Journal of Universal Computer Science, vol. 25, no. 11 (2019), 1394-1395
submitted: 20/10/19, accepted: 20/11/19, appeared: 28/11/19 © J.UCS

Cyberattack Detection and Response

J.UCS Special Issue

Jörg Keller
(FernUniversität in Hagen, Germany
joerg.keller@fernuni-hagen.de)

Wojciech Mazurczyk
(Warsaw University of Technology, Poland
wmazurcz@elka.pw.edu.pl)

Béla Genge
(University of Medicine, Pharmacy, Sciences and Technology of Targu Mures
Romania
bela.genge@umfst.ro)

Lothar Fritsch
(Karlstad University, Sweden
lothar.fritsch@kau.se)

Simon Vrhovec
(University of Maribor, Slovenia
simon.vrhovec@um.si)

Cyberattacks have evolved into a threat for modern society, as they affect both individuals and organizations alike. Attacks can have a multitude of different forms, ranging from denial of service to ransomware, and target government, critical infrastructure, businesses or private environments. As this threat cannot be ignored, it should be detected as early as possible, to prevent damage as much as possible. As attacks often employ multiple stages, that compromise more and more machines and/or remove more and more lines of defense, early detection seems all the more necessary. At the same time, attacks, especially if evolving over many weeks, try to stay undetected and hence employ many measures in order not to raise suspicion, which renders detection a difficult endeavor. When an attack is detected, an appropriate response is necessary, which can be as straightforward and painful as disconnecting the victim from the network, but also can take many other forms, up to offensive countermeasures that try to attack the attacker. Both attacks and countermeasures include technical and social means, as it is sometimes easier to find out e.g. the structure of a company network by interviewing careless employees than by performing a cyber reconnaissance.

This special issue targets actual research on the detection of and response to cyberattacks on all levels (e.g., individuals, organizations, ISPs, and critical infrastructure) that addresses technical, social or both aspects (including, e.g., social engineering and spear phishing detection). The call for papers for this special issue was distributed over relevant mailing lists, call-for-paper distribution websites, personal and university websites, and on the homepage of the journal. In addition to submissions of new articles, extended versions of accepted papers from the Central European Cybersecurity Conference CECC 2018 have been invited for submission under the condition of providing at least 50% new content. All submissions were peer-reviewed by experts in the domain.

Based on the reviews and our own judgment, five articles were selected for publication in this special issue. Steffen Wendzel, Florian Link, Daniela Eller and Wojciech Mazurczyk studied network covert channels that enable stealthy communications for malware and data exfiltration, and introduced the concept of countermeasure variation, i.e., a slight modification of a given countermeasure designed to detect covert channels of a specific hiding pattern (a family of similar hiding techniques) in a way that it can also detect covert channels representing other hiding patterns. Tomáš Bajtoš, Pavol Sokol, Andrej Gajdoš, Katarína Lučivjanská and Terézia Mézešová analyzed data collected by a telnet honeynet to determine specific attributes of telnet botnets' behavior during initial and secondary infection, and designed a model for profiling threat agents into telnet botnets groups. Samo Tomažič and Igor Bernik developed a novel Cyberattack Response Model to be used by Slovenias nuclear safety regulator and the regulator responsible for the physical protection of nuclear facilities, and nuclear and radioactive materials. Anže Mihelič, Matej Jevšček, Simon Vrhovec and Igor Bernik conducted a case study in a large Central European manufacturing company and observed the targeted employees and IT department staffs response to a phishing campaign. Halima Ibrahim Kure and Shareeful Islam proposed a novel cybersecurity risk management approach integrating cyber threat intelligence information with risk management activities, and demonstrated its applicability in collaboration with a power holding company in Nigeria.

We would like to express our gratitude to Christian Gütl (Managing Editor) and Dana Kaiser (Head of Editorial Team) for allowing us to organize this special issue of the Journal of Universal Computer Science. We also like to thank all reviewers who facilitated the review process, namely Igor Bernik, Luca Caviglione, Michal Choras, Tobias Eggendorfer, Petra Grd, Mordechai Guri, Piroska Haller, Georgios Karopoulos, Stefan Katzenbeisser, Jean-Francois Lalande, Olaf Maennel, Brad Malin, Anže Mihelič, Farnaz Mohammadi, Pal-Stefan Murvay, Gerardo Simari, Kai Simon, Daniel Spiekermann, Damian Weber, Edgar Weippl, Steffen Wendzel, and Christos Xenakis. Last but not least, we like to thank all authors for submitting their work to this special issue.