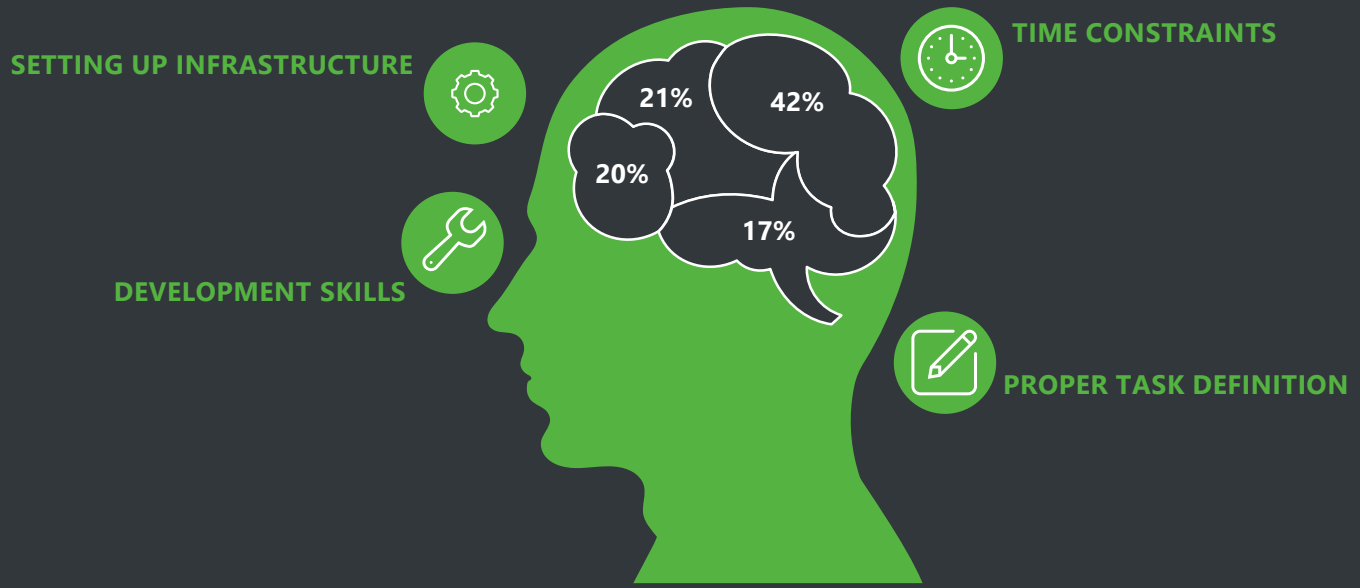
FOCUS ON YOUR MALWARE, NOT INFRASTRUCTURE!

OMRI SEGEV MOYAL
@GelosSnake

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



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

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…

ENTREPRENEUR

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

COMMUNITY ADVOCATE

Founder of world's largest and most active Malware Research group with over 700 members.
Co-founded Malware-Media group to shorten media and research gaps.
Admin, 9723 Defcon Chapter

MHFC ULTRA FAN

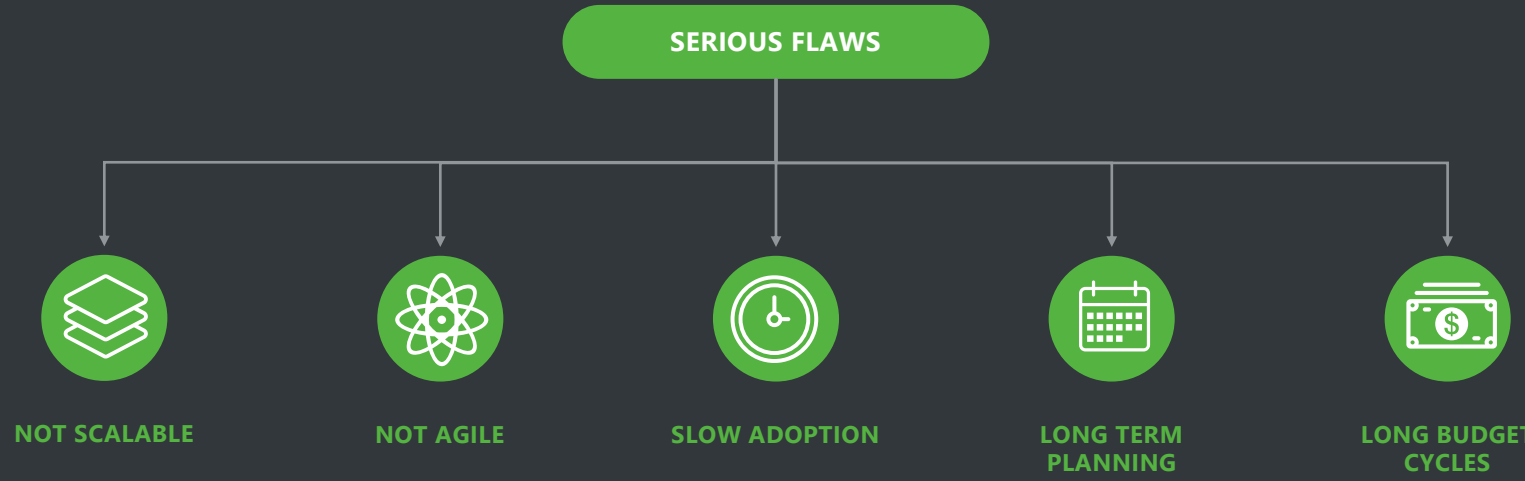
Maccabi Haifa Football club fan.
Born into it, never left.

SECURITY RESEARCH TODAY

How do we build our research apps today?

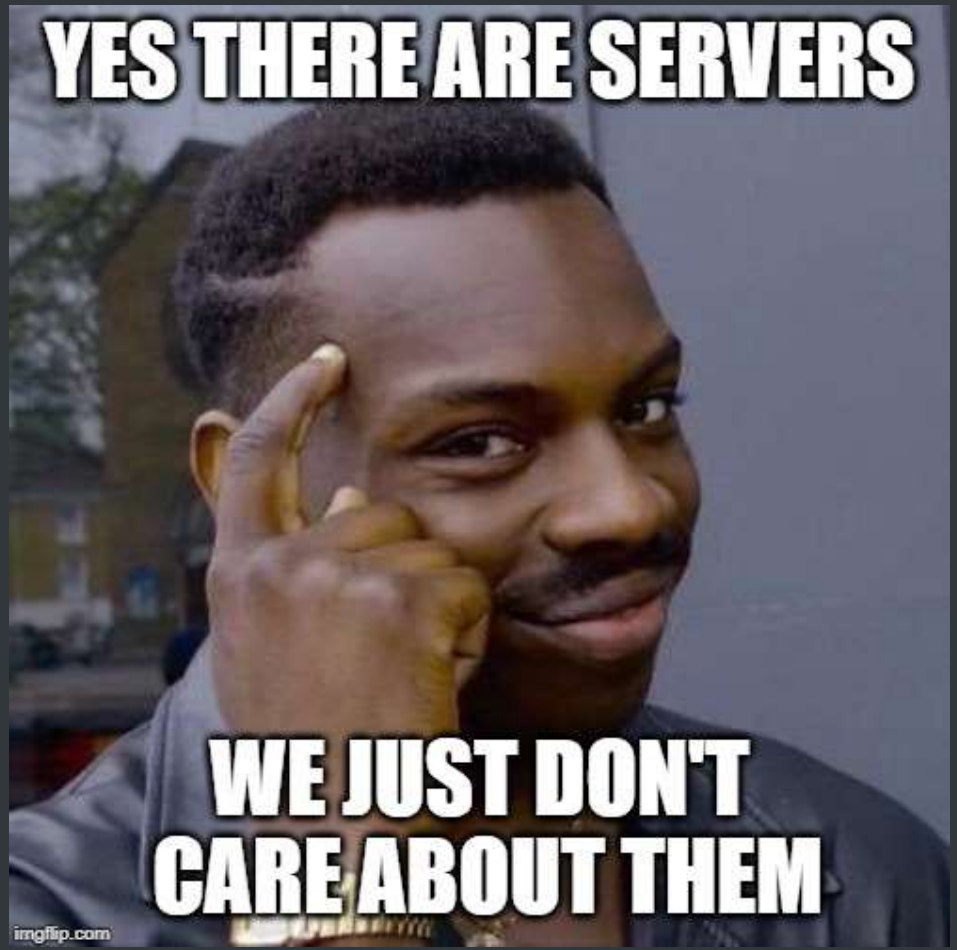
MODERN SECURITY RESEARCH TOOLS

SECURITY RESEARCH TODAY



QUICK INTRODUCTION TO SERVERLESS

- FOCUS ON WRITING CODE
- EVENT DRIVEN
- NEVER PAY FOR IDLE RESOURCES
- SCALABLE


YES THERE ARE SERVERS
WE JUST DON'T CARE ABOUT THEM
imgflip.com

SERVERLESS CONS & LIMITATIONS

LEARNING CURVE

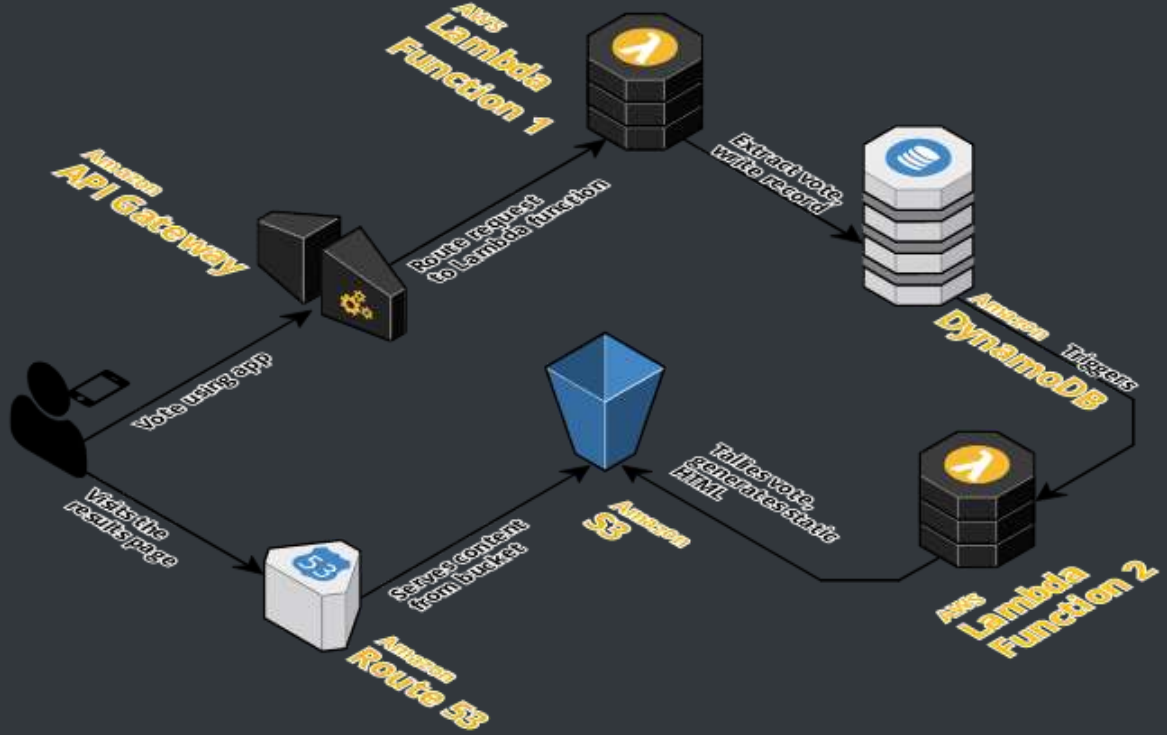
WARM AND COLD BOOTS

TOUGH TO DEBUG

INFRASTRUCTURE OWNED BY SERVICE PROVIDER

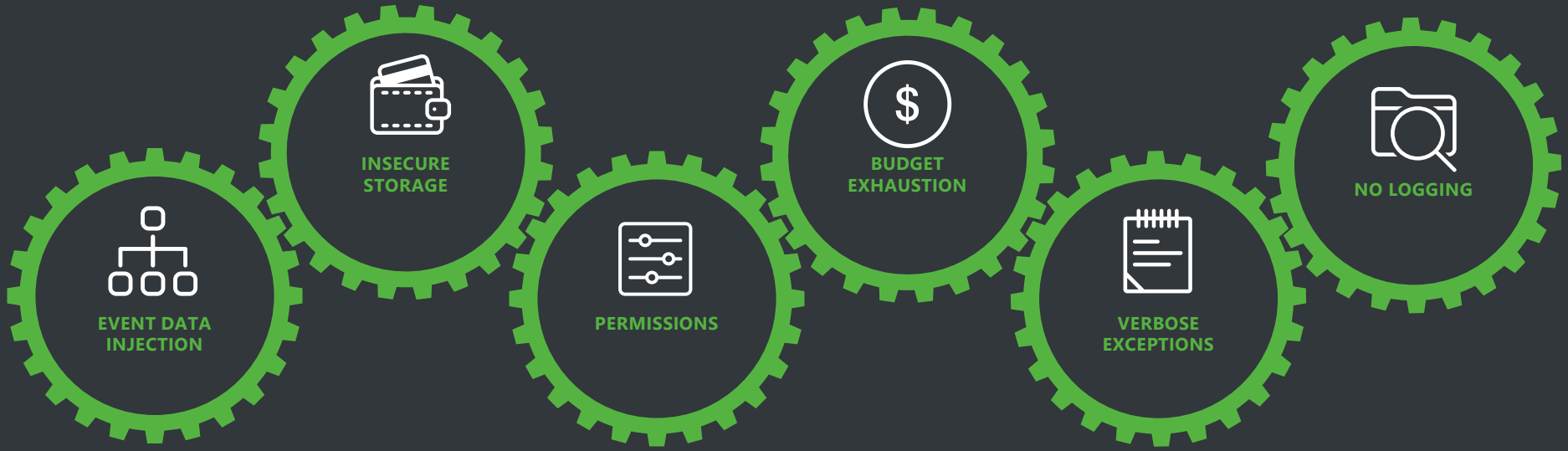
TECHNICAL LIMITATIONS

SIMPLE SERVERLESS VOTING APP



Created via https://cloudcraft.co

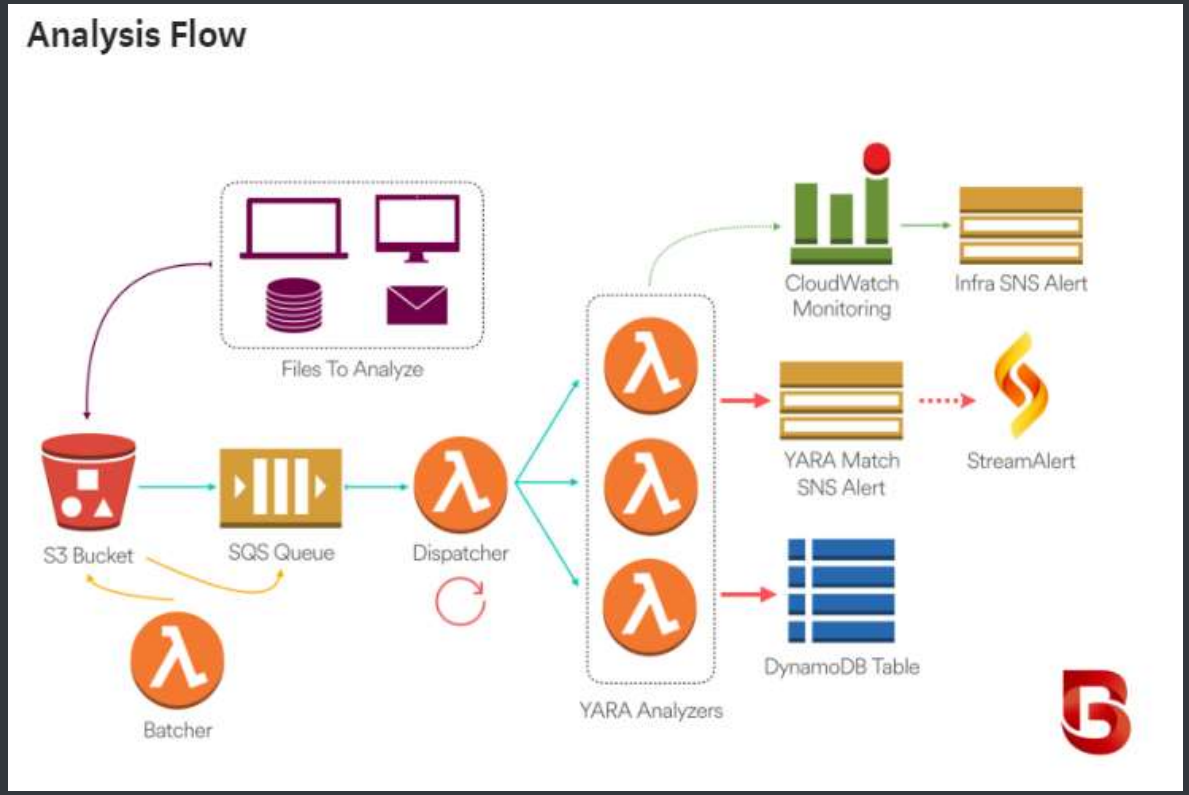
COMMON SECURITY PROBLEMS



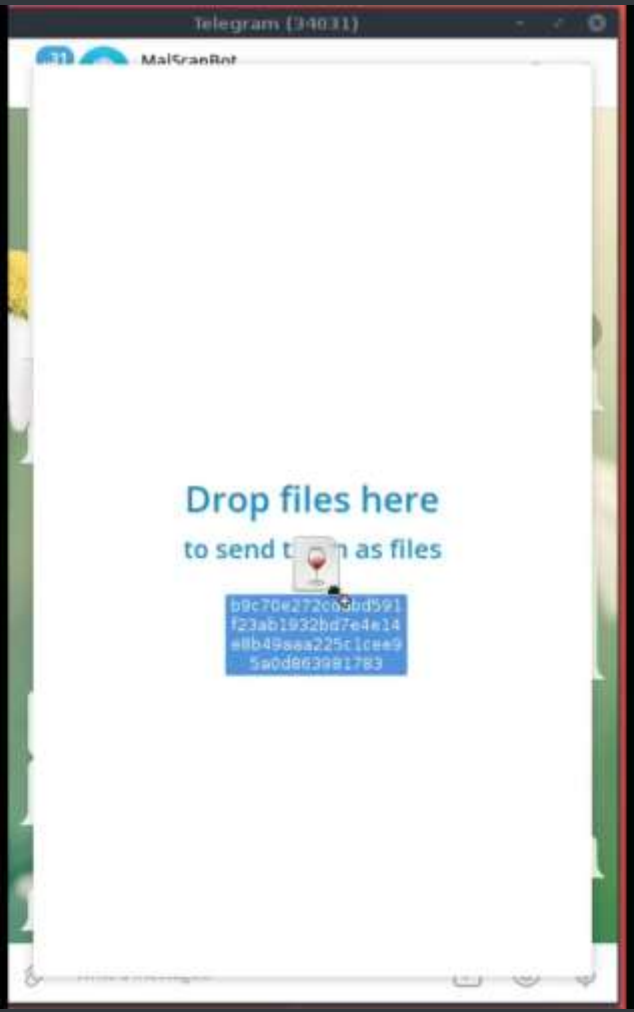
“A VERY INTERESTING QUOTE FROM THE ART OF WAR.”

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

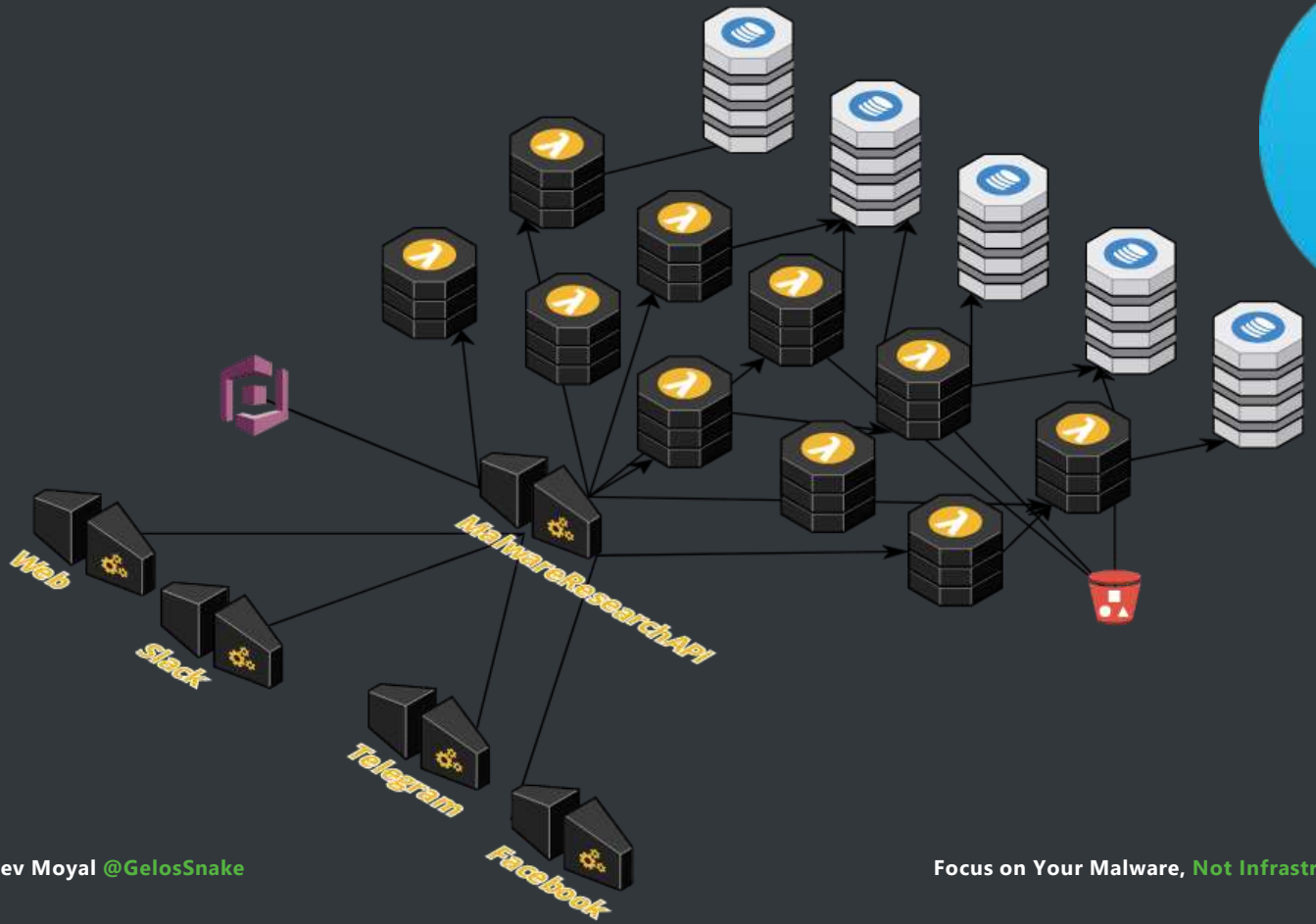
AIRBNB BINARY ALERT



http://www.binaryalert.io/

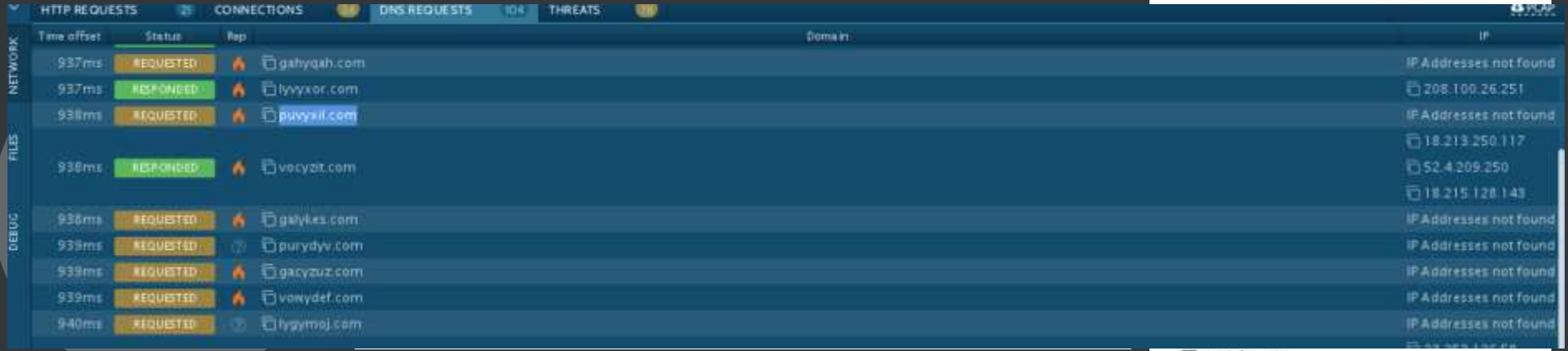

Telegram (34031)
MalGranBot
Drop files here
to send t n as files
b9c70e272c65bd591
f23ab1932bd7e4e14
e8b49aaa225c1cee9
5a0d863981783

MALSCANBOT SERVERLESS BACKEND

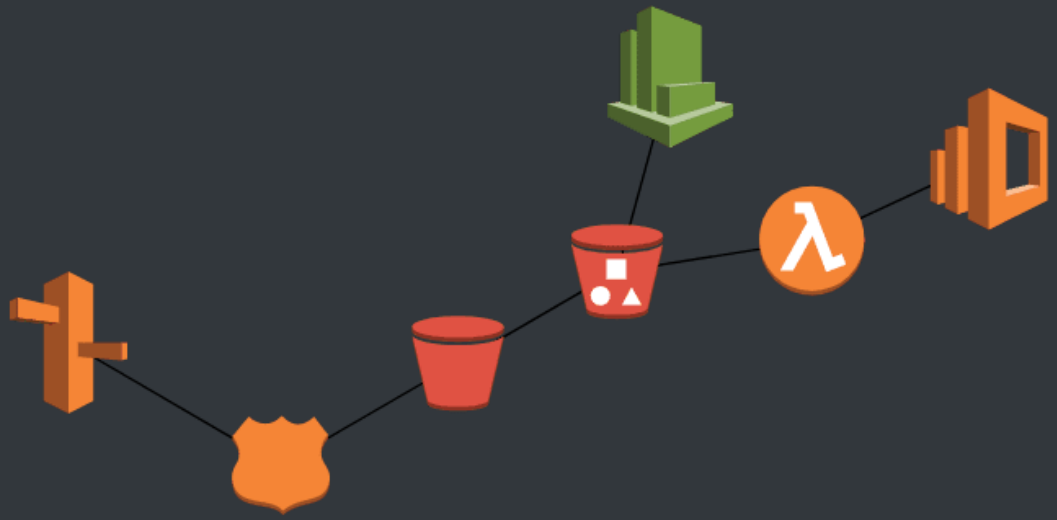


PRACTICAL EXAMPLE – BUILDING A SERVERLESS SINKHOLE

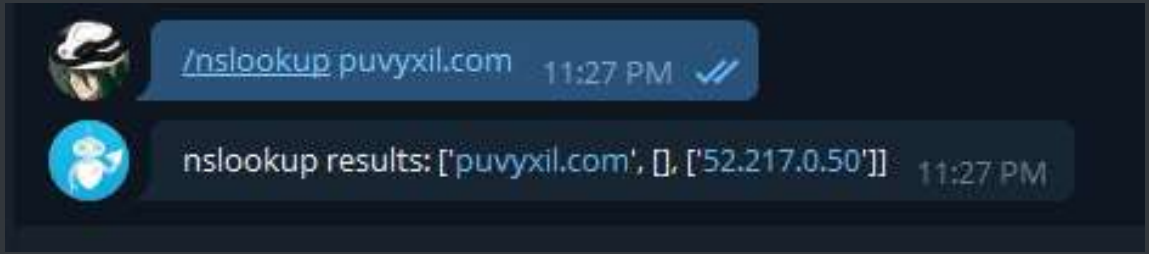
FINDING "SINKABLE" MALWARE



BUILDING A SERVERLESS SINKHOLE



MONITORING RESULTS




```
f6db3748ffe482d91860ac6d6626f4b014aa8b253eb6b889466c808e8d42807f puvyxil.com [04/Jun/2019:21:47:00 +0000] 65.154.226.109 - 9105123F58C08FE0
WEBSITE.GET.OBJECT login.php "GET /login.php HTTP/1.1" 200 - 108 108 16 16 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)" -
qEREcvVxy5bL9ERsMB80T1WcL/yPusdAen6y9yg6C2+XjaX56JSRVc1qszl1XEvYMgGgNok9LRg= - - - puvyxil.com -
```

SHOWING OFF


ICELAND
FINLAND
NORWAY
ESTONIA
LATVIA
Moscow
Москва
UNITED KINGDOM
DENMARK
REPUBLIC OF BELARUS
GERMANY
Paris
UKRAINE
FRANCE
AUSTRIA
ROMANIA
KAZAKHSTA
ANDORRA
ITALY
BULGARIA
PORTUGAL
GREECE
TURKEY
TUNISIA
IRAQ
IRAN
AFGHANIS
MOROCCO
ISRAEL
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
UNITED ARAB EMIRATES
MAURITANIA
NIGER
MALI
CHAD
SUDAN
ERITREA
YEMEN
SENEGAL
Hudson Bay
Labrador Sea
Norda Atlantika
Sargasso Sea
Gulf of Mexico
Atlantic
UNITED STATES OF AMERICA
Washington
Los Angeles
MEXICO
CUBA
DOMINICAN REPUBLIC
GUATEMALA

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

THANK YOU