Spænd ben for statsstøttede cyber-kriminelle – AI er næste udfordring

28. april - Experimentarium,

08:45 - 08:50	**Welcome and opening remarks** Andrew Lee, Director of Government Affairs, ESET
08:50 - 09:20	**Boogie down with Rook ransomware - a case study** Peter Kruse, Sikkerhedsekspert, Kruse Industries
09:20 - 09:35	**Live Q&A**
09:35 - 09:55	**The war in Ukraine and cyber: what we've seen, what we haven't and what to expect** Arthur de Liedekerke, Project Manager, Rasmussen Global
09:55 - 10:10	**Live Q&A**
10:10 - 10:40	**How APT groups have turned Ukraine into a cyber battlefield** Robert Lipovsky, Principal Threat Intelligence Researcher, ESET
10:40 - 10:55	**Live Q&A**
10:55 - 11:15	**Coffee break**
11:15 - 11:45	**The European Union Agency for Cybersecurity (ENISA) Efforts on AI Cybersecurity** Monika Adamczyk, Cybersecurity Expert, ENISA
11:45 - 12:00	**Live Q&A**
12:00 - 12:30	**SparrowDoor: A new variant**
12:30 - 12:45	**Live Q&A**
12:45 - 14:00	**Lunch**
14:00 - 14:30	**Will machine learning improve or disrupt the cybersecurity equilibrium?** Juraj Jánošík, Malware Analyst,, ESET
14:30 - 14:45	**Live Q&A**
14:45 - 15:15	**Zooming in on the current threatscape** Ondrej Kubovič, Security Awareness Specialist, ESET
15:15 - 15:30	**Live Q&A**
15:30 - 15:45	**Conference closing** Andrew Lee, Director of Government Affairs, ESET

08:45 - 08:50: Welcome and opening remarks



Andrew Lee
Director of Government Affairs
ESET / Partner

08:50 - 09:20: Boogie down with Rook ransomware - a case study



Peter Kruse
Sikkerhedsekspert
Kruse Industries / Keynote

This presentation focuses on an incident response that we conducted for a customer. It is a case study that looks at the technical parts of the malware, the intrusion of the network and exfiltration of data, launching the ransomware and events that followed.

Rook is based on the leaked Babuk ransomware code that was posted to a Russian underground forum in September 2021.

This is a step-by-step case study into a real-life incident response event and the days that followed after the attack.

09:20 - 09:35: Live Q&A

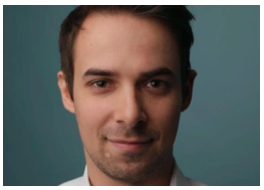
09:35 - 09:55: The war in Ukraine and cyber: what we've seen, what we haven't and what to expect



Arthur de Liedekerke
Project Manager
Rasmussen Global / Partner

09:55 - 10:10: Live Q&A

10:10 - 10:40: How APT groups have turned Ukraine into a cyber battlefield



Robert Lipovsky
Principal Threat Intelligence Researcher
ESET / Partner

With the brutal escalation of the war against Ukraine, we take a closer look at the 'cyber' part of it. What has been happening in Ukraine? Could the cyberwar spill over to other European countries? Should users be worried? Join us to learn about the most important cyberattacks related to the armed conflict – in the past weeks, as well as in the past eight years.

10:40 - 10:55: Live Q&A

10:55 - 11:15: Coffee break

11:15 - 11:45: The European Union Agency for Cybersecurity (ENISA) Efforts on AI Cybersecurity



Monika Adamczyk
Cybersecurity Expert
ENISA / Partner

Emerging technologies, such as AI are in the epicentre of the digital evolution. While they bring numerous benefits they also bring many risks that need to be addressed to ensure a secure and trustworthy environment. In its role as the Union's agency dedicated to achieving a high comment level of cybersecurity across Europe, ENISA has been actively working for the last few years on mapping the AI cybersecurity ecosystem and provding security recommendations for the forseen challenges.

11:45 - 12:00: Live Q&A

12:00 - 12:30: SparrowDoor: A new variant

NCSC Malware Team

12:30 - 12:45: Live Q&A

12:45 - 14:00: Lunch

14:00 - 14:30: Will machine learning improve or disrupt the cybersecurity equilibrium?

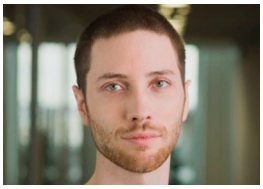


Juraj Jánošík
Malware Analyst,
ESET / Partner

While the idea of artificial intelligence and machine learning have been influencing various fields for decades now, their full transformative potential is yet to be realized. ML-based technologies increasingly help fight large-scale fraud, evaluate and optimize business processes, improve testing procedures and develop new solutions to existing problems. We, at ESET, recognized its potential early on and employed it to improve malware detection over 20 years ago. To this day, this symbiosis continues, various machine-learning technologies being an integral part of the ESETs protective layers. Like most innovations, however, even machine learning has drawbacks and limitations. Unfortunately, technological advances are not exclusively available to cybersecurity defenders. Cybercriminals are aware of the new prospects too and do not hesitate to utilize ML-based technologies to make their malicious code and activities more efficient. The question for the future remains, will the pros of machine learning outweigh the cons or will the technology lead to major disruption and deterioration of the cybersecurity equilibrium.

14:30 - 14:45: Live Q&A

14:45 - 15:15: Zooming in on the current threatscape



Ondrej Kubovič
Security Awareness Specialist
ESET / Partner

Hundreds of billions of password guesses aiming to break the protection of RDP remote access, the resurrection of Emotet, a threat described by Europol as the "most dangerous malware in the world" and over 400 % increase in Android banking malware year-over-year: those are just a few of the trends seen by ESET in the last months of 2021. And that is on top of the cyberespionage activity of groups such as The Dukes, OilRig, and others. Join our talk and find out what were the latest threats and trends detected by ESET.

15:15 - 15:30: Live Q&A

15:30 - 15:45: Conference closing



Andrew Lee
Director of Government Affairs
ESET / Partner