Who Am I?

Shaul Holtzman

• Headed cybersecurity training operations in the Israeli Defense Force (IDF)

• Former incident response analyst at Verint

• Account and Intezer Analyze community manager

@ShaulHol
The Needle in the Haystack

SO. MANY. ALERTS.
Common Solutions

Beautify

Playbooks
Common Solutions

**Beautify**

1) Better looking SIEM UI

2) Organize and cluster alerts

3) Additional metadata on alerts

**PROBLEM:** It’s just a bit more convenient. Many alerts are still not handled.
Common Solutions

Playbooks

1) Automatic playbooks for handling alerts

2) Utilizes external security systems for analysis and response

PROBLEM: If you don’t have the “brains”, automation is limited to simple cases.
In an ideal world, we would deeply investigate each alert.
Alert Analysis

Files

A handy team of reverse engineers would be able to answer the most critical questions about each alert:

1) Is it good or bad?

2) What is the risk level or priority?

3) What is the goal of the attacker?

4) Is the threat related to a previous incident we had?
Automating Malware Analysis & Reverse Engineering

How is that possible?
Software is Evolutionary

• Just like in biology, software has ancestral relations

• Every piece of software is based on previously written code

• Detecting code reuse is equivalent to mapping the DNA of an organism
Genetic Malware Analysis
Code Genome Database

Malware

Trusted software
Genetic Malware Analysis

Unknown file → Extracting genes → Code genome database containing billions of genes → Identifying and classifying unknown and reused code

File → Malicious ZeuS Malware → Trusted Microsoft
Genetic Malware Analysis

- Code from Adobe Photoshop 10.0
- Code from ZeuS malware
- Never before seen piece of code
- Common code seen previously in 462 applications
Examples

SHOW ME WHAT YOU GOT!
Emotet

1) Most common banking trojan in the world
2) Self-propagation and password guessing
3) Modular malware
4) Steals banking details, reads emails, passwords and browser history
5) Packed with custom packer
Straw-by-Straw Analysis & Response

- Automatically upload any file or hash from SIEM/SOAR/other
  - Suspicious file or hash
  - Genetic Analysis detects shared code w/ Emotet
    - Auto generates YARA from unique/malicious code
      - Classifies file as Emotet & sets alert priority to critical
  - Search for additional infections w/ YARA
    - Confirms file is malicious
Improves Every Stage of IR Cycle

NIST “Computer Security Incident Handling Guide”
Summary

1) We should not compromise on investigating only a handful of alerts

2) We can use automated malware analysis solutions and implement integrations to achieve that

3) Genetic Malware Analysis is an effective way to automatically reverse engineer any suspicious file, at scale
Thank You!

You’re welcome to contact us:

programs@intezer.com
@IntezerLabs