

---

FOCUS ON YOUR  
MALWARE, NOT  
INFRASTRUCTURE!

OMRI SEGEV MOYAL

@GelosSnake

## WHAT DO SECURITY RESEARCHERS FIND MOST CHALLENGING WHEN CREATING A NEW APPLICATION?



Based on twitter survey - <http://bit.ly/2MPAyyY>

Omri Segev Moyal @GelosSnake

Focus on Your Malware, **Not Infrastructure!**

# PRESENTATION AGENDA

01

Modern Research  
Practices

02

Serverless Introduction &  
Security Considerations

03

Current Usage  
& Pioneers

04

Hands-On Example

05

Live Demo

---

# OMRI SEGEV MOYAL



## RESEARCHER

Malware, APT, CryptoMiners, OSINT, Exploit Kits...



## COMMUNITY ADVOCATE

Founder of world's largest and most active  
Malware Research Group with over 700 members  
world wide. Join us! <https://malware-research.org/slack>  
Admin, 9723 Defcon Chapter



## ENTREPRENEUR

Private Consultant  
Co-Founder @ Minerva Labs  
Strategic Advisor @ ClearSky Cyber Security



## MHFC ULTRA FAN

Maccabi Haifa sport club fan.  
Born into it, never left.



---

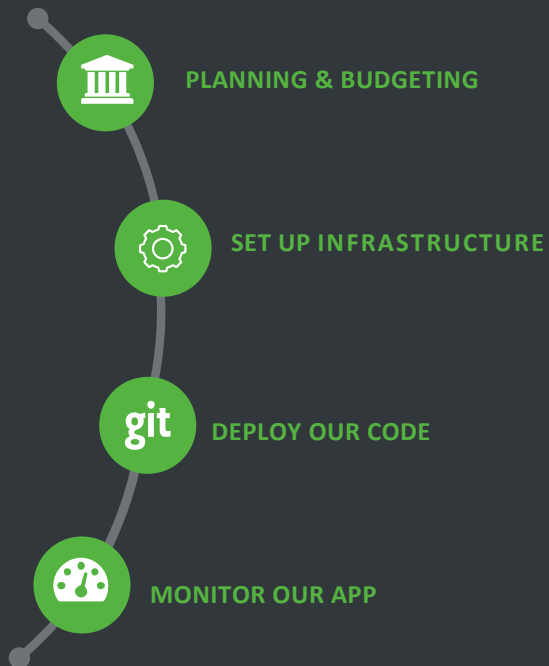
#OSDFCON #SERVERLESS  
@GELOSSNAKE

OMRI SEGEV MOYAL

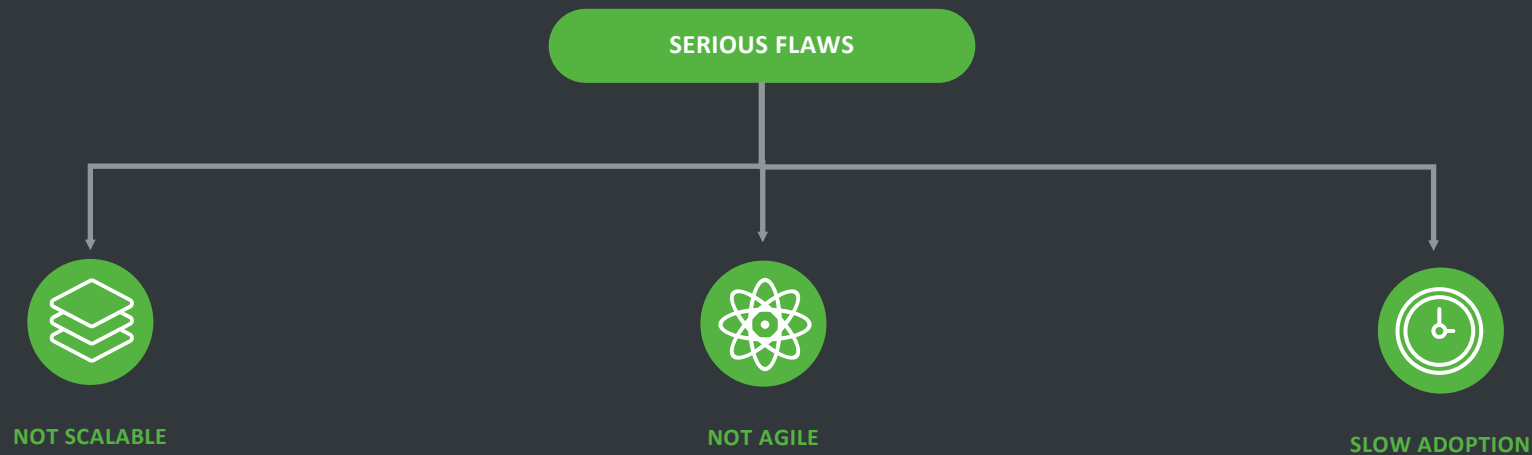
@GelosSnake

# SECURITY RESEARCH TODAY

How do we build our research apps today?



# SECURITY RESEARCH TODAY



# QUICK INTRODUCTION TO SERVERLESS

FOCUS ON WRITING CODE

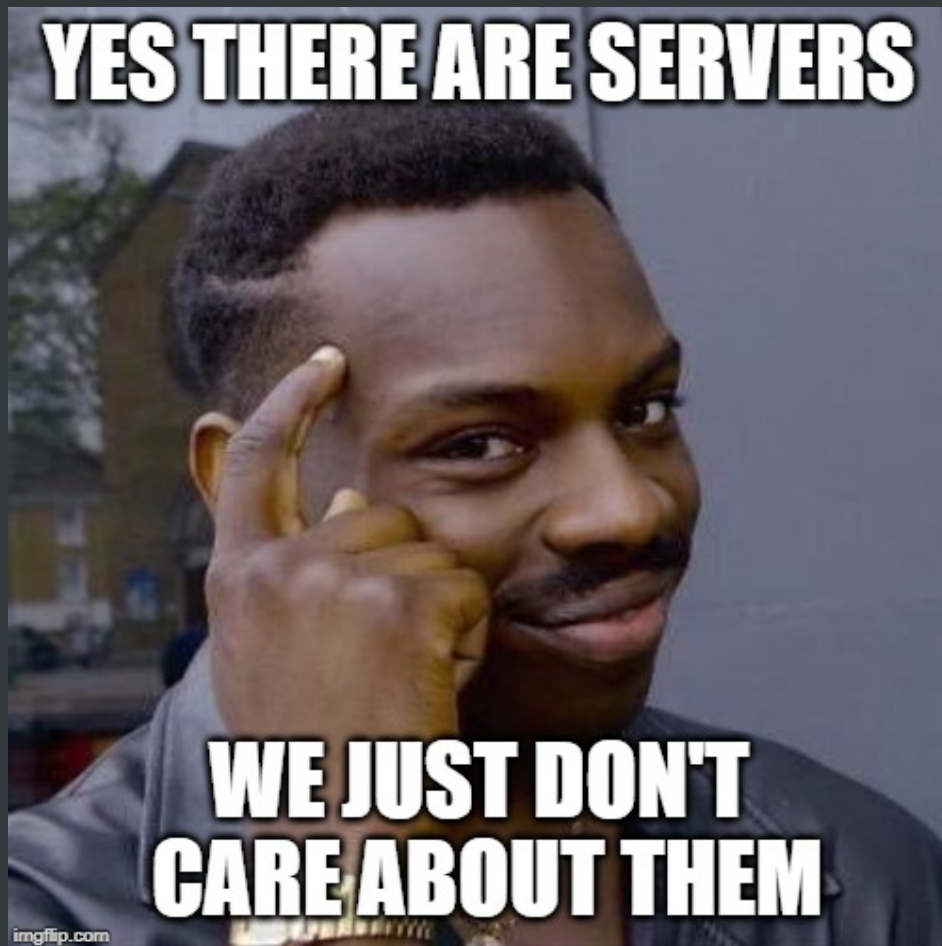
EVENT DRIVEN

NEVER PAY FOR IDLE RESOURCES

SCALABLE







---

# SERVERLESS CONS & LIMITATIONS



LEARNING CURVE



TECHNICAL LIMITATIONS



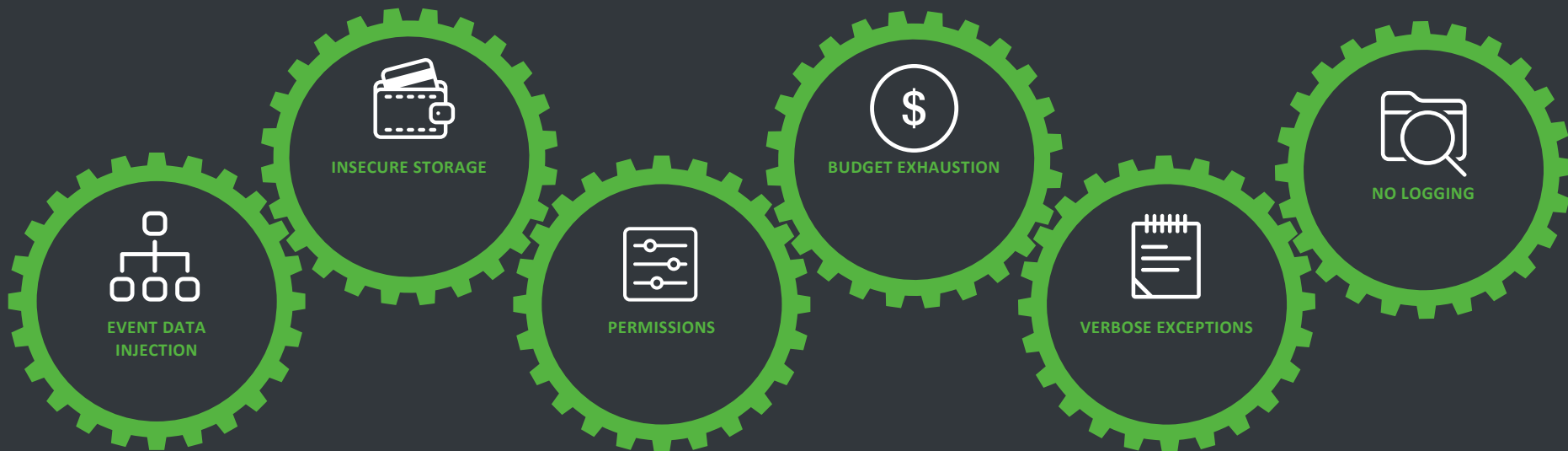
TOUGH TO DEBUG



WARM AND COLD BOOTS



# COMMON SECURITY PROBLEMS



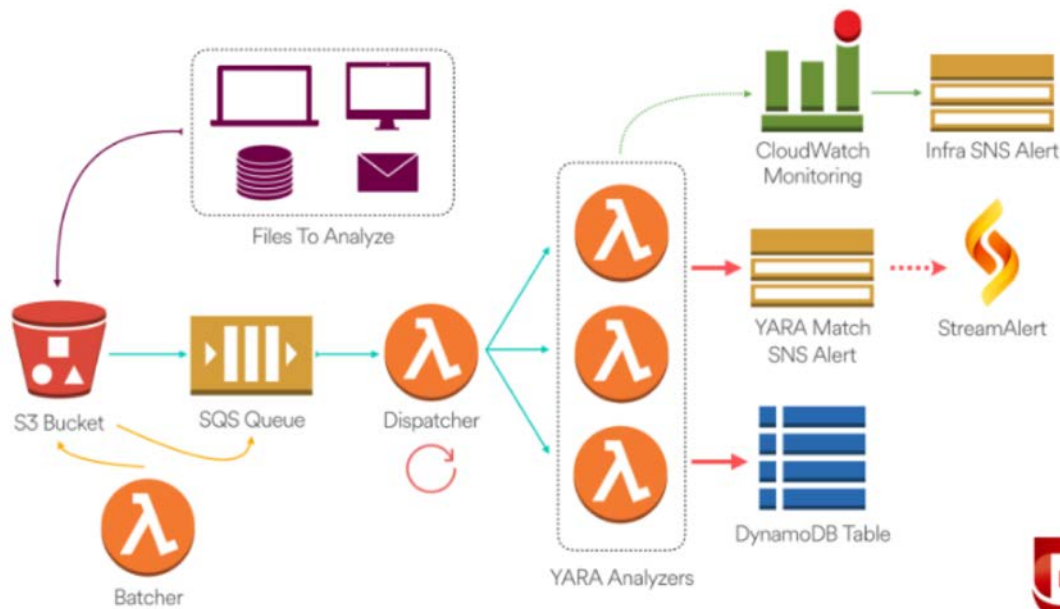
“A VERY INTERESTING  
QUOTE FROM THE ART OF  
WAR.”

Omri Segev Moyal,  
who could not find any  
Sun Tzu related quote.

# AIRBNB BINARY ALERT



## Analysis Flow



<http://www.binaryalert.io/>

Omri Segev Moyal @GelosSnake

Focus on Your Malware, Not Infrastructure!

14

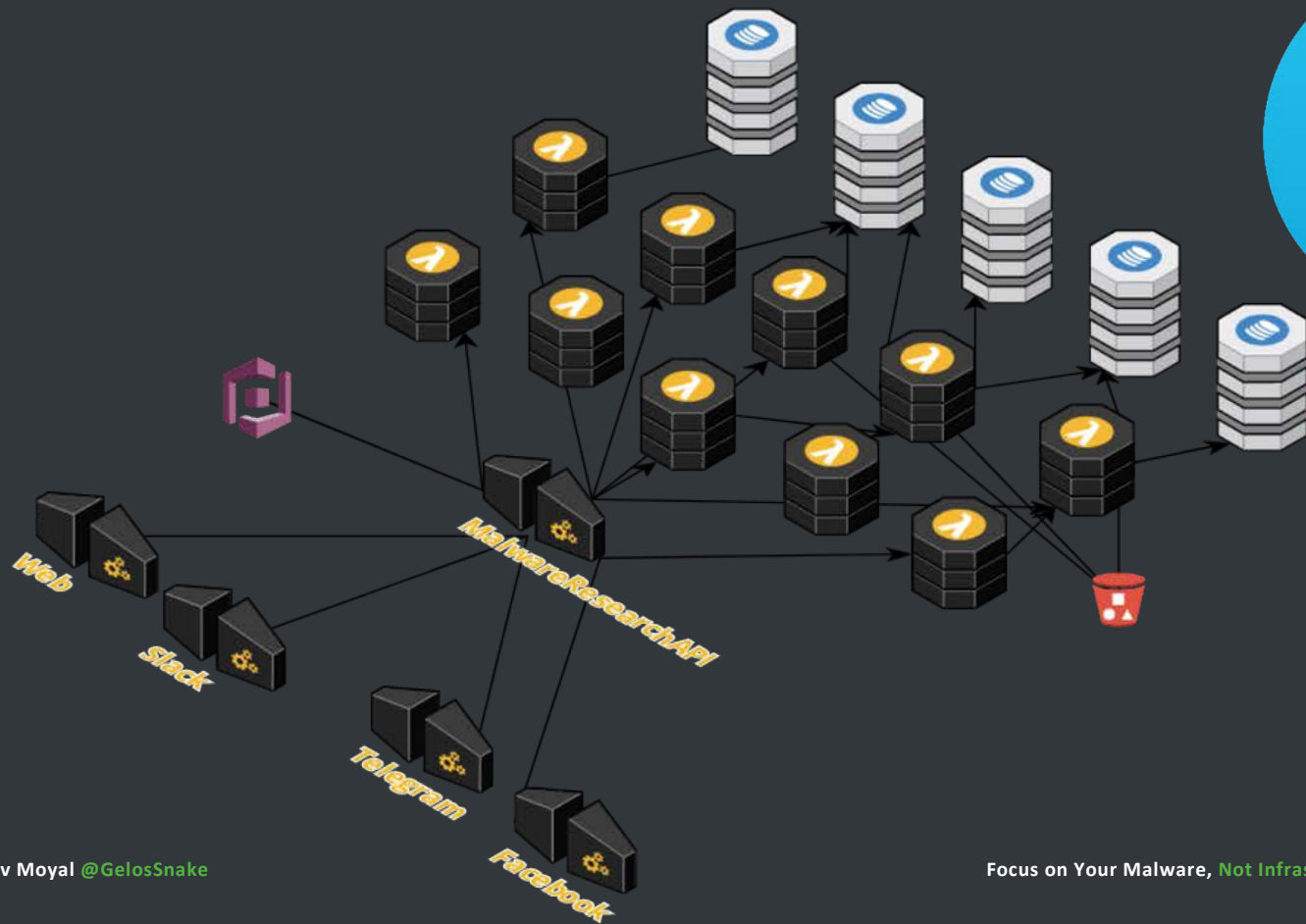


Drop files here  
to send them as files



```
b9c70e272c6bd591  
f23ab1932bd7e4e14  
e8b49aaa225c1cee9  
5a0d863981783
```

# MALSCANBOT SERVERLESS BACKEND





## PRACTICAL EXAMPLE – BUILDING A SERVERLESS SINKHOLE



# FINDING “SINKABLE” MALWARE

DNS Resolutions

	HTTP REQUESTS	CONNECTIONS	DNS REQUESTS	THREATS
NETWORK	21	14	104	78

Time offset	Status	Rep	Domain	IP
937ms	REQUESTED	🔥	gahyqah.com	IP Addresses not found
937ms	RESPONDED	🔥	lyvyxor.com	208.100.26.251
938ms	REQUESTED	🔥	puvyxil.com	IP Addresses not found
				18.213.250.117
938ms	RESPONDED	🔥	vocyzit.com	52.4.209.250
				18.215.128.143
938ms	REQUESTED	🔥	galykes.com	IP Addresses not found
939ms	REQUESTED	?	purydyv.com	IP Addresses not found
939ms	REQUESTED	🔥	gacyzuz.com	IP Addresses not found
939ms	REQUESTED	🔥	vowydef.com	IP Addresses not found
940ms	REQUESTED	?	lygyjoj.com	IP Addresses not found

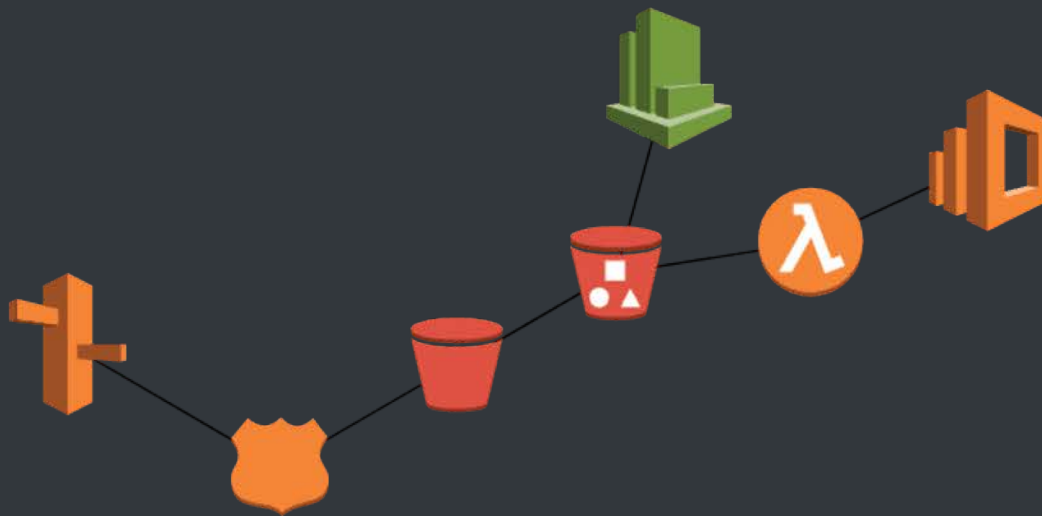
qetyfuv.com

104.239.157.210

puvyxil.com

No resolutions recorded

# BUILDING A SERVERLESS SINKHOLE



# MONITORING RESULTS



DEMO TIME

# PRESENTATION RECAP

01

Modern Research  
Practices

02

Serverless Introduction &  
Security Considerations

03

Current Usage  
& Pioneers

04

Hands-On Example

05

Live Demo

OMRI SEGEV MOYAL

@GELOSSNAKE



GELOSSNAKE

---

THANK YOU

OMRIMOYAL



OMRI@PROFERO.IO