Institution: Bournemouth University		
Unit of Assessment: 11		
Title of case study: Defeating the pirates: creating a technical guide to support EU law enforcement agencies in combatting audiovisual piracy		
Period when the underpinning research was undertaken: 2015 – 2020		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): Professor Vasilis Katos	**Role(s) (e.g. job title):** Professor in Computing and Informatics	**Period(s) employed by submitting HEI:** 2015 – current
Period when the claimed impact occurred: 2017 – 31 December 2020		
Is this case study continued from a case study submitted in 2014? No		

1. Summary of the impact (indicative maximum 100 words)

Audiovisual (AV) piracy generated more than EUR940,000,000 in unlawful revenue in Europe alone in 2018. Bournemouth University (BU) research mapped the illegal online video ecosystem for the first time and produced open source software tools and a digital forensic investigations guide, subsequently distributed to all EU law enforcement agencies (LEA). This led to:

- A reduction of current, and mitigation of future, losses attributable to AV piracy and related cybercrime, evident in the dismantling of two international criminal networks since research was first provided to EU LEA in May 2019.
- The improvement of litigation processes for securing intellectual property rights.
- The development of new analytical and technical skills deployed by LEAs and commercial actors, enhancing operational collaboration, cooperation and efficiency, following training of more than 300 prosecutors, LEA officers and rights holders in the use of the guide and tools since May 2019.

2. Underpinning research (indicative maximum 500 words)

Cyber attribution involves processes in the tracking and identification of perpetrators using computer networks for hacking or conducting other crimes. Lately, the cybersecurity community has made a significant effort to develop the science of cyber attribution, resulting in a more focused approach to delivering it in a specific domain, i.e. illegal Internet Protocol TV (IPTV - television content formatted for internet delivery) streaming.

The two subjects informing cyber attribution are malware forensics and open-source intelligence (OSINT). Together with digital forensics, these three areas of research – undertaken by Katos and academic collaborators [R1-5] - provided the basis for a technical guide [R6] to combat illegal IPTV streaming, commissioned by the European Union Intellectual Property Office (EUIPO).

Malware forensics

Katos's research, in collaboration with the University of Piraeus, into malware-facilitated ecosystems produced a method to detect encrypted malware commonly used in organised cybercrime (specifically botnets - a network of computers linked together by malware and remotely controlled by a third party) [R1]. Katos developed the methodology and empirical validation relating to the time series analysis of the dataset (HP filter). With colleagues in Greece and Switzerland, he developed a digital forensic tool that informs the end-user of a botnet's infection, exposes the botnet infrastructure, and captures verifiable data that can be used in a court of law [R2].

Digital forensics

When security controls fail, there needs to be a digital investigation process in place in order to collect evidence that will be admissible in a court of law. Continuing with the malware studies mentioned above, Katos and collaborators developed research bridging botnets and forensics [R2].

As systems are not designed with forensics capabilities in mind, the collaboration with the University of the Aegean produced a forensic-readiness framework for cloud services, where there was an extensive study and identification of the processes and patterns that need to be in place in order to conduct efficient investigations in cloud infrastructure [R3]. Katos was responsible for the identification and mapping of the concepts relating to cloud investigations, i.e, how to enable a law enforcement agent to investigate in a cloud environment. This research was instrumental in the development of investigation processes for illegal IPTV investigations as IPTV pirates rely heavily on cloud services and, in particular, Content Delivery Networks (CDNs).

Open-source intelligence

Digital forensic investigations are integrated with, and informed by, open-source intelligence (OSINT), where a wealth of information is readily available online. Katos's collaboration with Aristotle University developed this angle of research by creating an approach to effectively sift through the wealth of (big) data and quickly obtain potentially incriminating evidence [R4]. In particular, Katos developed the main concept of the paper (definition of triaging concept in the threat intelligence domain), methodology and validation approach (excluding the empirical testing).

Together with the University of Piraeus, Katos highlighted an emerging threat in blockchain-based Domain Name Systems, where malicious actors exploit distributed ledgers in order to conduct activities such as domain name fraud, and ensure more effective communication for malware [R5].

The technical guide

Following an extensive analytical process [R1-5], Katos led the research team to combine its findings into a 217-page technical guide [R6]. The guide identifies the actors, functions and layers of the 'unauthorised IPTV ecosystem' and outlines a series of technical remedies to expose and block illegal activity, as well as describing the scale and impact of AV piracy and its links to organised crime. After a three-month review by industry experts (e.g. BT, Sky), law enforcement agencies such as Europol, and the European Agency for Criminal Justice Cooperation (Eurojust), the final version was circulated to all EU law enforcement organisations, who now use it in IPTV investigations. It is also included as training material on the European Union Agency for Law Enforcement Training's restricted-access e-learning platform.

3. References to the research (indicative maximum of six references)

R1-5 were all subject to rigorous peer review. R6 was subject to an extensive three-month review (see section 2);

R1: Patsakis, C., Casino, F. and Katos, V. (2020), "Encrypted and Covert DNS Queries for Botnets: Challenges and Countermeasures," *Computers and Security*.88, https://doi.org/10.1016/j.cose.2019.101614

R2: Hatzivasilis, G., Soultatos, O., Chatziadam, P., Fysarakis, K., Askoxylakis, I., Alexandris, G., Katos, V. and Spanoudakis, G. (2019), "WARDOG: Awareness detection watchdog for Botnet

infection on the host device," *IEEE Transactions on Sustainable Computing*, 10.1109/TSUSC.2019.2914917. (Katos's contribution: Sections 7 (100%) and 9 (50%), research on the forensic investigation and cross-border investigation processes.)

R3: Simou, S., Kalloniatis, C., Gritzalis, S. and Katos, V. (2019), "A framework for designing cloud forensic-enabled services (CFeS)," *Requirements Engineering*, 24 (3), pp. 403-430. https://doi.org/10.1007/s00766-018-0289-y

R4: Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D. and Pangalos, G. (2019), "Improving forensic triage efficiency through Cyber Threat Intelligence," *Future Internet*, 11 (7). https://doi.org/10.3390/fi11070162.

R5: Patsakis, C., Casino, F., Lykousas, N. and Katos, V. (2020), "Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS," in *IEEE Access*, vol. 8, pp. 118559-118571.https://doi.org/10.1109/ACCESS.2020.3004727.

R6: EUIPO (2019), *Illegal IPTV in the European Union – Investigating illegal IPTV services: collection of practices*, November 2019 [Confidential; available on request].

4. Details of the impact (indicative maximum 750 words)

Impact on commerce and the economy: Reducing current, and mitigating future, losses attributable to AV piracy and related cybercrime

The technical guide [R6] produced 'the first pan-EU estimate of losses attributable to audiovisual piracy' (almost EUR1,000,000,000 in 2018) [E1], and an estimate of subscribers to illegal services in Europe (13,700,000 people) [E2]. Eurojust presented the research to the European Intellectual Property Prosecutors Network in May 2019 and distributed it to the Public Prosecution Services of all 28 EU Member States [E3]. The EUIPO distributed the research to all EU law enforcement agencies [E4].

R1 was used by Eurojust and Europol to support recent multinational operations, which resulted in: 'a joint action [by six EU member states in September 2019] to dismantle an international criminal network responsible for IPTV crime with estimated damages of EUR6,500,000' [E3]; and the closure in June 2020 of an illegal international service with more than 2,000,000 subscribers and totalling profits for the criminal network at an estimated EUR15,000,000 [E5a, E5b, E6].

Eurojust further notes that R1 'is not only a valuable tool in the fight against intellectual property crime but can also be used as a guide for the investigation of broader online cybercrime, as this requires a similar approach' [E3]. This is corroborated by the Danish State Prosecutor for Serious Economic and International Crime, who states 'the [guide] is providing a point of reference for AV piracy and similar IP crimes. This is particularly important for a prosecutor and for a successful prosecution.' [E6]

Impact on creativity, culture and society: Improving legal frameworks for securing intellectual property rights

The prior lack of rigorous, detailed research and evidence has discouraged policymakers and law enforcement agencies from tackling online video piracy [E1]. R6 outlined how to identify pirate services, provided investigative tools, and mapped, for the first time, the illegal online video streaming ecosystem. The BU research 'demystified a crime which has, in the past, sometimes been put in the "too difficult" box' [E1] and 'enhanced understanding of the illegal industry and created confidence amongst…law enforcement that they have the knowledge and skills to tackle this crime' [E1].

The secretary-general of the Italian branch of the International Federation of the Phonographic Industry (and CEO of a content and brand protection company) confirmed that ‘[R6] represents a true milestone in the disclosure of all the technical, economical and legal aspects of a truly complicated form of piracy…[It] has served to train hundreds of law enforcement agents committed daily in sophisticated investigations.’ [E7]

EUIPO reports that law enforcement officers’ and prosecutors’ feedback has been ‘very positive and indicates that the guide is used in IPTV investigations’ [E4]. Feedback from a training workshop with prosecutors and law enforcement officials in November 2019 revealed:

- 100% participants (n=25) agreed/strongly agreed that the guide will make IPTV infringement investigations more efficient [E8];
- 100% agreed/strongly agreed that the guide helped them develop better understanding of the IPTV piracy ecosystem [E8];
- 95% agreed/strongly agreed that the guide will improve collaboration among agencies [E8].

Impact on public policy, law and services: Changing current processes and equipping prosecutors, law enforcement agency staff and commercial providers with new analytical and technical skills and strengthening operational cooperation

The Danish State Prosecutor for Serious Economic and International Crime testifies that the research on mapping the AV piracy ecosystem [R1] ‘is crucial in understanding the different parties involved, from sellers of infringing services, to money mules, and from content providers to the so-called content aggregators. [BU’s] research has provided a systematic way of describing these parties, for understanding how these interact, and how the evidence can be gathered and correlated through path-to-court processes.’ [E6]

More than 300 European judges, prosecutors and law enforcement officials have been trained in how to use the findings of R1 and the open source software tools at five events since May 2019 [E4]. In feedback collected at an event jointly organised by Eurojust, Europol, and Audiovisual Anti-piracy Alliance in November 2019, 100% of participants agreed/strongly agreed that R1 helped them develop a better understanding of the IPTV piracy ecosystem, and 28% specifically identified the tools and the ecosystem map as being of potential use in their work [E8].

Italian digital forensics investigations company Re@lity Net identifies two benefits of applying concepts learned from the research in two recent cases: ‘First, the investigation efficiency was increased, as the time needed to perform the analysis was substantially improved. This is of high importance to any company with finite investigation resources. Second, the structured way the AV piracy ecosystem was described has helped in communicating with other parties (law enforcement, and members of the judiciary process).’ [E9]

The UK Intellectual Property Office states that ‘research conducted by BU has been critically important in providing a credible and collective analysis of how the environment of online streaming is both used and abused’ and has already identified the potential for transferring the research to other areas of IP crime. In addition, it highlighted the improved capacity building and coordination with ‘private sector, police, trading standards, customs’, not only within the UK and EU, but across the world, and ‘especially in South East Asia, where there has been significant recognition of the threats…’ [E10].

5. Sources to corroborate the impact (indicative maximum of 10 references)

E1: Audiovisual Anti-piracy Alliance. (2020). Letter to Vasilis Katos, 14 June.

E2: European Union Intellectual Property Office, 2019. *Illegal IPTV in the European Union*. [online] EUIPO, p.6. Available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_ in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf [Accessed 11 February 2021].

E3: European Union Agency for Criminal Justice Cooperation. (2020). Letter to Vasilis Katos, 18 June.

E4: EU Observatory on Infringements of IP Rights, European Union Intellectual Property Office. (2020) Letter to Vasilis Katos, 12 June.

E5:
E5a. Europol. 2020. *Illegal streaming service with over 2 million subscribers worldwide switched off*. [online] Available at: https://www.europol.europa.eu/newsroom/news/illegal-streaming-service-over-2-million-subscribers-worldwide-switched [Accessed 8 February 2021].
E5b. Europol. (2020). Email to Vasilis Katos, 23 June.

E6: Danish State Prosecutor for Serious Economic and International Crime. (2020). Letter to Vasilis Katos, 17 July.

E7: Italian branch of the International Federation of the Phonographic Industry. (2020). Letter to Vasilis Katos, 23 October.

E8: Surveys of participants (prosecutors, law enforcement officials) at training workshops, November 2019.

E9: Re@lity Net. (2020). Letter to Vasilis Katos, 10 June.

E10: UK Intellectual Property Office. (2020). Letter to Vasilis Katos, 12 November.