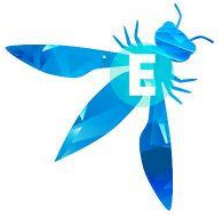
OWASP
Open Web Application Security Project

Catching up with today's malicious actors

Current security posture and future possible actions

OWASP EEE Bucharest Event 2015
Adrian Ifrim

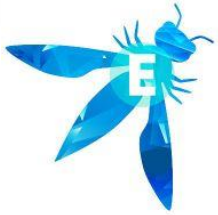


OWASP

Open Web Application Security Project

Disclaimer

The content of this presentation does not reflect the official opinion of the my current employer or former employers. Responsibility for the information and views expressed in the presentation lies entirely with the author.



OWASP

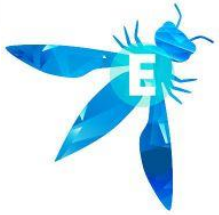
Open Web Application Security Project

id -un

Adrian Ifrim

cat .bash_history | grep jobs

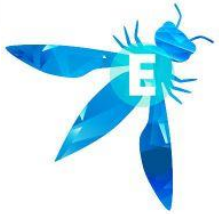
- Helpdesk/Network Administrator
- Junior System Administrator
- Support Engineer
- IS Analyst
- IT Auditor
- Tech Security Lead



uname -a

OWASP
Open Web Application Security Project

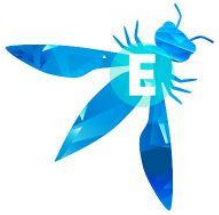
- cat /proc/cpuinfo | grep hobbies
  - Information Security
  - Information Security
  - Information Security
  - Information Security



OWASP

Open Web Application Security Project

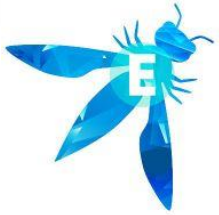
Chapter 1
Current state



OWASP
Open Web Application Security Project

Who are we dealing with?

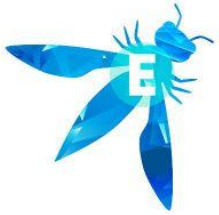
- State sponsored attacks
- Organized Hacking Teams
- State-sponsored hackers: hybrid armies
- Terrorist organizations
- One-man-show
- Internal disgruntled employees
- Malicious vendors – Software/Hardware
- Trusted Third Party



OWASP
Open Web Application Security Project

What are their strengths?

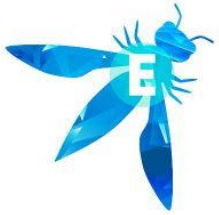
- Time
- Unlimited budget
- Open source tools
- Open Knowledge base (the Internet)
- No bureaucratic approvals
- New tricks up their sleeves (0days)
- Strong Motive (financial, political, patriotic, fun)



Who do we usually have?

OWASP
Open Web Application Security Project

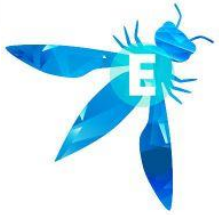
- Small teams of security professionals
- Limited time
- Limited budgets
- Limited tools (if you don't have support you cant use it)
- Bureaucratic approvals
- Security testing requirements



Losing the war - Tools

OWASP
Open Web Application Security Project

- Anti-Virus
  - ✓ veil framework
  - ✓ backdoor factory
  - ✓ mitmf
  - ✓ metasploit
  - ✓ powershell
  - ✓ wmic
  - ✓ vbscript
- Cost to make an undetected virus ~ 0

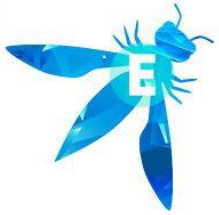


Losing the war – More tools

OWASP
Open Web Application Security Project

- Maintained by people for the people

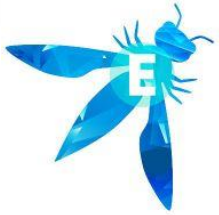
  - ✓ Firewalls/Routers/Switches)
  - ✓ Web Site filtering
  - ✓ Data Leakage Protection
  - ✓ Web Application Firewalls
  - ✓ Database Activity Monitoring
  - ✓ SIEMs
  - ✓ Vulnerability scanners
  - ✓ IDS/IPS
  - ✓ Anti Malware
  - ✓ etc



Losing the war: Monitoring those tools

OWASP
Open Web Application Security Project

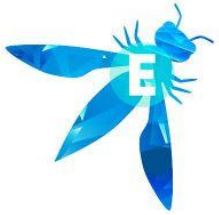
- Maintained by people for the people
- Various time formats
- Various log formats
- Alert/parsing configuration
- Huge number of events



The hype:

OWASP
Open Web Application Security Project

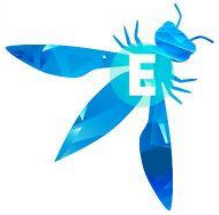
- Stagefright bug
  - ✓ Scary but not working on latest version of Android
  - ✓ Other countries may be affected :)
- Heartbleed
  - ✓ http://siui.casan.ro/cnas/ is protected btw (no certificate)
  - ✓ introduced in 2012 and publicly disclosed in 2014
- Various 0days: flash,adobe reader, windows, osx, android, php, anti-virus



Start being afraid of the right things
Your real problems:

OWASP
Open Web Application Security Project

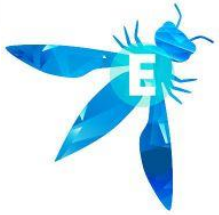
- Your assets. The inventory
- Personnel
- ~6000days
- Everyone's a coder
- Availability
- Did you know you use IPv6? Yeah you do
- Tools
- Old mindsets
- Credentials everywhere
- No two factor
- No encryption
- Wireless
- Monitoring
- APT (Antivirus Fail)
- Unauthorized tools



Various questions and answers received over the years

OWASP
Open Web Application Security Project

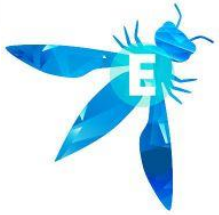
- Why would I need security advisory in change management?
- I know all my systems
- But we do vulnerability scanning
- If its internal they can't get in and we should not use encryption
- Our anti-virus definitions are up-to-date



OWASP

Open Web Application Security Project

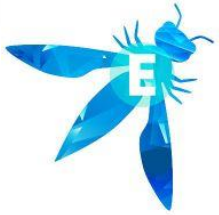
Chapter 2
Future State of Security



It's over

OWASP
Open Web Application Security Project

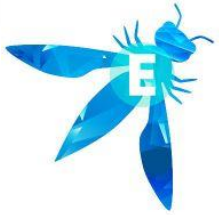
- Traditional ways of protecting our networks are not working anymore
- The victory of **300 Spartans** is a not quite true:
  - 300 Spartans
  - 700 Thespians
  - 400 Thebans
  - and perhaps a few hundred others
  - most of whom were **killed**.



But people say

OWASP
Open Web Application Security Project

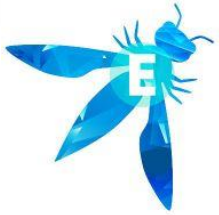
- Waving the white flag means you've lost
- You're compromised and you don't even know it.
  Are you a **target**?



Start being afraid of the right things

OWASP
Open Web Application Security Project

- 80%+ percent of you problems come from 20% of you issues
- Exploiting the 20% problems left would require some skills
- It's **OK** to fail.
- It's **NOT OK** not to know that you have failed or failing over and over again

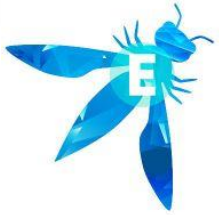


Understand what you are trying to protect

Next steps

OWASP
Open Web Application Security Project

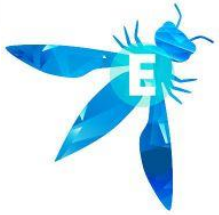
- Artificial intelligence
- Self-protecting mechanism just like the human immune system
- Shape-shifting networks
- Big Data
- Advanced Honeypots
- **On the fly patching**



Next steps

OWASP
Open Web Application Security Project

- Listening
- Learning
- Doing



The future is here

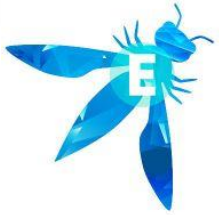
OWASP
Open Web Application Security Project

- Checkout DARPA Cyber Grand Challenge

The challenge:

Systems will autonomously create network defenses, deploy patches and mitigations, monitor the network, and evaluate the defenses of competitors.

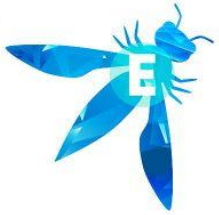
- Sounds like something the US would do ☺



OWASP
Open Web Application Security Project

What we will need to do

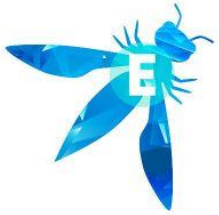
- Gather **all** information
- From **all** devices
- Process that information
- Identify malicious events and patterns
- Establish automated alerts
- Establish automated decisions and actions



What we will need to do

OWASP
Open Web Application Security Project

- Establish correct incident response plans
- Create production like environments
- Add this layer on top of the old layers
- Automate as much as you can



Q&A

OWASP
Open Web Application Security Project

Wait, what are you trying to say?