Journal of Cyber Forensics and Advanced Threat Investigations

Volume 2(1), 1-2. https://doi.org/10.46386/ijcfati.v2i1.28

Editorial: Volume 2, No 1 (2021) of the *IJ*CFATI

John William Walker[1]

Abstract

This article introduces volume 2, no 1 (2021) for the *International Journal of Cyber Forensics and Advanced Threat Investigations*. The article outlines some insights, updates and summarizes the articles published in the issue.

Keywords

cybersecurity, digital forensics, incident response, threat investigations.

Submitted: 19/05/2021— **Accepted: 22**/05/2021 — **Published: 23**/05/2021

Corresponding author [1] Address: School of Science & Technology,Nottingham Trent University, 50 Shakespeare St, Nottingham NG1 4FQ

Editorial

Following our successful launch of the First Edition of the ***'International Journal of Cyber Forensics and Advanced Threat Investigations'*** or *IJ*CFATI for short in 2020, the team have been working on this current release. As we forge forward with the journal, we do so in the knowledge that the age of Cyber (Digital) security has never faced such challenges, with what seems to be an unrelenting onslaught of successful Ransomware attacks taking place on a known, weekly basis – and of course multiples of other daily unreported attacks adversely impacting global targets. With these high levels of Ransomware attacks in mind, I conducted a small OSINT research project, focusing on a high-profile international $3 trillion government-backed funding scheme of which concerns were expressed relating to the deployed security posture. However, what was quickly and easily discoverable through tracing their Bitcoin Wallet transactions was, this institution had already suffered the consequences of successful Ransomware attacks, followed by several discreet transactions into dubious Bitcoin Wallets marked as suspicious – what one may label as, investing in the future stocks of crime!

In an age of what seems to be suffering from a Digital Crime Pandemic, within the last two quarters of 2020, and moving into O/1 2021, the interconnected world encountered the logical impact of the compromise of security solutions, which were interwoven into the Infrastructures of Global companies, leading to an astronomical digital compromise on a scale never seen before – I ,of course, refer to the SolarWinds hist out of the hands of Russian actors. The real focus however should not be on the historical fact that this breach occurred but should be considering the potential implications of all other remote Third-Party services we are plugged into. Say to provide remote support for a security application, provide cloud space and add-ons such as IaaS (Infrastructure as a Service), or to connect in and manage the buildings services, such as lighting, heating, CCTV, and other such mundane features – mundane that is, until such time they are unavailable or compromised. On this note, to serve as an example from my world of engagements, akin to the fictional work by Michael Dobbs, The Edge of Madness which conjurors up a future world of how Digital Crimes could impact the world.

About 8 years ago I was on a security assignment in Scotland, where I had raised an observation about the local authorities use of, what appeared to be insecure cloud services. To my surprise, the client denied any knowledge of the cloud, and in fact, was completely adamant that the authority did not use any cloud services. That was, until an unauthorised actor from a local school hacked into a Residential Care Home in the depths of one of the coldest Scottish winters on record, remotely turned off the heating, and turned on the air conditioning, an act, when taking into the account the age of the residents was potentially life-threatening – yes, they did have cloud!

The implications of our digital era would seem to indicate that there are 3 types of deployment facing the Internet, and they are:

Those who have been compromised and know it.
Those who are unaware that you have been compromised.
Those that will be compromised.

Based on the inference it would seem to be essential that CTI (Cyber Threat Intelligence), conjoined First Responder Incident Response, and Digital Forensics capabilities are accommodated prior to any such event occurring. It is in this capacity in which

we here at ***International Journal of Cyber Forensics and Advanced Threat Investigations'*** are working to provision the quality subject matter, and expert-based papers to support our readership to meet the digital defensive objectives of the day, with this volume including some excellent papers as introduced below.

In the first article, the authors analyzed the phenomenon of advanced bot scanners by designing and implementing a platform inspired by the traditional honeypots. The authors studied specific web scraping botnets that target airlines' websites. Additionally, the article also contains a method to investigate the claim commonly made that proxy services used by web scraping bots have millions of residential IPs at their disposal. Mathematical models were proposed, which indicate that the amount of IPs is likely 2 to 3 orders of magnitude smaller than the one claimed. This finding suggests that an IP reputation-based blocking strategy could be effective, contrary to what operators of these websites think today.

The second article discusses and presents techniques and methodologies for the investigation of timestamp variations between different Raspberry Pi ext4 filesystems (Raspbian vs. UbuntuMATE), comparing forensic evidence with that of other ext4 filesystems (i.e., Ubuntu), based on interactions within a private cloud, as well as a public cloud. Sixteen observational principles of file operations were documented to assist in our understanding of Raspberry Pi's behavior in cloud environments. This study contributes to IoT forensics for law enforcement in cybercrime investigations.

The third article looks specifically at phishing and what new trends are observed due to COVID-19. The article is grounded in routine activity theory and demonstrates its relevance to both the physical and cyberspace. The implications of this research can be used by scholars who want to continue researching this new phenomenon. Practitioners can utilize the findings of this article to look for ways to improve the corporate security posture by protecting the employees and customers working from home. Developing new phishing training and awareness programs should be focused around possible scenarios involving COVID-19. the study suggests victims are more likely to fall prey to those during times of fear and uncertainty like the current pandemic.

In the fourth article, a Hot Spot Note builds on previous findings in the workshops of the EU project Next GenEration Internet Forward Strategy team. A new area of research and innovation has been introduced that focuses on both regulating device ecologies and the creation of moral and ethical guidelines for a governance model. Based on the team's previous findings, it is now believed to be the end of a paradigm of a government model that has outsourced capabilities to the market. Now, it is the time of privatizing the last public capability: identity management. This will be leading to tremendous stress in systems, services, organizational procedures, and individuals. A holistic perspective was presented to distribute security on two points: at the device level and a moral movement at a societal level. Finally, the article ends by defining a model of SSI and disposable identities.

Other notable events to report in this release are that we have expanded our advisory board to include six highly accomplished professionals to lend their knowledge and experience to underpin the *IJ*CFATI mission, and they are as follows:

- Valentina Palacín: Threat Operations Lead at Marqeta, Inc - (Argentina)
- Andrew Alston: Co-Founder & Managing Director at BreachAware - (UK)
- Nihad Hassan: Consultant - Computer Forensics and Digital Evidence Acquisition - (Turkey)
- Osvaldo Falabella: Electronic engineer at INET Computer Networking Consultants - (Argintina)
- Rob van Kranenburg, Ecosystem Manager for the EU project Next Generation Internet, and Head of the Public Domain Program at Waag Society - (Belgium)
- Víctor Mayoral-Vilches, Founder of Alias Robotics- (Spain)

So, now to move on to the main thrust of our Journal, information. I hope you enjoy and find our latest copy of *IJ*CFATI interesting, and above all useful.

Stay safe out there, it is a dangerous world.

Declaration of Conflicting Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) declared no financial support for the research, authorship, and/or publication of this article.

Acknowledgments

To the DFIR and cybersecurity communities.