FOCUS ON YOUR MALWARE, NOT INFRASTRUCTURE!

OMRI SEGEV MOYAL
@GelosSnake
WHAT DO SECURITY RESEARCHERS FIND MOST CHALLENGING WHEN CREATING A NEW APPLICATION?

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...

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 worldwide. Join us! https://malware-research.org/slack
Admin, 9723 Defcon Chapter

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

Omri Segev Moyal @GelosSnake
SECURITY RESEARCH TODAY

How do we build our research apps today?

- Planning & Budgeting
- Set Up Infrastructure
- Deploy Our Code
- Monitor Our App
Security research today:

- Serious flaws
  - Not scalable
  - Not agile
  - Slow adoption

Focus on your malware, not infrastructure!
QUICK INTRODUCTION TO SERVERLESS

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

Focus on Your Malware, Not Infrastructure!
YES THERE ARE SERVERS

WE JUST DON'T CARE ABOUT THEM
SERVERLESS CONS & LIMITATIONS

- LEARNING CURVE
- TOUGH TO DEBUG
- TECHNICAL LIMITATIONS
- WARM AND COLD BOOTS
Focus on Your Malware, Not Infrastructure!

Omri Segev Moyal @GelosSnake
COMMON SECURITY PROBLEMS

- Insecure Storage
- Permissions
- Budget Exhaustion
-Verbose Exceptions
- Event Data Injection
- No Logging
“A VERY INTERESTING QUOTE FROM THE ART OF WAR.”

Omri Segev Moyal, who could not find any Sun Tzu related quote.
Focus on Your Malware, Not Infrastructure!

AIRBNB BINARY ALERT

http://www.binaryalert.io/
Omri Segev Moyal @GelosSnake
Focus on Your Malware, Not Infrastructure!

Omri Segev Moyal @GelosSnake

https://t.me/MalScanBot
https://github.com/GelosSnake/MalwareResearchAPI

INTRODUCING MALSCANBOT

Drop files here
to send them as files

b9c70e272c03dbd591
t23ab1992bd7e4e14
ebb49faa225c1c0e6
5a0d639b1783
Focus on Your Malware, Not Infrastructure!
FINDING “SINKABLE” MALWARE

Site: virustotal.com

Tip: "nxdomain"
BUILDING A SERVERLESS SINKHOLE
Focus on Your Malware, Not Infrastructure!

MONITORING RESULTS

Omri Segev Moyal @GelosSnake
DEMO TIME
PRESENTATION RECAP

01 Modern Research Practices
02 Serverless Introduction & Security Considerations
03 Current Usage & Pioneers
04 Hands-On Example
05 Live Demo
THANK YOU

OMRI SEGEV MOYAL

@GELOSSNAKE

GELOSSNAKE

OMRIMOYAL

OMRI@PROFERO.IO