This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SEC-2016-2017-1, under grant agreement no 740685.

I-LEAD

WP4 Report

Recommendations on Standardisation and Procurement in the Area of

Cyber Extortion: Crime-as-a-Service

Report number	Crime as a Service WP4 report	
Version:	1.0	
Delivery date:	05.01.2021	
Dissemination level:	Public	
Classification level:	Unclassified	
Status	Final	
Nature:	Report	
Main author(s):	Bartosz Kożuch	Polish Platform for Homeland Security
Contributor(s):	Rashel Talukder	Polish Platform for Homeland Security
	Natalia Jarmużek-Troczyńska	Polish Platform for Homeland Security
	Paul Folten	The Royal Netherlands Standardization Institute (NEN)
	Tom Hoogendijk	The Secretary of CEN/TC 419 "Forensic Science Processes"

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	30.09.2020	Bartosz Kozuch	First version
0.2	01.10.2020	Rashel Talukder Natalia Jarmużek-Troczyńska	First review, added points to the report
0.2	09.12.2020	Paul Folten Tom Hoogendijk	Updates on standardisation and procurement state of the art
1.0	05.01.2021	Bartosz Kożuch	Finalisation of the documents and adapting the remarks.

DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.

This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

Document was prepared in cooperation with FORMOBILE Project – From Mobile Phones to Court (H2020-SU-SEC-2018, under grant agreement no. 832800)

WP4 report
Recommendations on Standardisation and Procurement in the field of Crime-as-a-Service

1. I-LEAD abstract

The i-LEAD, (Innovation – Law Enforcement Agencies Dialogue) is a coordination and support action project funded by the European Commission through the Horizon 2020 Programme. The main aim of the project is to develop a Pan European Network of practitioners and other actors in the field of security, to:

1) Monitor research and innovation projects - with a view to recommending the uptake or the industrialisation of the results.
2) Express common requirements of Law Enforcement Agencies (LEAs) with regards to capability gaps and determine innovative and fit for purpose solutions to address the gaps and improve future performance.
3) Indicate priorities regarding domains requiring more standardisation.

The official start of the 5-year project was September 2017 and is coordinated by the Dutch National Police and consists of a consortium of 19 partners.

The i-LEAD project will build LEA community networks, around 5 specific key Practitioner Groups; these being:

- Front Line Policing
- Cross Border Crime
- Cybercrime
- Crime & Intelligence
- Forensics

More information about the project at can be found at: www.i-lead.eu

2. WP4 description

Work Package 4 (WP4) is viewed as the supporting department for the i-LEAD project. It will liaise with practitioners of the community networks to determine the present situation with regards to standardisation, and if relevant and required, put forward recommendations for the development of existing standards or the creation of new standards.

This objective is to support LEAs within Europe to strengthen cross border cooperation in the fight against crime and terrorism - via the standardisation of technologies, procedures and processes. This covers the activities of; criminal investigation, offender detection and the gathering and submission of evidence that is acceptable by courts of law.

Further, EU-wide standards will also enable economy of scale advantages for both LEAs and suppliers (industry and SME's) of technologies, tools, systems and services, as the same product will meet the requirements of each LEA (in most) of the EU Member States. For that reason, developing new tools and solutions will be more cost-effective. Finally, common standards will also accelerate pre-commercial procurement (PCP) and public procurement of novel solutions and products.

WP4 is designed to meet the following main objectives:

- Examine the opportunities for standardisation as the result of Practitioner Group workshops
- Build the European LEA capacity and knowledge for joint procurement actions
- Accelerate the process of joint PCP and PPI projects.

3. Crime-as-a-Service - Introduction to the topic

Cyberattacks and cyber treats have become a regular occurrence. According to SonicWall 9.9 billion malware attacks, 187.9 million ransomware attacks and 4 trillion intrusion attempts were detected globally in 2019. Cybercriminals are taking advantage of the ever-increasing internet usage and devices that are linked to the internet, using new technologies, methods and strategies to commit cybercrimes. An example of a new method is 'Formjacking', which can be seen as a new type of (digital) Skimming. With the number of web shops increasing, this is an attractive option for the cybercriminal. Other developments include browser-based Malware which contains evil cryto-miners, more aggressive Ransomware, more sophisticated DDos attacks and more advanced hacking methods which contains social engineering and the list goes on. Another growing trend is the commercializing of cyber criminality so-called Crime-as-a-Service, in which the 'as-a-Service' part is based on business models from the legal corporate culture and incorporated in cybercriminal markets (underground economy). The aim is to provide easier access to digital means for the lesser skilled cybercriminal to achieve cybercrime. This lowering of the threshold may lead to an increase in the number of cybercrimes committed. The following figure shows an example of a CaaS.

On these flourishing 'underground' markets, a broad array of tools and services are offered. The cybercriminal can choose to purchase or rent entire packages, so-called 'toolkits', or to buy or rent parts of the toolkit. These toolkits can include malicious software, supporting infrastructure, stolen personal and financial data and the means to monetize criminal assets. The prices for these 'services' are completely out of proportion to the damage they can cause and can be paid by anyone who has a little bit of money and enough motivation for bad intentions.

To investigate and disrupt these criminal activities, it is essential to understand what important (indispensable) enablers and actors are regarding CaaS schemes.

- Forums, websites and dark markets- The CaaS scheme is highly dependent on websites, forums, market places and hubs where supply and demand meet. These are pre-eminently suitable places to buy/sell products and services, advertise, network, share experience and expertise.
- Supportive infrastructures – To stay under the radar from Law Enforcement, cybercriminals require infrastructure which provide a high level of anonymity and security. Hosting providers have a crucial role providing secure storage, especially Bullet-proof hosting services (BpHS). According to Europol, 'they are highly sought after in online marketplaces'. VPN and proxy services have an important part in providing anonymity to cybercriminals, as well as the TOR browser contribute in making it more difficult to trace.
- Actors- First level : Administrators, experts (e.g. creators/code writers of malicious software)

As mentioned earlier, the CaaS scheme provides easier access to digital means for the lesser skilled cybercriminal to achieve cybercrime. This lowering of the threshold can lead to an increase in the number of cybercrimes committed. At the same time, various services that anonymize criminal activities, such as BpHS, disrupt police investigations. As Europol describes, the demand of these type of services is increasing, which in turn disrupts the investigations even more and making it more complex. The experts or code writers often stay off the LEA radar, because they outsource their criminal activities. Moreover, due to the diversity of the crimes involved, the organized criminal structure of CaaS and even more geographical diffusion of the crimes involved, investigations are very time consuming and difficult to solve. How will Crime-as-a-Service effect the future of policing.

4. State of the art in the field of Crime-as-a-Service in terms of standardisation and procurement

Relevant standards:

- **ISO/IEC 27001:2013**, reviewed and confirmed in 2019: *Information technology — Security techniques — Information security management systems — Requirements*
  - This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.
- **ISO/IEC CD 27032,** *Information Technology — Cybersecurity — Guidelines for Internet Security*
  - This document is under development and expected late 2021.
- **ISO/IEC 27035 series**, *Information technology — Security techniques — Information security incident management*
  - This series provides basic principles for information security incident management (Part 1), Guidelines to plan and prepare (Part 2), Guidelines for response operations (Part 3) and Coordination (Part 4)
  - Part 1 and 2 are currently being reviewed, Part 3 has only recently been published, Part 4 is now being developed.
- **ISO/IEC 27042:2015:** *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*
  - This document provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.
  - This document is currently under vote for review.
- **ISO/IEC 27043:2015**, reviewed and confirmed in 2020: *Information technology — Security techniques — Incident investigation principles and processes*
  - This document provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence.
- **ISO/IEC TR 27103:2018,** *Information technology — Security techniques — Cybersecurity and ISO and IEC Standards*
  - This document provides guidance on how to leverage existing standards in a cybersecurity framework.

Relevant TCs:
- ISO/IEC JTC 1/SC 27: 'Information security, cybersecurity and privacy protection'

5. Recommendations on standardisation and procurement in the field of Crime-as-a-Service, concentrating on the 'THOR' dimensions (*technical, human, organisational and regulatory*)				
	Practitioners' needs and requirements *(based on PG meeting)*	**Standards recommendations**	**Legislative recommendations**	**Joint Procurement recommendations**
1.	Crime reports standarisation	A setting of reporting schemes and common agreement on boundary reporting fields and areas would be helpful for the investigation and data collection purposes.	EU recommendations in this field might be helpful	-
2.	Standarisation of exchange of information with private insititutions	Unification of data and information exchange and regulations is necessary for LEA to effectively combat CaaS. This relates mostly to the communication with Internet Service Providers.	EU recommendations in this field might be helpful	-
3.	Standardisation of data formats and gathering methods	– Unification of data sharing methods and formats would be beneficial to improve the ability to share data with both national and international LEAs; – The Cloud (see procurement ideas) could also summarize, calssify and link the cases inputted by LEA.	EU recommendations in this field might be helpful	
4.	Joint platform for the major ISP	-	-	Procurement of a joint platform for all LEA and Internet Service Providers that would allow asking for data and the standardization of the request process.

5.	Harmonisation of law/harmonisation of LEAs procedures as the crimes outreach single jurisdiction	Standardisation of procedures covering all aspects of investigation – from the scene to the courts	EU recommendations in this field might be helpful	-
6.	Standardisation of trainings	Unification and implementation of technical training for LEA are necessary. They will allow officers to have the right skillset and knowledge to use the digital elements in their investigation. Awareness raising.	EU recommendations in this field might be helpful	-
7.	PCP/PPI of technologies that would allow efficient CaaS fighting	-	-	Practitioners underlined that there is a growing need to procure cloud tool to allow common data gathering and classifying the cases. Moreover a tool for real-time decryption is needed.

6. Recommendations for Pre-Commercial Procurement (PCP) / Public Procurement of Innovative solutions (PPI) / Fast Track for Innovation (FTI), regards to Crime-as-a-Service

There is a common agreement that an enhanced technology is needed for more efficient cloud repository tool to allow common data gathering and classifying the cases Thus the outcomes of the Practitioners Meeting can be a basis for further work on a joint PCP/PPI for the LEAs.

7. Additional recommendations and remarks

8. Identified WP4 stakeholders in the area of Crime-as-a-Service

	LEA	Industry	Science Academia	EU/national bodies	Other
1.	Europol, Frontex, CEPOL, Interpol, European LEA	Cybercrime vendors *(identified in i-Lead WP3)*	Academia working on Cybercrime tools *(identified in i-Lead WP3)*	DG Home	EuroISPA (European Association of European Internet Services Providers Associations)

9. Planned additional dissemination actions
-

Contact

Anyone who is interested in more information related with the report above , please contact the Polish Platform for Homeland Security (i-Lead's WP4 leader) sekretariat@ppbw.pl or project@i-lead.eu