


Speakers

Security BSides Athens 2019




Cybersecurity in the EU: Athens the heart of Cybersecurity in Europe.



by **Marnix Dekker**  @marnixdekker (<https://twitter.com/marnixdekker>), & **C.**

Keynote

Skouloudi  @miss_narbi (https://twitter.com/miss_narbi)

Abstract: Network and information systems and electronic communications networks and services play a vital role in society and have become the backbone of economic growth. Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals. Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. The Cybersecurity Act re-establishes ENISA's role in the changed cybersecurity ecosystem to ensure that it contributes effectively to the Union's response to cybersecurity challenges emanating from the radically transformed cyber threat landscape.

Bio: Marnix Dekker works at ENISA, the EU agency for Cybersecurity, on critical information infrastructure protection, telecoms security, cloud security and EU-wide breach reporting legislation. He leads the security breach reporting team at ENISA and coordinates the Network and Information Security Directive (NISD) activities. Marnix has a Ph.D. degree in Computer security and a master degree in Theoretical physics (Quantum physics). From 2015 to 2017 he was at the IT security directorate European Commission, responsible for developing the corporate IT security strategy, the corporate policy, cascading incidents, linking between senior management and the operational IT security teams. Before joining ENISA he worked as an auditor at KPMG in The Hague, as an IT architect and protocol designer for the Dutch government's e-ID system, as a software programmer in Pisa, and as a university teacher and a sailor in the North Sea offshore.

Bio: Ms Christina Skouloudi works at ENISA, the EU agency for Cybersecurity. Christina

has a background on computer science and holds a master's degree on Digital Systems Security. At the early stage of her career, she worked for several years as a Full stack developer and moved to the Information Security area working as a Network and Information Officer at ENISA. Combining the two things she is passionate about, namely Software development and Information security, she likes to offer smart and innovative solutions through her work. A maker and breaker, who loves to contribute to both development and security community. Her main research interests focus on Internet of Things, Wireless Sensor Networks, Cloud Security, Incident Reporting and technical development of Cyber Security Exercises. She has published various papers on these topics and has also presented pieces of her work and developments in conferences like BSides.



Guest
Talk

The challenge of the third millennium: the resilience of computer systems. Definition of specialized didactic paths tested in three eastern countries. The results of the Erasmus + LMPI project

by **Elpidio Romano** , @ElpidioRomano (<https://www.twitter.com/ElpidioRomano>)

Abstract: The objective of the LMPI project is the development of e-learning and master degrees for the protection of IT systems and networks in three partner countries: Vietnam, Moldova and Kazakhstan. In order to fill up the technical and engineering skills gaps, the project partners directed by Uninettuno University (ITA) and Gip Fipag (FRA) are developing a lifelong learning program in this area for employers. The curriculum developed meet the needs of private companies that are looking for specialists to protect themselves from cybercrime.

Bio: Elpidio Romano is currently an Assistant Professor in Management Engineering in the UNINETTUNO University. His research activities are in the field of Industrial Mechanical Plants, Production Planning and Control, maintenance strategies, and supply chain management and design, using and implementing simulation models to support the Decision Making in a complex Systems. Other Research interests are in traffic and transportation simulation and analysis, air traffic management, risk assessment in air traffic, in which numerous research and papers were carried out in a past years.



Talk
#1

Cycl0ps+ aka Manually infused automation

by **Argyris Makrygeorgou**

Abstract: Two-parted presentation covering what is Commodity & how to treat it, along with the - not so - new trends in Security Operations. Also, after having interviewed more than 100 people from 2015 onwards, going to give some advice for the vanilla

people luring to go full-Cyber. The Ops character (and) of Cyber has become far more than a buzzword, thus while human intelligence & intervention are key to make it happen, one ought to scale and thrive using automation.

Bio: ICT/IS Professional with more than 12 years of experience in Systems and Networks Administration, Operations, Architecture and Information Security. He is juggling strictly Cyber since 2013, undertaking senior roles in Dublin, Ireland & Athens, Greece and contemplating projects around the globe. Favorite work moto would be "Let's keep things Simple & Secure". He joined Algosystems on Q4 2018, as the Head of Managed Cyber Security Services, leading the new Security Operations Center, orchestrating in parallel the Security Integration part. He holds a BSc in Computer Science & an MSc in Information Security both from Athens University of Economics & Business, along with numerous-industry leading certifications such as CISSP, CISA, CISM, IPMA and more. He is member of the ISC2 and very often offers Security consulting when needed.



Talk
#2

The Vulnerability Landscape of Greece

by **Dimitrios Patsos**, @AdacomCyber (<https://www.twitter.com/AdacomCyber>)

Abstract: The Vulnerability Landscape of Greece is a technical report which entails the findings of Greek-based organizations as defined through a series of 200 penetration testing engagements during the period of 2016-2018. It includes original findings, statistics and associated analyses in the areas of Infrastructure, web and mobile applications as well as Social Engineering, while it also provides useful insights on these findings.

Bio: Dr. Dimitrios Patsos is the Chief Technology Officer of ADACOM S.A. He has more than 20 years of experience in information security having managed and delivered projects for multinational organizations in more than 28 countries in EMEA. He holds a B.Sc in Computer Science, an M.Sc and a Ph.D. in Information Security and he has received multiple international awards for his research and professional work, including the Literati Network's awards for Excellence for his contribution to topological vulnerability analysis. He participates in the Advisory Board of many software vendors and startups, while he offers professional advice to a number of VCs and research firms, including the 451 Alliance. He is a member of the ISC2, the Electronic Frontier Foundation and many other professional organizations.



Talk
#3

Android malware from Global to Local: How a Different View Can Change Perspectives

by **Jan Sirmer & Nikolaos Chrysaidos**, @virqdroid (<https://www.twitter.com/virqdroid>)

Abstract: Monitoring threat trends on a global scale can be beneficial, showing, for

example prevalent threats, how vulnerable the Android ecosystem is and if it is getting safer. This approach can, however, sometimes be misleading. When comparing global data for 2018, a gradual drop in the overall numbers of detections can be seen. However, does this really prove that the Android ecosystem is becoming safer? When we move from a global perspective to a more local one and dive into the regional distribution of threats, a different picture emerges. We chose three big regions to illustrate our findings: Europe, North America, Russia, and Australia. Worldwide, the data clearly shows a significant drop of less sophisticated malware strains, such as downloaders and rooters. This is either because the threats are no longer effective on new Android versions, or because the market value for these types of strains has decreased. These types of threats used to be the biggest categories of threats. But, they are also the ones that are the easiest to prevent and track down on a system level, which is precisely what Google aims to do. Especially in the aforementioned regions, we have observed a rise in technically advanced and covert malware such as bankers, fake apps and even targeted attacks. Studying local data allows us to better pinpoint threats and their distribution in specific regions. We saw again that threats differ by region. Just looking at threats on a global scale can be misleading and can cause oversight of regionally diverse threats. In our presentation, we will compare data from last year, show how this can help us predict new malware strains, but more importantly, discuss how we can use it to prevent and detect these threats. We will give examples of how we cluster detections, demonstrate how to recognize threats and provide guidelines on how to successfully prevent devices from getting infected in the first place. Last but not the least, we will show that the Android ecosystem remains a dangerous space, on a global scale not only to single victims, but for entire businesses.

Bio: Jan Sirmer is a Malware Analysis Team Lead at Avast. His main specialization is analyzing malicious Java threats, Android applications and exploits, macro viruses, web-based malware and other non-executable malware. During the course of his career, Jan has authored blog posts about phishing threats, malicious web exploits and Android threats. In the past, he has successfully presented his research at various conferences such as AVAR, Botconf, CARO, FIRST, RSA, Virus Bulletin.

Bio: Nikolaos Chrysaídos has over ten years of experience in the cybersecurity and information security sector. Currently, he is Head of Mobile Threat Intelligence and Security at Avast, leading mobile security, threat intelligence, and threat prevention projects. He is passionate about promoting innovation in the cybersecurity field. He has successfully presented his research at various conferences such as AVAR, CARO, RSA, BSides.



Talk
#4

Understanding malspam

by **Martijn Grooten**, @martijn_grooten (https://www.twitter.com/martijn_grooten)

Abstract: Email continues to be the main vector through which malware is delivered and through which people have their credentials stolen. This often happens in opportunistic (i.e. non targeted) campaigns, which distinguishes them from very targeted spear-phishing campaigns. Yet these 'malspam' campaigns also differ in a


number of fundamental ways from ordinary spam, which positively affects their effectiveness and negatively affects our ability to analyse them. In this talk, I will explain how most malspam campaigns differ from ordinary spam, how this makes them a lot better at bypassing email filters and how this affects their visibility. I will also discuss more general trends when it comes to malspam. From this talk, the audience will hopefully get a better understanding of modern email-based threats and get some advice on

Bio: Martijn Grooten has worked more than a dozen years in IT security. He has a broad interest in security with a lot of experience working in email security and a weak spot for cryptography, He is an active blogger, tweeter and public speaker. He is currently the Editor of Virus Bulletin and lives in Athens.



Talk
#5

Powershell Best Security Practices and how to bypass them

by **Isidoros Monogioudis** ,  @isidor_mon (https://www.twitter.com/isidor_mon)

Abstract: As we know Powershell is widely used for offensive operations and is clearly defined as one of the most popular techniques according to MITRE ATTACK framework. Best security practises have been already addressed quite a few times and Microsoft as well as other most security vendors detect and prevent efficiently almost every powershell suspicious activity. However attackers have found other ways and techniques to bypass those security controls and evade traditional and modern detection measures. What are those techniques/tools being used in the wild? What else defenders need to do keep the protection level high? The presentation will cover all updated powershell security practices, tools and techniques to evade powershell based detection methods and the associated countermeasures for blue teams.

Bio: Isidoros Monogioudis is a Senior Cyber Security Analyst with more than 20 years' experience in the cyber security and defense domains. As a Senior Cyber Defense Officer in the Greek Ministry of Defense, Isidoros was involved in several cyber security operations and defense exercises at both national and international levels (Panoptis, NATO Cyber Coalition, Locked Shields, Cyber Europe). Following his retirement, he joined Digital Shadows where he works on adversary tools, tactics and techniques (TTP) research, threat intelligence operations and internal security activities, including local Purple Team exercises.



Talk
#6

Wormhole: How to sneak malware past SOC teams

by **Vasilios Hioureas** ,  @maniatisVH (<https://www.twitter.com/maniatisVH>)

Abstract: There is a new method of remote code execution which we have been seeing lately in the wild using dynamic compiled remote source code. The technical details

behind this attack are very interesting and the implications are potentially dangerous if they evolve, so I decided to stay one step ahead and use these concepts to actually do some real damage. I succeeded in creating a POC to infiltrate a number of corporations using this method. Because the binary does not initially contain malicious code, the benign application will pass whitelisting. Only then will the worm hole open, remote malicious source code is streamed into the executable and without spawning a new process or altering the binary itself will be executed. We tested this method and succeeded in bypassing full enforcement white-listing in environments ranging from a small IT company to the corporate headquarters of a large bank. This is the story of how "The Wormhole" was born. Technical details and a live POC will be performed.

Bio: Vasilios Hioureas is a programmer and malware analyst specializing in reverse engineering. Over the course of his career he has worked on everything from game programming to internal cyber security at the headquarters of a bank in the US. He currently is living in Greece, working for MalwareBytes as an analyst on the intelligence team. Specifically working on APT analysis and writing articles on research. He previously worked for Kaspersky labs as a reverse engineer where he specialized in smart city hacking and firmware reverse engineering.



Talk
#7

Beyond Windows Forensics with Built-in Microsoft Tooling

by **Thomas V Fischer** ,  @FVT (<https://www.twitter.com/FVT>)

Abstract: Microsoft has slowly been introducing tools to help organisations better manage and troubleshoot Windows performance and issues; these are now entirely integrated into Windows. To improve performance and troubleshooting capabilities, Microsoft introduced System Resource Usage Monitor (SRUM) in Windows 8 and beyond. PowerShell has become the default "command line" management tool for windows administrators. These tools provide both a wealth of information into what has happened and is present on the system. For Forensics and even Incident Response, these tools are now a go to built-in option to bootstrap and drive the forensics process including opening access to artefacts that overzealous user or even a "smart" attacker has removed. SRUM for instance can provide data points ranging from network to process activity providing insight into what, who, when and how an attacker or malicious process introduced itself into the environment. This talk will help the participant build the foundations to identify which built in tools can assist in the Windows Forensics process and the data points that are available as well as examine how services such as SRUM can be used to extract key data points to provide information for incident response or threat hunting activities.

Bio: Thomas has over 30 years of experience in the IT industry ranging from software development to infrastructure & network operations and architecture to settle in information security. He has an extensive security background covering roles from incident responder to security architect at fortune 500 companies, vendors and consulting organisations. He is currently security advocate and threat researcher focused on advising companies on understanding their data protection activities against malicious parties not just for external threats but also compliance instigated. Thomas is

also an active participant in the InfoSec community not only as a member but also as director of Security BSides London, ISSA UK chapter board member and speaker at events like SANS DFIR EMEA, DeepSec, Shmoocon, and various BSides events.



Talk
#8

Data Breaches: Barbarians in the Throne Room

by **Dave Lewis**, @gattaca (<https://www.twitter.com/gattaca>)

Abstract: Often defenders worry about the intangible security problems. Defenders need to concentrate their efforts defending the enterprise by focusing on the fundamentals. Too often issues such as patching or system configuration failures lead to system compromise. These along with issues such as SQL injection are preventable problems. Defenders can best protect their digital assets by first understanding the sheer magnitude that a data breach can have on an enterprise. In this talk I review my findings after analyzing hundreds of data breach disclosures as it pertains to what went wrong.

Bio: Dave Lewis has twenty five years of industry experience. He has extensive experience in IT security operations and management including a decade dealing with critical infrastructure. Lewis is a Global Advisory CISO for Duo Security (now Cisco). He is the founder of the security site Liquidmatrix Security Digest and cohost of the Liquidmatrix podcast. Lewis serves on the advisory boards for several firms. Lewis writes columns for Forbes, Daily Swig and several other publications.



Talk
#09

Looking through Muddy Waters: Insight into TTPs of a Middle Eastern threat actor

by **Jaromir Horejsi**, @JaromirHorejsi (<https://www.twitter.com/JaromirHorejsi>)

Abstract: MuddyWater is a threat actor likely based in Middle East, with known activities since at least the middle of 2017. It targets various individuals, government organizations and industries in many countries all across the Middle East and Central Asia, with the highest intensity of targets in Turkey, Pakistan, Afghanistan and Jordan. Starting with spear phishing emails and macro-powered attachments sent to carefully selected high profile targets, the threat actor attempts to deliver and install various backdoors written in different programming languages to the victims' computers – all with the purpose of performing cyber espionage. One of these backdoors has interesting capabilities, such as disk wiping, anti-analysis and numerous false flags. To increase stealthiness, C&C communication is forwarded via PHP proxies hosted on hacked websites, creating an asynchronous communication channel. We took advantage of this configuration to monitor the activity of this actor, discovering the identities of some of the victims as well as some commands which attackers attempted to execute on victims' machines. In this presentation, we will show the most recent

evolution of the tools, tactics and procedures of this threat actor. We will present some examples of targeted documents and the multiple layers of obfuscation added to their payloads. We will also detail the different tools this threat actor uses, and we will propose some ideas on how to prevent and hunt for these threats.

Bio: Jaromir Horejsi is a threat researcher at Trend Micro. He specializes in hunting and reverse-engineering threats that target Windows and Linux. He has researched many types of threats over the course of his career, covering threats such as APTs, DDoS botnets, banking Trojans, click fraud and ransomware. He has successfully presented his research at RSAC, Virus Bulletin, FIRST, AVAR, Botconf and CARO.



Talk
#10

Leveraging osquery for effective Incident Response as well as stealthy enumeration

by **Dimitrios Bougioukas**

Abstract: This talk is oriented towards both Blue team and Red team members (a.k.a Purple Team talk). osquery is an open source solution that can extend a Blue team's endpoint visibility, in an efficient and centralized manner. It does so by exposing operating system configuration data in the form of relational database tables. All Blue team members have to do is submit or schedule queries against these tables to collect valuable data about the current state of an endpoint/server as well as changes performed on it over time. The great thing about Osquery (especially when deployed on a Windows environment) is that it provides detailed insight into the registry, WMI, hardware events and many other areas that were previously disregarded by other endpoint monitoring agents or could not be interrogated through a single endpoint monitoring solution. During this talk, Blue team members will learn how to detect modern attacks leveraging osquery's capabilities. Specifically, fileless malware, ransomware, malicious browser extensions and a variety of post-exploitation actions will be detected during a live demonstration, through osquery. Some of osquery's insufficiently secure libraries and common deployment shortcomings can be leveraged by attackers to perform stealthy enumeration. During this talk, Red team members will learn how to perform osquery injections and leverage deployment misconfigurations in order to perform stealthy enumeration or even detailed reconnaissance. In addition, tips on how to evade osquery by tampering with a system's kernel will also be presented to the audience.

Bio: Dimitrios Bougioukas is the Director of IT security training services and IT security research lead of eLearnSecurity. He also authors advanced IT security courses (Red & Blue), taken by individuals, Fortune 100 companies and government/military agencies alike. In the past, he has worked as an information security engineer and analyst for a major financial institution, as a Senior instructor for eLearnsecurity and as a penetration tester within EY's practice. Dimitrios specializes in advanced cyber threat simulation, threat intelligence and purple team tactics. He has been engaged on numerous penetration testing activities and he has presented at information security conferences, such as BSides. Dimitrios has also received acknowledgements from security, telecom

and other major companies for reporting vulnerabilities in their applications (IBM Trusteer, LG etc.). In the context of his professional career, his work led to international and regional information security awards in highly competitive contests such as Retail Banker International Awards.



Smart locks: dumb security, dumber API



by **David Lodge**, @tautology0 (<https://www.twitter.com/tautology0>) & **Vangelis Stykas**, @evstykas (<https://www.twitter.com/evstykas>)

Talk
#11

Abstract: The rise of cheap, low powered communication technology has been most prominent in the fields of locks, where the traditional model of a key, rfid reader or magnetic stripe does not work for many use cases. This talk will be demonstrating how many smart locks fail to fully think out security and in many ways make the smart locks weaker than its low-tech equivalent. Some of these methods will be destructive, as much as can be done in an unventilated room at least. We will be going through several smart locks, all designed for convenience and showing where the security flaws are and the different vectors to attack. Some locks will be focused on, specifically the Nokelock series of products, the slok lock and ultraloq. Including demonstration of how the protocols were reversed and how they can be used to unlock a padlock from a python script or Android device. Just for BSides Athens, we will be focusing on the API that supports most of these devices and their weaknesses, which often make it possible to not only compromise a lock, but prevent the lock's owner from using their own lock.

Bio: David Lodge has been doing this sort of stuff for too long. Pen tester by day, pretender at hardware by night; likes taking stuff apart, but is unable to get it back together afterwards.

Bio: Vangelis Stykas is a backend engineer turned into a pentester. Playing around with bits and bytes for the past 30 years, he has hacked ships, cars and locks. He has a weak spot for breaking APIs and web stuff but hates building them.



The Role of Mobile Malware in Stalking Cases

by **Jessica Amery**, @jessicaamery_ (https://www.twitter.com/jessicaamery_)

Talk
#12

Abstract: This talk will cover basic techniques involved in reverse engineering Android .apk files alongside common obfuscation techniques used by developers. I will showcase my findings from investigating 'Stalkerware', a branch of mobile malware that allows users to spy on spouses, children and co-workers. Stalkerwear allows paranoid users to spy on those closest to them and this talk will cover three main area regarding 'Stalkerwear'; the legality of such software, the technical capability of the software and how it operates and finally how we can prevent the spreading of these malicious applications.

Bio: My name is Jessica Amery and I am a current third year Ethical Hacking student at Abertay University, Dundee, Scotland. Researching all things Android Security related and passionate regarding online privacy and how we can educate users to protect their data.



Talk
#13

Past, Present and Future of DDoS

by **Vaggelis Daravigkas**,  @edaravig (<https://www.twitter.com/edaravig>)

Abstract: DDoS has always been one of the greatest threats in the Internet landscape, especially towards high-profile organizations and governments. The goal is simple; Profit and financial gain -or damage. But how actually DDoS are currently being executed? Conversely, how are they mitigated? Is it always possible to mitigate an attack? (Hint: NO!) How have the techniques changed throughout the years? Most importantly, in the era of millions of connected devices to the Internet, which every one of the them is a potential bot to the next DDoS, does everyone know what DDoS is and how it works? On 2018, the largest volumetric attack targeting GitHub was recorded. Misconfigured memcached servers were utilized and fortunately for GitHub, the attack was not a zero-day at that point; meaning that it was timely mitigated. However, not all DDoS attacks are the same. Different layers, different attacks. From SYN Flood to DNS amplification, from HTTP GET Flood to CLDAP Reflection, to name a few. Nowadays, more and more DDoS attacks take place. One of the reasons is due to the fact that there are countless zombie devices lying around, but are still connected to the web and thus, composing botnets. In addition, zero-day attacks are inevitable, when it comes to software vulnerabilities. And if this is not enough, the attacker might always be able to take control (C&C) of a device with social engineering tricks, "exploiting" the unaware user(s). DDoS are here to stay. Since the mitigation techniques are evolving, the same applies for the type and techniques used for DDoS. Briefly stated, the sophisticated techniques focus now on the content; the payload (what does the packet contain), rather than the context (i.e the packet or the request on its own). Furthermore, DDoS-as-a-Service makes the future look grimmer rather than brighter. However, both engineers and end users need to understand that in the end it's up to us. It's up to our susceptibility for security and our willingness to take the necessary measures and stay safe and aware. This place -the Internet- will never be safe, but we can always do our best.

Bio: My name is Vaggelis (Evangelos) Daravigkas and I am working as a SOCC (Security Operations and Command Centre) Specialist for Akamai in Krakow, Poland. In addition, I am an OMS (Online Masters Degree) Cybersecurity student at GeorgiaTech. Furthermore, currently I am preparing for the CCNA certification, as I believe that a basic and strong background in networks is essential for anyone involved in the field. In my spare time, I go running, catch up with friends or watch series; yes, Mr.Robot is my favorite one. Finally, when time allows, I try to volunteer, regardless of the occasion or the event.



Social Engineer's Mindset and Toolset

WorkShop

by **Sharka**,  @__Sh4rk__ (https://www.twitter.com/__Sh4rk__)



Abstract: Do you want to be a social engineer or you are already one and want to learn a framework to use? We would start from beginning, what are our basic checks we should make, what tools and tricks we can use to gather as much OSINT as we can using different tools and how to combine them to get best possible results. We will build a social engineering mind map that brings the best results while hunting for available information for your target. I will take you through the whole process, including the initial OSINT gathering, to working with your target physically on site and also process on what to do once you manipulate your target into wither divulging information or letting you get inside the target building or office. Within the mind maps we will cover couple scenarios. For example one where we will use out of the box to bring out the best results for our engagements. We will be working through scenarios where as result from our initial basic checks, we will be impersonating the target company employees that exist, build new characters, impersonate employees of delivery companies, lost tourist or other 'opportunistic' scenarios. We will also look at some bad examples of pretext we should try to avoid on social engineering and physical security engagements. We will look at OSINT search for each scenario and for each one of them using different browsers, Google earth, different social media platforms and tools. We will see what we can use with direct interaction with the target and what to do once everything works and we find ourselves in middle of our target office and we get first strange look. You will walk away with a new social engineer mindset that you can build upon further when building your own social engineering framework and skills.

Bio: Sharka is known by some as social engineering pirate queen with her pirate social engineering alter ego. She is researching different techniques for social engineering toolset especially for direct interaction with her targets as well as radiofrequency technologies. She has experience working on both sides of security spectrum, defensive and offensive. In her free time, she loves to get involved in community projects, she is co-organising local chapter of OWASP in Manchester, she is an ambassador of BSides Athens/Greece as well as BSides BSides Cairo/Egypt and she co-founded a local DEF CON group in Paris , DC11331. She also co-founded Infosec Hoppers a group that is offering buddy system to go to conferences and building a pool of professionals to help each other.



Tell me where you are? - a case study of GPS trackers security

WorkShop

by **Martin Hron**,  @thinkcz (<https://www.twitter.com/thinkcz>) & **Nikolaos Chrysaidos**,  @virqdroid (<https://www.twitter.com/virqdroid>)

Abstract: Every day we hear about weak security of IoT devices, about vendors that don't take security seriously and how using and not changing default passwords could

lead to a leak of important and personal data. We will present such a case. GPS trackers made with a default password and predictable serial number allowing full control of the tracker and leaking user's position. Moreover, due to heavy white labelling and use of the same cloud infrastructure the scale of the problem is huge. In our presentation, we will discuss affected models, their weaknesses and the standard onboarding process of the GPS tracker. Later we will focus on the vulnerabilities of the web portal and control panel. A detailed report will be given about the Android applications that exist on Google PlayStore for those devices. Finally, we will provide statistics and data about all affected models. Last part of our talk will show you possible attack vectors and ways how to leverage them for exploitation of devices.

Bio: Martin Hron is a Security Researcher at Avast. Martin leads research across various disciplines such as dynamic binary translation, hardware-assisted virtualization and malware analysis, lately focuses on firmware and IoT security. Martin is devoted to technology and is a true software and hardware reverse engineer, game programmer, tinkerer, AI and IoT mantras practitioner. Prior to Avast, Martin held the position of artificial intelligence and game programmer, working on the MAFIA II (AAA game title) project, and as a Windows kernel software engineer with encryption file system drivers. Martin brings more than 20 years of experience in the IT industry and deep knowledge of hardware and operating system architectures to Avast, where he leads research, mainly in the domain of dynamic malware analysis, and general security. Martin is always on the hunt and keeping an eye on new emerging technologies.

Bio: Nikolaos Chrysaïdos has over ten years of experience in the cybersecurity and information security sector. Currently, he is Head of Mobile Threat Intelligence and Security at Avast, leading mobile security, threat intelligence, and threat prevention projects. He is passionate about promoting innovation in the cybersecurity field. He has successfully presented his research at various conferences such as AVAR, CARO, RSA, BSides.



Of Ships and Speedboats – What is and isn't working?

WorkShop

by **Tom Owen**,  @TomSionCati (<https://www.twitter.com/TomSionCati>)

Abstract: Whether it's through differing threats, leadership priorities, operational scale or resource availability, all organisations are unique. A speedboat has different risks, constraints and opportunities when compared an oil tanker or a warship, and visa-versa. Nothing freshens up thinking like a focussed, echo-chamber free round-table (strictly Chatham House rules) where we can identify and discuss our problems amongst a safe, private group of peers. It might even be just the thing to throw a different light on a chronic problem, revitalise someone for a specific task or identify a new angle on a difficult issue. Interested in what makes Energy difficult vs E-Commerce? What problem are you banging your head against? What issue makes you sad every day? Come along, participate in this round-table discussion and let's talk in through. Format:

- Facilitated discussion with 10-15 attendees around a table. 2x 1 hour sessions with a break in-between. Room to extend a little if everyone is still hugely engaged.
- All facilitator notes recorded onscreen and shared in a much anonymised, mutually editable

format before the workshop ends.

Ground rules:

- Strictly Chatham House
- Vendors can be praised and criticised, but state vested interests first
- No directly plugging your own company's services
- Keep things collegiate and friendly
- Bring no egos, acknowledge no rock stars. All opinions have merit
- Understanding the problem is (harder and) more important than finding the solution
- You don't have to declare your employer or personal details

Agenda:

- Quick facilitator, attendee and workshop introductions
- Answer in turn – three important questions:
 - My role and scale
 - My resources
 - My top three problems
- Identify 4-6 common and/or interesting areas for discussion after the break
- Break, break, break
- Work through the agreed areas
- Agree notes / redact as requested
- Ensure everyone had a copy, and close

Requirements:

- Table and chairs for 10-15
- Projector and screen
- Backup flip chart and markers
- Table for drinks and snacks
- Enough privacy to encourage discussion

Bio: Tom is Head of Security & Business Services at Memset Ltd, a security-focussed Cloud hosting provider in the UK. Previously he did security at Accenture and spent some time as a Security Analyst with Rackspace. He is definitely not an industry rock-star and had not completed his 10,000 hours, but he spends a lot of time thinking about important and scary things. He is also an ex-medic and Emergency Planning Officer for one of the busiest land Search and Rescue organisations in the UK and an ex-responder for the ambulance service.

Network

Educate

Participate

Contact Us



info |@| bsidesath |.| gr



(<https://goo.gl/vqrB5Q>)



(<https://goo.gl/coUx5J>)



(<https://goo.gl/i1dgyI>)



(<https://goo.gl/WWxGQ1>)



(<https://bit.ly/2VdHHvM>)

Find us on Facebook

 **Consiglia**

Condividi

393 persone consigliano questo elemento. [Iscriviti](#) per vedere cosa consigliano i tuoi amici.

Subscribe to our channel



Security BSides Athens



Download our Apps



(<https://goo.gl/gAotoA>)



(<https://goo.gl/KIKodP>)

Copyright © www.bsidesath.gr 2016 - 2019