TRAINING

HUNT APTS WITH YARA LIKE A GREAT NINJA

COSTIN RAIU
Director,
Global Research & Analysis Team, Kaspersky Lab

VITALY KAMLUK
Principal Security Researcher,
Global Research& Analysis Team, Kaspersky Lab

SERGEY MINEEV
Principal Security Researcher,
Global Research & Analysis Team, Kaspersky Lab

$2 700

(price includes hotel accommodation, breakfast, lunch and coffee breaks, and does not include SAS 2017 pass)

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

Have you ever wondered how Kaspersky Lab discovered some of the world's most famous APT attacks? Now, the answer is within your reach. This training will lead you through one of the essential tools for the APT hunter: the Yara detection engine.

If you've wondered how to master Yara and how to achieve a new level of knowledge in APT detection, mitigation and response, it all breaks down to a couple of secret ingredients. One of them is our private stash of Yara rules for hunting advanced malware.

During this training you will learn how to write the most effective Yara rules, how to test them and improve them to the point where they find threats that nobody else does. During the training you will gain access to some of our internal tools and learn how to maximize your knowledge for building effective APT detection strategies with Yara.

TOPICS COVERED

- Brief intro into into Yara syntax
- Tips & tricks to create fast and effective rules
- Yara-generators
- Testing Yara rules for false positives
- Hunting new undetected samples on VT
- Using external modules within Yara for effective hunting
- Anomaly search
- Lots (!) of real-life examples
- A set of exercises for improving your Yara skills

CLASS REQUIREMENTS

Level:
medium and advanced

Prerequisites:
knowledge of the Yara language and basic rules

Class:
imited to max 15 participants

Hardware:
Own laptop

Minimum Software to install:
Yara v. 3.4.0

Duration:
2 days

Date:
April 1-2, 2017

TRAINING

MALWARE REVERSE ENGINEERING COURSE

NICO BRULEZ
Principal Security Researcher,
Global Research & Analysis Team, Kaspersky Lab

$5 000

(price includes hotel accommodation, breakfast, lunch and coffee breaks, and does not include SAS 2017 pass)

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

Day 1: Manually unpacking Malware
During the first day, students will focus on unpacking files manually in order to get working executables. Most famous packers will be covered in order to introduce various techniques that can be used on unknown packers. Also known as: How to unpack properly. Once completed, students will work on "malicious packers" and learn how to unpack samples of famous malware families. Nowadays, malware uses custom polymorphic packers to slow down analysis and thwart detection.

Day 2: Static Shellcode Analysis and IDA Primer
The second day focus on extracting shell codes from malicious documents and to reverse engineer them statically. The day focuses on tricks and shortcuts to use in IDA Pro for efficient static analysis, as well as introduction to IDA Python scripts used to speed up static reverse engineering.
A special approach to handle import by hash will be presented to the students, which can be used in many other scenarios.

Day 3-4: APT Reverse Engineering
Using the information learned in the first two days, students will work on several APT samples.
The goal of those two days is to be able to identify the actions of the threats, to be able to document their features and understand how they interact with C&C servers to receive commands.

INTENDED AUDIENCE

This class is intended for students who have been working with malware and doing reverse engineering in the past. Professionals doing Forensics Investigations, Incident Response, Malware Analysis can benefit from the course as long as they have the prerequisites listed below.

CLASS REQUIREMENTS

Level:
medium and advanced

Prerequisites:
Students should be familiar with Debugging and IDA Pro: The class is not an introduction to reverse engineering. Students should be familiar with Assembly: We won't cover assembly basics during the class. Students should have a laptop with required software installed before attending the class. Students should be familiar with VMware Workstation (or the VM of their choice).

Hardware:
- Legit version of IDA Pro (latest version preferred as the instructor uses the latest version)
- Virtual Machine with XP SP3 installed (to avoid troubleshooting tools problems during the class)
- OllyDbg
- Python 2.7 should be installed in both the host and on the guest machine.
- PE Editor (eg: LordPE or your favorite PE editor)
- Hex Editor (eg: Hiew of your favorite hex editor)
- Import Reconstructor/fixer: Imprec, Universal Import Fixer 1.2
- PEID

Class:
limited to max 20 participants

Duration:
4 days

Date:
March 30 through April 2, 2017

TRAINING

DIGITAL INTELLIGENCE GATHERING USING MALTEGO

ROELOF TEMMINGH
Managing Director and Founder, Paterva

PAUL RICHARDS
Lead Developer, Paterva

$2 700

(price includes hotel accommodation, breakfast, lunch and coffee breaks, and does not include SAS 2017 pass)

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

OVERVIEW:

The IT security and intelligence community love Maltego – whether it be mapping a target's infrastructure or profiling a person's sphere of influence.

During this course we will help you unlock the true potential and raw power of Maltego – from helping you to understand the underlying technologies to exploring the full potential of Maltego's analytic capabilities. Join us and we'll show you how to navigate and map the Internet's darkest rivers...

From stalking, finding people and who influence them to uncovering internal IP addresses and technology used at major corporations this course will propel you into the world of open source intelligence feet first. Expect to be shocked out at how much data is 'out there' and what people can do with it as well as how you can reach this data for both defending and attacking.

This is a two-day hands-on course packed with practical exercises using real world data, giving participants real world experience with the tool whilst being trained by the very people that developed the tool. Bring your overalls and expect to get your hands dirty!

INTENDED AUDIENCE

This course offers skillets that apply to almost anyone interested in gathering information and gaining intelligence. Specifically people in the following industries will benefit greatly:

- Open source intelligence
- IT security
- Law enforcement or intelligence
- Data mining

CLASS REQUIREMENTS

Level:
advanced

Hardware:
- Notebook (PC or Mac) with at least 2GB of RAM, a decent resolution display and some space to install the latest version of Maltego.
- External mouse
- Enthusiasm to learn about open source intelligence and what you can do with it

Prerequisites:
Students are required to know common Internet services (like HTTP, DNS), Search engines (basic 'Google hacking'), basic IT security principles (port scanning etc), some scripting or programming experience (Python, PERL) is definitely an advantage!

Class:
limited to max 15 participants

Duration:
2 days

Date:
April 1-2, 2017