Juan Antonio Calles.

@fluproject
info@flu-project.com
http://www.flu-project.com

Detector

- Stratosphere IPS (SLIPS) https://www.stratosphereips.org/stratosphere-ips-suite
- Behavior-based detection
- Does not depend on static signatures / IOCs
- Models netflow characteristics such as periodicity, size, duration of flows
- Set to detect Facebook chat traffic

88*y*y*i*H*H*H*y*0yy*H*H*H*y*y*y*y*H*h*y*h*h*H*H*h*H*y*y*y*H*

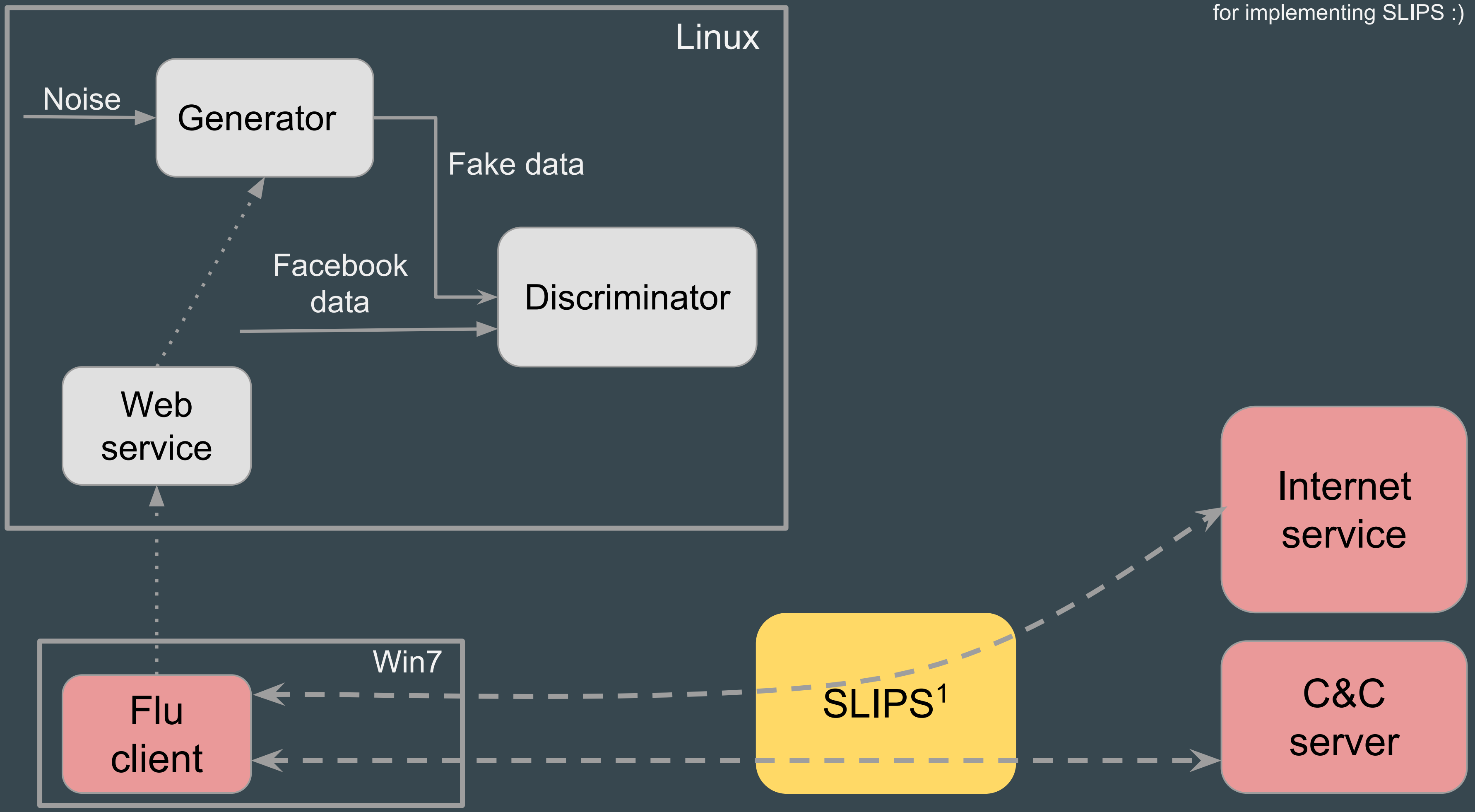


	Size Small			Size Medium			Size Large		
	Dur. Short	Dur. Med.	Dur. Long	Dur. Short	Dur. Med.	Dur. Long	Dur. Short	Dur. Med.	Dur. Long
Strong Periodicity	a	b	c	d	e	f	g	h	i
Weak Periodicity	A	B	C	D	E	F	G	H	I
Weak Non-Periodicity	r	s	t	u	v	w	x	y	z
Strong Non-Periodicity	R	S	T	U	V	W	X	Y	Z
No Data	1	2	3	4	5	6	7	8	9

Symbols for time difference:

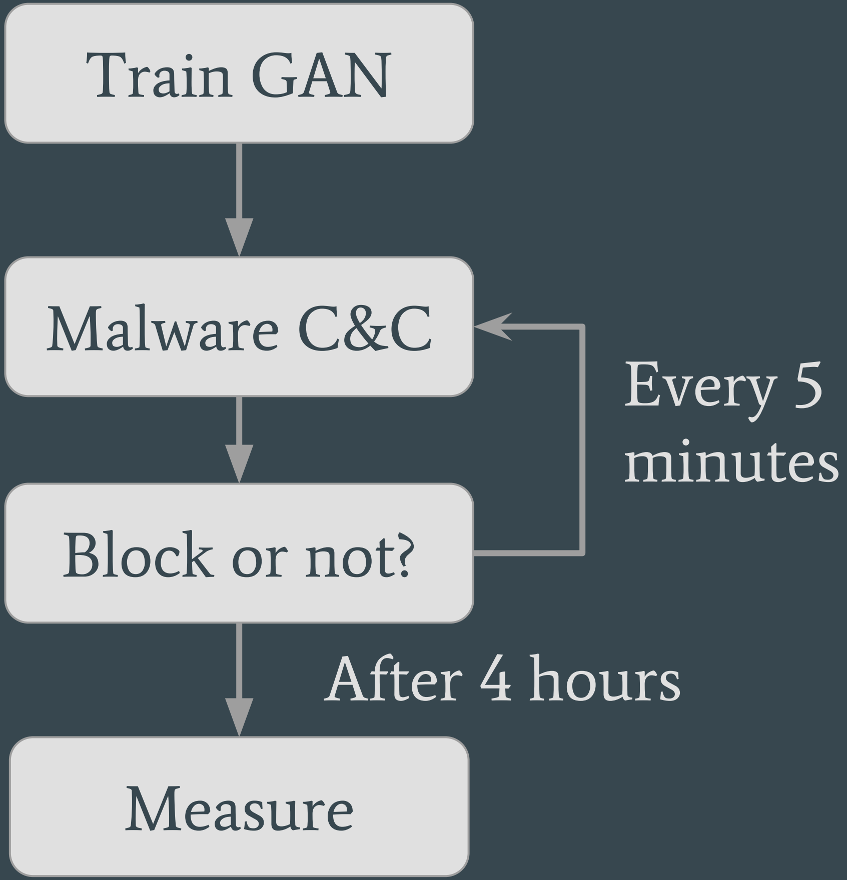
Between 0 and 5 seconds:	.
Between 5 and 60 seconds:	,
Between 60 secs and 5 mins:	+
Between 5 mins and 1 hour:	*
Timeout of 1 hour	0

Experiment Setup



[1] Thanks to Ondrej Lukas for implementing SLIPS :)

Phase 1



Train GAN

Malware C&C

Block or not?

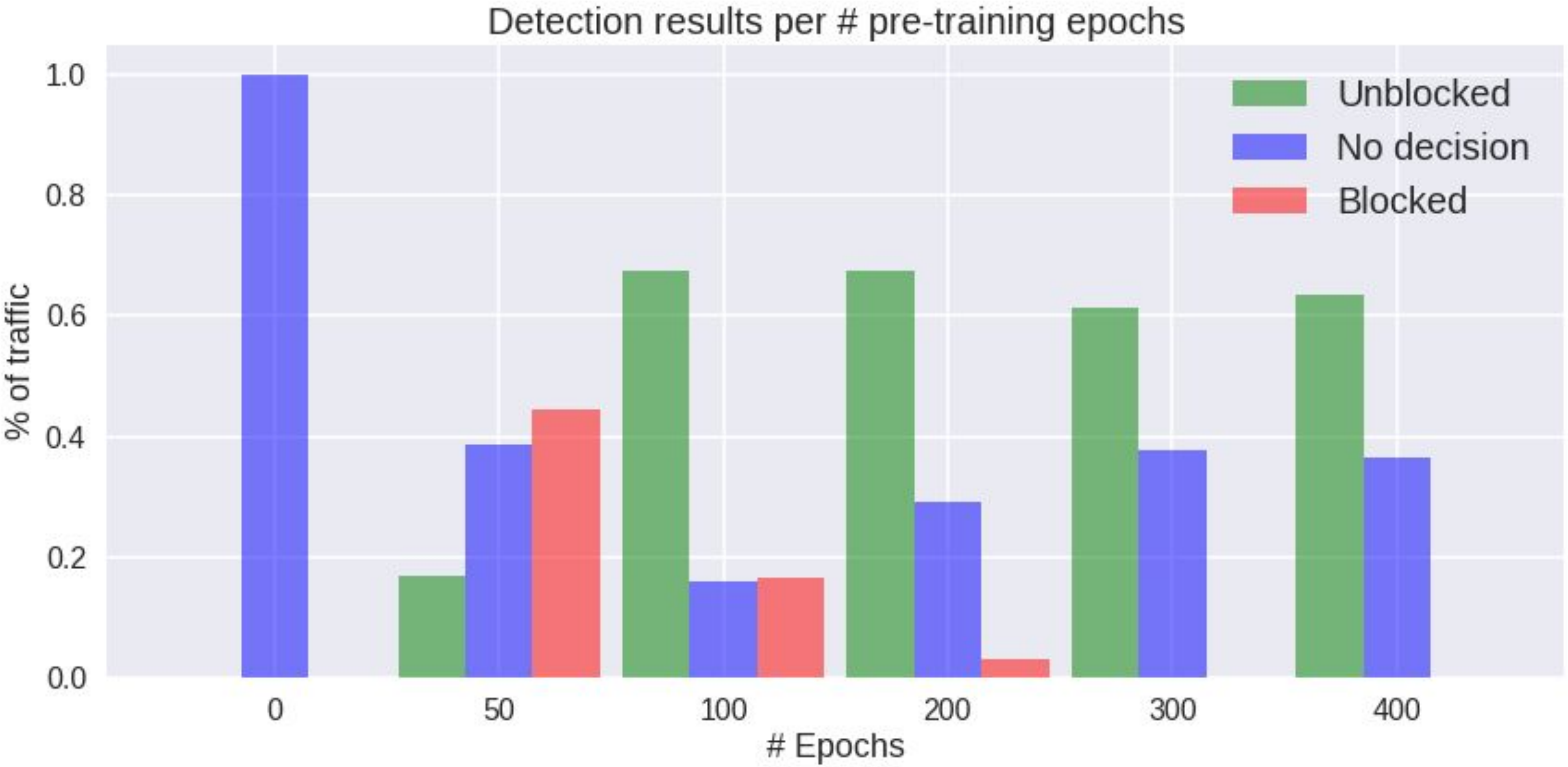
Every 5 minutes

After 4 hours

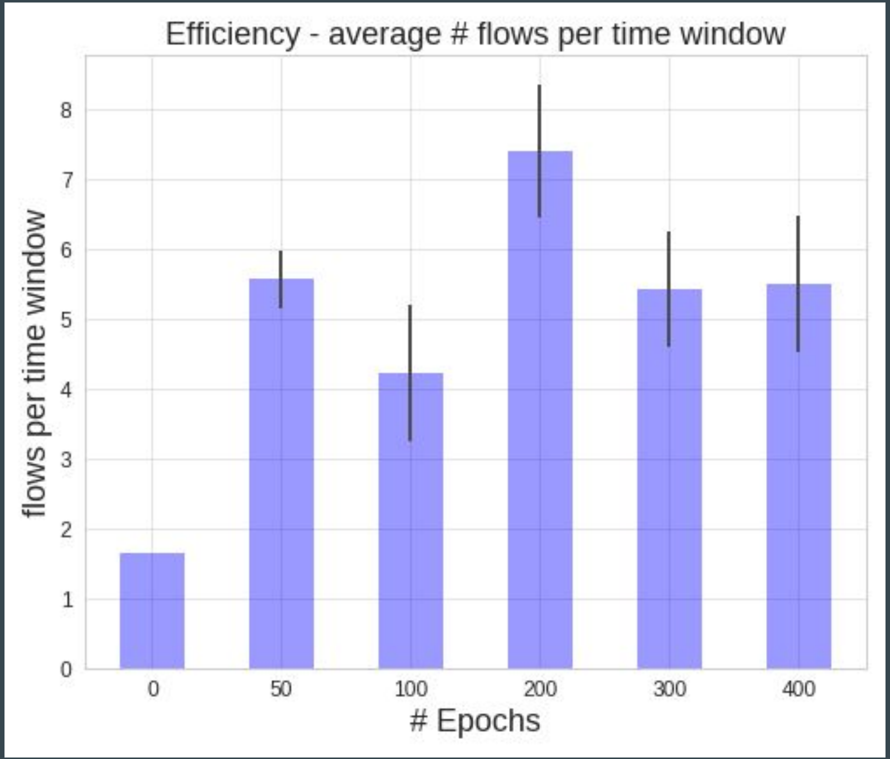
Measure

Results

Detection Results - Phase 1



Efficiency - Phase 1



- Maximum efficiency is 7.5 flows / time window
- 1 connection every 40 seconds

What’s next?

Potential improvements

- Add support for HTTPS
- Combine generator and malware
- Test with different types of traffic / detectors
- Incorporate in a red team tool
- Improve the feedback loop
- Automate the time window discovery

Discussion

- Yes we can! use GANs for mimicking traffic characteristics
- Other areas: censorship circumvention, network traffic generation
- Maybe an overkill now, but...

Thank you for listening!

maria.rigaki@aic.fel.cvut.cz

@mrigaki

mariarigaki

https://www.stratosphereips.org/