T05_08/10/2020 **ACTIVITY CURRICULUM**	**Malware Investigation** **38/2021** **CEPOL** **20-24 September 2021** **NOK ITC, Budapest, Hungary**

Organiser/Host (name and address)	CEPOL with the support of ECTEG
Host (name and address)	CEPOL Cybercrime Academy hosted at International Training Centre (NOK-ITC) Böszörményi Street 21., H-1126 Budapest
Online Platform	CEPOL's Law Enforcement Education Platform (LEED)
Activity Manager (name and contact)	Ionut STOICA Ionut Stoica@cepol.europa.eu
Assistant(s) (name and contact)	Magdolna Szabo Magdolna.szabo@cepol.europa.eu
Number of Participants	Up to 26
Number of Trainers	2
Overall Aim	To enhance cyber-investigation by obtaining information from the malware analysis process that will help locate criminals and their infrastructure. Note: This course does not address reverse engineering and the disassembly of binary files.
Target group	Law enforcement officers who have a good knowledge of Digital Forensics, Computer Networking and the Microsoft Windows OS Architecture.
Learning Strategy	The learning strategy is focused to support the participants to achieve the learning outcomes by following a learner-centred approach and interactive, participatory, practical and experiential principles in accordance with andragogic theory. The activity involves didactic learning through presentations by subject matter experts, practical exercises and experiential learning by group work.
Assessment Strategy	In order to ensure the participants in this residential training activity will indeed meet the target group requirements, they are asked to complete the Participant Profile for pre-selection. The participants will complete daily evaluation at the end of each day. A summative assessment will be conducted by the participants at the end of the activity in form of online feedback, which is a condition for receiving the Attendance Certificate. The outcomes will feed into a Trainers' Report, which will be used for quality enhancement of the activity in future.

Learning Outcomes	After completion of the training activity, the participant will be able to: 1. Create malware from a construction kit and deploy malware in a controlled lab environment; 2. Demonstrate malware extraction techniques to identify infected machines; 3. Apply the malware analysis process to a malware sample; 4. Document the malware analysis process for evidential purposes; 5. Determine the botnet architecture of a malware sample from network analysis; 6. Explain the botnet takedown methodology for each architecture type; 7. Build a sinkhole server for deployment in a botnet takedown; 8. Utilise OSINT techniques to identify criminals and enumerate their infrastructure. Note on Mandatory Assessment: Formative or summative test assessing the gained knowledge of participants shall be conducted in the framework of the course as a mandatory measure.	
Methods	☒ Kick-off webinar ☒ Presentations ☒ Practical exercise ☒ Assignments	☒ Group Work ☒ Live Discussions ☒ Platform Discussions (in writing) ☐ Role-play
Pre-activity assignments on LMS	☐ Reading Lists ☒ Recorded Webinars	☐ Assignments ☐ Online Modules
Use of CEPOL LEEd (LMS) during the residential stage is mandatory for participants evaluation		
Post learning activities	TBC	
Additional language to English	n/a	
Duration	Days: 5	Training Hours (residential): 30 Total (including pre and post course):
Learning environment	Training activity will take place in CEPOL Cybercrime Academy (CCA) hosted @ NOK ITC at address mentioned above. One classroom for 26 participants, equipped with desktops and presentation equipment.	
Other Remarks	n/a	