MODELLING THE NETWORK BEHAVIOR OF MALWARE TO BLOCK MALICIOUS PATTERNS.

THE STRATOSPHERE PROJECT

Garcia Sebastian, PhD . CTU University, Prague.
sebastian.garcia@agents.fel.cvut.cz
@eldracote

Current Network Solutions

IoC

- Domains
- URLs
- IPs

FINGERPRINTS

- Payloads

BEHAVIORS

- Anomaly Detection

Current Network Solutions

IoC

- Domains
- URLs
- IPs

FINGERPRINTS

- Payloads

BEHAVIORS

- Anomaly Detection

ISSUES

- Lifetime
- Verification and Errors
- Huge Amount
- Static
- **Easy adaptation from attackers**

Current Network Solutions

IoC

- Domains
- URLs
- IPs

FINGERPRINTS

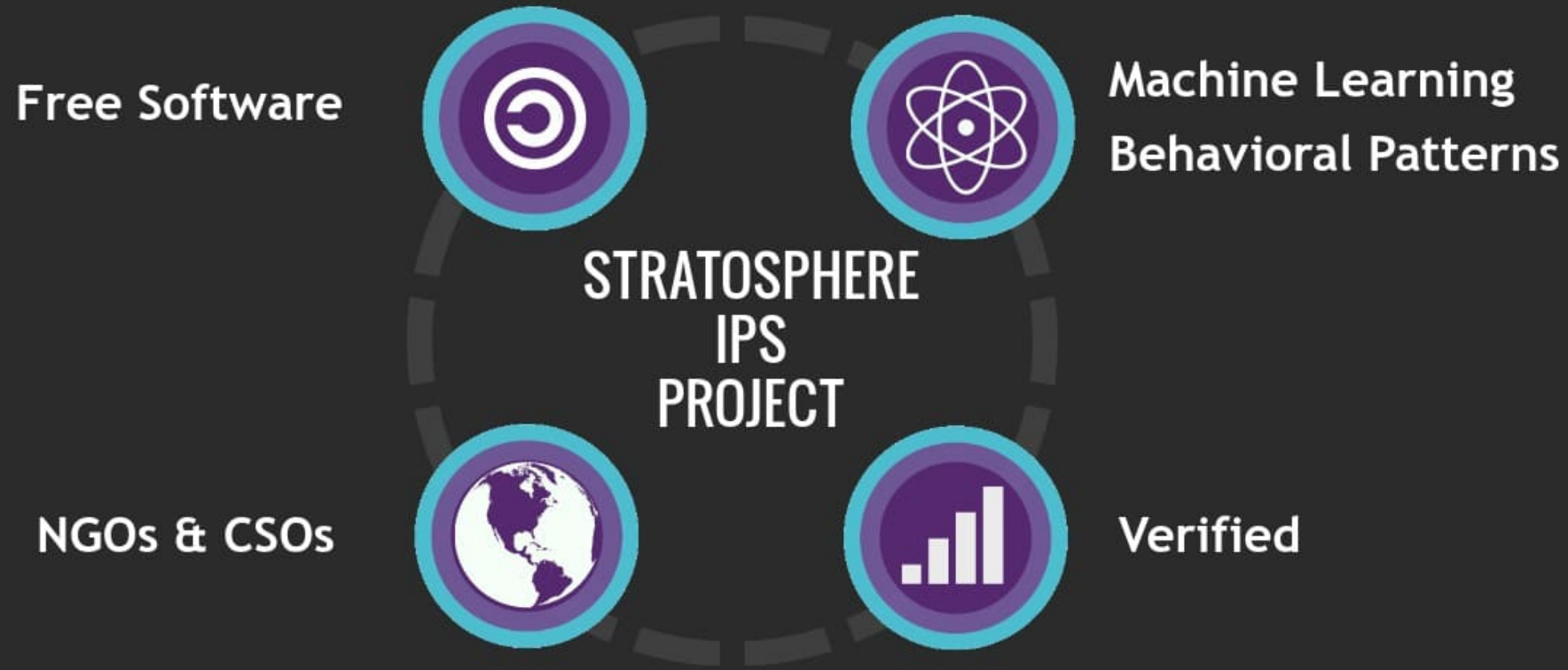
- Payloads

BEHAVIORS

- Anomaly Detection
- Behavioral Models

ISSUES

- Lifetime
- Verification and Errors
- Huge Amount
- Static
- **Easy adaptation from attackers**


Free Software
Machine Learning
Behavioral Patterns
STRATOSPHERE
IPS
PROJECT
NGOs & CSOs
Verified

STRATOSPHERE TECHNICAL PILLARS

LESS IS MORE

DISASSOCIATE

VERIFY

STRATOSPHERE PILLARS

LESS IS MORE

Analyze the behavior of connections, not host or networks.

DISASSOCIATE

"Represent the behavior" from "Detect the behavior".

VERIFY

Verify the models with real and labeled data.

LESS
IS MORE

- Your behavior is usually the same when connecting with the same service.
- Group the flows going to a specific service by ignoring the source port. We have a connection.
- The connection, composed of several flows, now shows a behavior.

LESS
IS MORE

- When using a service, you go from a specific state to the next state.
- Each flow inside the connection gets its own state.
- We model the states based on four features.
  - Size of the flow.
  - Duration of the flow.
  - Periodicity of the flow.
  - Time between consecutive flows.

BEHAVIORAL STATES

	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

BEHAVIORAL STATES

BEHAVIORS ARE MORE STABLE

- Malware generate the same behavior over and over again.
- $ Changing the behavior is costly for the attacker.
- Behaviors do not expire quickly.
- Infections go unnoticed for hours. There is time.
- We collect normal and malware behaviors.

DETECTION MODELS

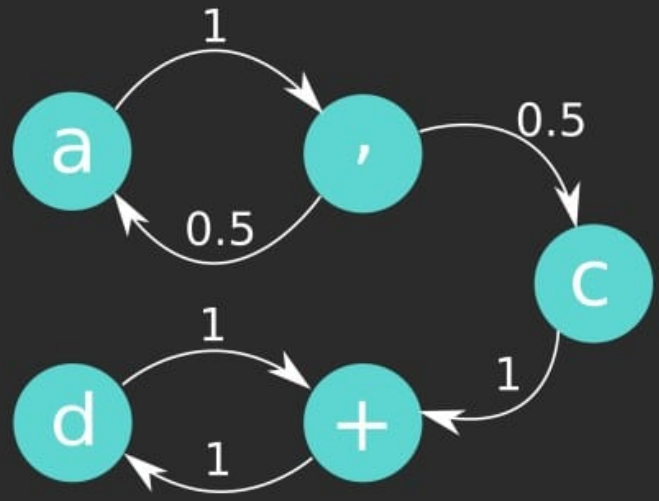
- Several models can be implemented. Currently two working and two under development.
- Interpret the transition from one state to the other as a Markov Chain.

DETECTION MODELS

- Interpret the transition from one state to the other as a **Markov Chain**.

a , a , c + d + d +

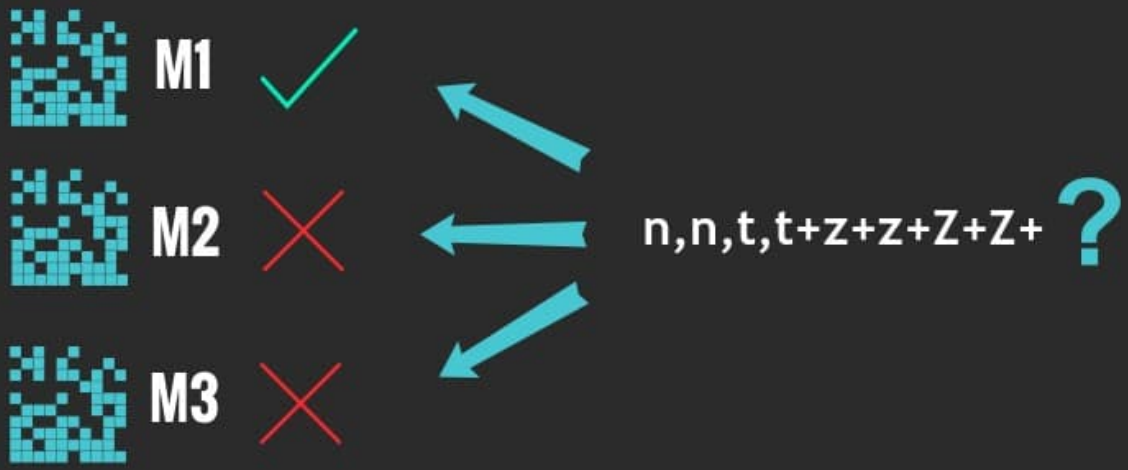
	a	,	c	+	d
a		1			
,	0.5		0.5		
c				1	
+					1
d				1	



IV: +=0.2 ,=0.2 a=0.2 c=0.11 d=0.22

DETECTION MODELS

- Train Markov Models with known behaviors.
- Compare the unknown traffic to each Markov Model of the trained behaviors.



DETECTION MODEL

- Detect similar behavior in unknown networks by generalizing the Markov Models.
- Compute the winner model.
- Are results good?

VERIFICATION

- Yes, but...
- Depends in
  - Datasets
  - Time Frame
  - Verification Method
- Large, public, labeled and real datasets with normal, malicious and hybrid behaviors.
- Compare different approaches.
- Crucial for predicting the performance.

CONCLUSION

- Network behavioral patterns work well as a complement of current detection solutions.

Thanks!

- Sebastian Garcia
- sebastian.garcia@agents.fel.cvut.cz
- @eldracote
- https://stratosphereips.org