



Kaspersky

SECURITY ANALYST SUMMIT

Barcelona, Spain
April 6-9, 2020

E V E N T K I T

KASPERSKY® SECURITY ANALYST SUMMIT 2020

The 12th annual Kaspersky® Security Analyst Summit is an **invite-only** event that attracts high-caliber anti-malware researchers, global law enforcement agencies and CERTs and senior executives from financial services, technology, healthcare, academia and government agencies.

The conference provides an exclusive atmosphere that encourages debate, information sharing and display of cutting-edge research, new technologies, and ways to improve collaboration in the fight against cyber-crime.

SAS 2019 speaker

Andrew “bunnie” Huang
Independent Researcher



Kaspersky® Security Analyst Summit 2020 will discuss the following topics:

- Advanced malware threats
- Mobile device exploitation
- Threats against banks, financial institutions:
 - PoS systems
 - ATMs
 - Crypto-currencies
 - E-commerce data breaches
- Critical infrastructure protection (SCADA/ICS)
- Internet of Things:
 - Autonomous transportation (self-driving cars, drones)
 - Smart homes and smart devices
 - Smart cities
- Attacks on medical devices
- Threats to Gaming industry:
 - Game cheats and defense mechanisms
 - Server and client-side vulnerabilities
 - Industrial espionage targeting gaming industry
 - Mass infections via gaming vendor breach
- Cross-border law-enforcement coordination and information sharing
- Vulnerability discovery and responsible disclosure
- Techniques for development of secure software and systems
- Side Channel and Physical Attack
- Blockchain and smart contracts



#THESASCON BY THE NUMBERS

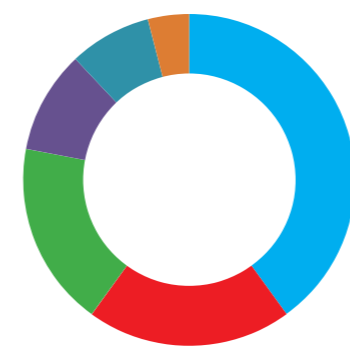
SAS YEAR-OVER-YEAR GROWTH ATTENDANCE HAS GROWN 90% OVER LAST 4 YEARS:

SAS 2017: **290**
 SAS 2018: **350**
 SAS 2019: **450**
 SAS 2020: **Expecting 550**

SOCIAL + PRESS ENGAGEMENTS

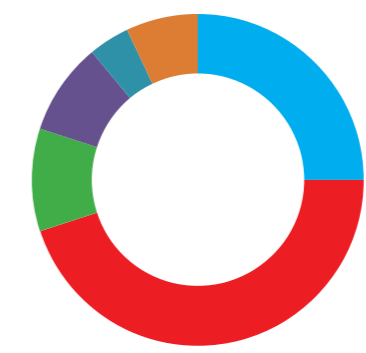
-  **127 000+** Tweets and retweets
-  **75 000+** Facebook Likes
-  **23 000+** LinkedIn Engagements
-  **18 000+** Global News Articles

SECTOR/
INDUSTRY



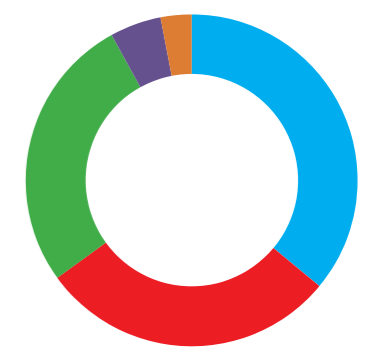
- 40%**  Threat Intelligence
- 20%**  Critical Infrastructure
- 18%**  Government/CRT/LE
- 10%**  Financial
- 8%**  Media and Communications
- 4%**  Healthcare






SAS ATTENDEE
PROFILE



- 25%**  VPs, Security Directors
- 45%**  Treat Intelligence Analysts
- 10%**  Software Developers
- 9%**  CEO/CTO/CISO/Founder
- 4%**  Venture Capital Investors
- 7%**  Press

REGIONS
IN ATTENDANCE



- 36%**  Eupore
- 29%**  North America
- 27%**  APAC
- 5%**  EMEA
- 3%**  Latin America

Attendees from 50+ countries

Sponsors and attendees include representatives from the software vendor community, anti-malware researchers, law enforcement professionals, vulnerability researchers and security response teams.



SAS 2019 speaker



Maddie Stone
Google

SAS 2019 speaker



Luca Bongiorno
Bentley Systems

SAS attendees include trusted, high-profile journalists from the following media brands:

- **Bob McMillan**, Wall Street Journal
- **Jim Finkle**, Reuters
- **Riva Richmond**, The Economist
- **Marcel Rosenbach**, Der Spiegel
- **Karim Salah Amer**, Netflix
- **Andy Greenberg**, Wired
- **Charlie Osborne**, CNET
- **Alp Börü**, BusinessWeek
- **Dan Goodin**, Ars Technica
- **Kelly Jackson Higgins**, Dark Reading
- **Mike Lennon**, SecurityWeek
- **Fahmida Rashid**, Infoworld
- **Violet Blue**, ZDNet
- **Greg Hale**, ISS Source
- **Dennis Fisher**, OnTheWire
- **Sergio López**, Netmedia
- **Sam Jones**, Financial Times
- **Peter Nicolai Devantier**, Computerworld
- **Byron Acohido**, USA Today/Three Certainty
- **Kim Zetter**, Independent Journalist

I had such a wonderful time at SAS. It was an amazing event, both very substantive but also a lot of fun. I hope we can stay in touch and if I ever get another invite to your conference I would be honored to come and speak again or just engage with you guys.

Catherine Lotrionte
Georgetown University

Thank you so very much for having me at SAS. It was a pleasure and an honor to speak at the best security conference I have ever attended. The content was great, the networking was even better, and being in paradise with all of the events was the best.

Chris Sistrunk
Mandiant

This was a brilliant conference and the YARA training was also excellent! Thanks for your awesome hard work on this event.

Chris Firman
CERT-AU



Juan Andres Guerrero-Saade
Chronicle Security



Joe FitzPatrick
SecuringHardware.com



Eva Galperin
Electronic Frontier
Foundation



Peter Kruse
CSIS Security Group

SPONSORSHIP OPPORTUNITIES



Platinum Package

\$30 000

- Three full SAS event passes. Hotel, transfers, meals and all summit activities included.
- One speaking slot (must be vetted by conference organizers).
- Free six-month subscription to Executive Summaries of Kaspersky Security Intelligence Services, plus advanced access to IOC data.
- Table-top or a place for a booth in conference registration area.
- Inclusion of your company's logo in all marketing material (banners, brochures, badges, agenda).
- Back cover AD placement on event program.
- Display of your company's logo on the SAS web site.
- Inclusion of your printed materials in conference package.

Gold Package

\$20 000

- Two full SAS event passes. Hotel, transfers, meals and all summit activities included.
- Free three-month subscription to Executive Summaries of Kaspersky Security Intelligence Services plus advanced access to IOC data.
- Inclusion of your company's logo in all marketing material (banners, brochures, badges and agenda).
- Display of your company's logo on the SAS web site.
- Inclusion of your printed materials in conference package.

Silver Package

\$10 000

- One full SAS event pass. Hotel, transfers, meals and all summit activities included.
- Inclusion of your company's logo in all marketing material (banners, brochures, badges and agenda).
- Display of your company's logo on the SAS web site.
- Inclusion of your printed materials in conference package.

*all prices are in USD



Starting this year, SAS will donate 10% of all proceeds from conference sponsorship sales to the following security community initiatives:



shecodes.ly
She Codes aims to give women in Libya the tools and opportunities to empower their future, be confident and independent. By creating a business that can yield a return on investment as well as a social enterprise that conducts its commercial activities in a way that maximizes the empowerment of the Libyan females.



bilancodes.org
A non-profit striving for gender parity in technology by inspiring, educating and equipping girls in Somali girls with coding & computing skills.



mangrove-foundation.com
An initiative [of Mangrove Capital Partners] acting and encouraging others to act in view of preserving the environment by funding projects to combat climate change and to empower and educate women around the World for the implementation of sustainable practices.



SPONSORSHIP PACKAGES ALSO AVAILABLE FOR:



SAS UNPLUGGED

SAS Unplugged is an adjoining mini-conference providing workshops, presentations, technical classes, career advice, and interactive games and challenges to the local security community.

CAPTURE THE FLAG

A **capture the flag (CTF)** contest is a competition for cybersecurity experts organized in the form of a game, in which the participants solve computer security problems. They must either capture (attack/bring down) or defend computer systems in a CTF environment. Typically, these competitions are team-based and attract a diverse range of participants, including students, enthusiasts and professionals.

#TheSAS2020 CTF is a unique cybersecurity challenge that combines ICS/IOT/smart-home hacking challenges with traditional CTF components to expand the range of challenges to the teams of players.




Dedicated session sponsorships:

- Lanyard sponsorships
- Breakfast and lunch sponsorships
- Media room and Wi-Fi sponsorships
- Full-page ads in conference brochure
- Gala dinner sponsorship





PARTICIPATION OPPORTUNITIES

	REDUCED PACKAGE	STANDARD PACKAGE
SAS conference pass	✓	✓
Hotel accomodation 3 nights (April 6-9, 2020)		
Welcome dinner (arrival day)	✓	✓
Ice-breaking party (1st conference day)	✓	✓
Gala dinner (2nd conference day)	✓	✓
EARLY-BIRD (ends December 10, 2019)	\$1 800	\$2 400
REGULAR (ends on April 4, 2020)	\$2 000	\$2 600
ON-SITE (ends on April 7, 2020)	\$2 100	\$2 700

T R A I N I N G



HUNT APTS WITH YARA LIKE A GREAT NINJA

COSTIN RAIU

Director,
Global Research & Analysis Team
Kaspersky



SERGEY MINEEV

Principal Security Researcher,
Global Research & Analysis Team
Kaspersky



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 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

Hardware:
Own laptop

Minimum Software to install:
Yara v. 3.6.0

Class:
Limited to max 15 participants

Duration:
2 days

Date:
April 5-6, 2020

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

T R A I N I N G

THE GOD-MODE PRACTICAL TRAINING IN STATIC ANALYSIS OF APT MALWARE

IGOR SOUMENKOV

Principal Security Researcher,
Global Research & Analysis Team
Kaspersky



BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!



Every flashy new computer incident involving previously unseen malicious code boils down to one question: 'what are the attackers trying to do?' Answering this question requires a keen investigative mind and skills to match in order to determine the functionality of that code and boil it down into actionable artifacts: either a basic set of IOCs or a complete technical description that reveals the TTPs of the attackers. With these products in hand, an organization can proactively defend against the most cutting-edge attackers.

Easier said than done. Organizations affected by a true APT-level attack will require a deep understanding of the APT toolkit to truly understand the extent of the capabilities and intentions of the determined intruders. Only with this can they ever be sure that their damage assessment and incident response efforts are accurate and effective. The only way to reach this level of understanding with true fidelity is to statically analyze the malicious code (no "if's", "and's", or dynamic "but's" about it).

Unlike easier dynamic analysis techniques, Advanced Static Analysis allows to produce high fidelity descriptions of the executable code regardless of execution flow and tricky runtime checks. It allows analysts to produce an extensive set of actionable items, including lists of C&C servers, file and memory signatures, crypto implementations and more. A combined understanding of unique code sequences and algorithm employed by the malware developers is key in malware classification, toolset attribution, and the creation of the most advanced hunting signatures.

This course will cover most of the steps required to analyze a modern APT toolkit, from receiving the initial sample, all the way to producing a deep technical description with IOCs. The course material is based on many years of experience analysing the most complex threats ever discovered in-the-wild, including: Equation, Red October, Sofacy, Turla, Duqu, Carbanak, ShadowPad, and many more. It's time to set your static analysis game to God-Mode.

TOPICS

- Unpacking
- Decryption
- Developing own decryptors for common scenarios
- Byte code decompilation
- Code decomposition
- Disassembly
- Reconstruction of modern APT architectures
- Recognizing typical code constructs
- Identification of cryptographic and compression algorithms
- Classification and attribution based on code and data
- Class and structure reconstruction
- APT plugin architectures (based on recent APT samples)

CLASS REQUIREMENTS

Level:
Medium and Advanced

Prerequisites:

- Understanding of x86 and x86_64 assembly, Python
- Basic knowledge of C/C++
- Experience with analysing code in IDA Pro

Hardware & Software requirements:

- Laptop with VMWare / VirtualBox virtualization solution
- Legitimate copy of IDA Pro (latest version preferred)
- Working C/C++ compiler toolset: clang, g++, mingw

Class:
Limited to max 15 participants

Duration:
2 days

Date:
April 5-6, 2020

T R A I N I N G

THE GOOD AND THE GREAT – STEPPING UP YOUR THREAT INTELLIGENCE GAME

BRIAN BARTHOLOMEW

Principal Security Researcher,
Global Research & Analysis Team
Kaspersky



BRIAN CANDLISH

Principal Threat Researcher
Telstra Threat Labs



In the past decade, 'threat intelligence' has become one of the hottest commodities in the infosec market for companies to either purchase or create. As a threat intel analyst, one must be a Jack-Of-All-Trades, without over-specializing in any one thing. Unfortunately, there are few guidelines and fewer training courses for analysts to obtain a solid foundation. Even seasoned threat intel analysts find themselves creating specific tools to accomplish a task, only to find out that someone else has already done so. And in those rare cases where expert analysts are stumped, who can they turn to for guidance? This course is designed to serve threat intel analysts of all levels of experience, providing a solid foundation for beginner-to-intermediate intel analysts, as well as showing more advanced analysts how the Global Research and Analysis Team (GRaT) conducts their research in special fringe cases.

The course will span two full days and cover the entire gamut of threat intelligence. Some of the topics covered include:

- Concepts of threat intelligence
- Intelligence life cycle
- Defining intelligence requirements
- Collecting and processing data
- Maximizing data through automation
- Open source / custom tools
- Threat hunting in large security datasets
- Intelligence reporting
- Dealing with biases
- Using estimative language
- Each day will end with large hands-on labs (approx. 2 hrs each)

CLASS REQUIREMENTS

Level:
Intermediate or above

Prerequisites:
Students should be interested in learning about the many aspects of threat intelligence. Preferably, the student should be part of a threat intel team as an analyst or lead. Familiarity with commercial and open source tools such as VirusTotal, PassiveTotal, or DomainTools is helpful. Experience hunting threats and analyzing malware considered a plus.

Each student should have their own laptop with access to whatever tools they use on a daily basis. Students will be provided access to other tools as needed during the class

Hardware:
Laptop with a minimum 20GB free space HD and 8GB RAM capable of running VMs

Minimum Software to install:
Windows / MacOS / Linux equivalent
VMWare / Virtualbox

Class:
Limited to max 15 participants

Duration:
2 days

Date:
April 5-6, 2020

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

T R A I N I N G



REMOTE FORENSICS FOR THE MODERN MALWARE HUNTER

VITALY KAMLUK

Principal Security Researcher,
Global Research & Analysis Team
Kaspersky



NICOLAS COLLERY

Head of Offensive Security Services
DBS Bank



BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

The increased frequency and complexity of advanced cyberattacks require swift response and silent navigation through compromised assets of sometimes large distributed networks. One of most popular approaches today relies on EDR or other live agent-based solutions. This is useful when responding to attacks by low skilled or below-average adversaries. However, the activation of security agents and activities on live compromised systems may trigger the attacker's alerts, which may lead to a massive cleanup operation and destruction of evidence. Offline system analysis, on the other hand, may not be easy due to physical distance to the compromised system or scale of the network. This is where remote offline digital forensics becomes an incredible useful approach.

This training introduces the free, open-source forensics tool Bitscout. Attendees will learn how to build their own remote analysis tool, package with their own arsenal and how to handle customizations.

The training will be conducted by the author of the tool.

CLASS PLAN:

1. Introduction and theory
2. Building your own remote ninja tool
3. Exercises:
 - Discovering malware remotely
 - Finding attack infection vectors
 - Remote disk image acquisition methods
 - Virtualization-based wizardry
 - Breaking through proprietary disk encryption
 - Analyzing non-Windows platforms
 - Converting compromised host into safe honeypot

CLASS REQUIREMENTS

Level:
Medium and Advanced

Prerequisites:

- Familiarity with digital forensics principles
- Malware analysis and basic reversing skills
- Understanding of virtualization, networking, OS architecture, coding and scripting

Hardware & Software requirements:
Laptop or VM with Debian-based Linux, i.e. Ubuntu

Class:
Limited to max 15 participants

Duration:
2 days

Date:
April 5-6, 2020

T R A I N I N G

BODY LANGUAGE AND NONVERBAL SKILLS FOR SOCIAL ENGINEERS AND RED TEAMS

ALEX FRAPPIER

Cyber Security Speaker and Trainer
CanCyber Foundation



TYLER MCLELLAN

Director of Cyber Threat Intelligence
CanCyber Foundation



BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!

Learn how to master and detect nonverbal skills used by social engineers and red teams during physical engagements. While you may be a master hacker when you are able to get your hands on the technology or keyboard, you will not have success if you are not able to get the physical access you require.

Body language plays an essential role in human communication and interactions.

Understanding nonverbal communication will allow you to look more confident, convincing, charismatic, while avoiding common indicators of deception. These skills will have a major impact as a social engineer should you be doing impersonation, voice elicitation (vishing) or physical access. Perhaps more importantly, you will also learn how to decode when someone uses these skills against you and if the other person may be lying to gain access to your company. Combined with core knowledge in influence and elicitation, this training will empower you to take your skills to a whole new level, either on offense or defence.

You will learn science based laws of nonverbal communication, including : trust indicators, negative nonverbal, vocal power, and deception detection. See how these can be successfully applied to cybersecurity and physical security, but also learn how use them in your day to day work in making you a better presenter and negotiator.

Be prepared for a hands-on training that will include core knowledge, fun activities, and opportunities to practice. It will be valuable and adapted to both introverts and extroverts.

INTENDED AUDIENCE

Security researchers and incident response personnel, malware analysts, security engineers, network security analysts, APT hunters and IT security staff.

TOPICS COVERED

Body Language Laws:

- Introduction to body language
- Nonverbal foundation
- Trust indicators
- Haptics
- Gazing
- Proxemics
- Power nonverbal
- Vocal laws
- Facial macro and micro expressions
- Micro positives
- Micro Negatives

Applications:

- Impersonation
- Voice elicitation
- Deception detection
- Pitching
- Negotiations
- Presentation skills

CLASS REQUIREMENTS

Level:

Suitable for Beginner to Advanced

Prerequisites:

There are no prerequisites for this training

Hardware & Software requirements:

Own laptop

Class:

Limited to max 20 participants

Duration:

2 days

Date:

April 5-6, 2020

T R A I N I N G



IOT VULNERABILITY RESEARCH AND EXPLOITATION TRAINING

ROLAND SAKO

Security Researcher
Kaspersky ICS CERT



ANDREY MURAVITSKY

Security Researcher
Kaspersky ICS CERT



Approaching IoT devices from a security assessment standpoint can be intimidating, especially when you need to work hands-on with hardware but fear not! This is the training for you, if you want to take your first steps into how to discover vulnerabilities in any smart devices: homes, cars, routers, PLC's, medical equipment and other IoT devices.

We will guide you through systematic analysis of IoT devices to identify vulnerabilities. You will interact directly with many hardware interfaces, and become comfortable with using the hardware and software tools of the trade to pentest and evaluate IoT devices.

After the training, you will be able to analyze and exploit the hardware and software attack surface of IoT devices to secure them. Going forward you will tackle most situations confidently, including when the firmware is not publicly available.

INTENDED AUDIENCE

This course is for all security researchers, product security teams, software and security architects, and product managers (with a security background).

TOPICS COVERED

- Extracting and analyzing firmware
- Understanding PCB chip identification
- Reverse engineering ARM binaries
- Identifying and working with unknown architectures
- Emulating firmware
- Identifying pinsPin identification
- Mastering / Gaining confidence with communication protocols and interfaces (UART, SPI, JTAG, I2C, BLE)
- Analyzing and fuzzing open source code
- Automating vulnerability identification

Each part of the course consists of a mix of theory backed by relevant practical tasks.

CLASS REQUIREMENTS

Level:
Beginner to Intermediate

Prerequisites:

- Experience with any programming language
- Familiarity with basic Linux commands
- Basic knowledge of C and/or C++
- Basic reverse engineering skills
- Knowledge of / Grasp of the most common network protocols

Experience using a disassembly tool would be helpful, but not necessary

Hardware:
A laptop with at least 20GB of free space, 4GB of ram and two USB Type-A ports available

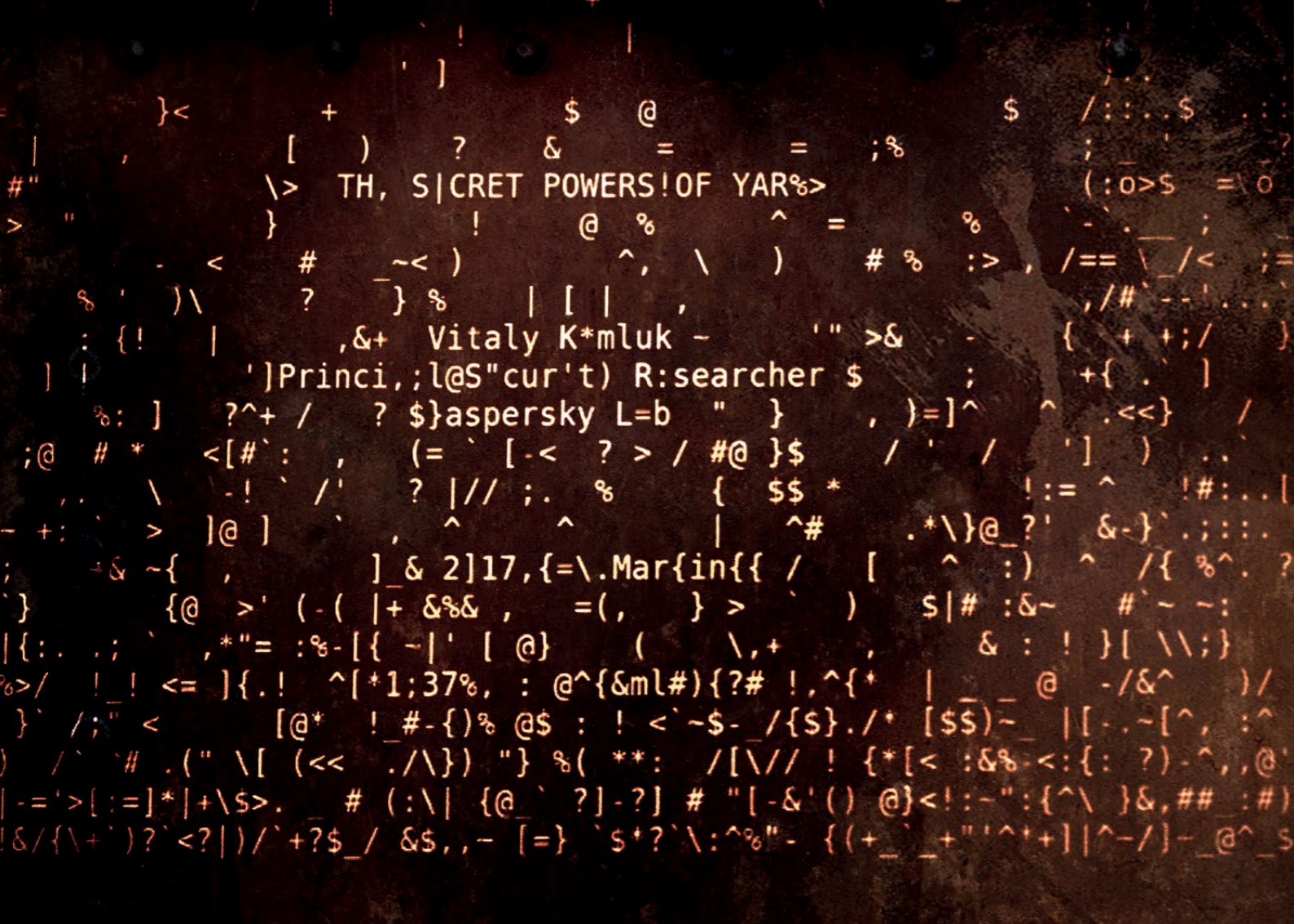
Minimum Software to install:
Virtual Box and admin access to install additional software

Class:
Limited to 20 max participants


Duration:
2 days

Date:
April 5-6, 2020

BOOK EARLY AND GET A DISCOUNT ON SAS CONFERENCE PRICING!



TRAINING COURSE FEES

	REDUCED PACKAGE	FULL PACKAGE
SAS 2020 training fee	✓	✓
Hotel accomodation 2 nights + breakfast (April 4-6, 2020)		
Lunches & coffee-breaks	✓	✓
EARLY-BIRD (ends December 10, 2019)	\$2 000	\$2 500
REGULAR (ends on April 1, 2020)	\$2 300	\$2 800
ON-SITE (ends on April 4, 2020)	\$2 400	\$2 900



LOCATION

Barcelona, Spain
April 6-9, 2020

Hilton Diagonal Mar Barcelona

Passeig del Taulat, 262-264,
08019 Barcelona, Spain



CONTACTS

sas2020@kaspersky.com
thesascon.com

[#TheSAS2020](https://twitter.com/TheSAS2020)