After the Attack: Introduction to the Cybercrime Minitrack

Piotr Siuda
Kazimierz Wielki University
piotr.siuda@ukw.edu.pl

J. Tuomas Harviainen
Tampere University
tuomas.harviainen@tuni.fi

Juho Hamari
Tampere University
juho.hamari@tuni.fi

Robert W. Gehl
York University
rwg@yorku.ca

Abstract

At the HICSS-56 held in 2023, cybercrime was introduced as a multidisciplinary study area. Following a series of informative presentations, the Cybercrime minitrack returns in 2024 for HICSS-57, featuring a wealth of high-caliber research. In response to the call for papers, nine manuscripts from various disciplines were submitted and subjected to peer and editorial review. Three papers were accepted for presentation and publication. All of these have a strong focus on how to respond optimally when organizations and individuals are successfully cyber-attacked. Hence, despite initial submissions on a range of significant topics, the final shape of this year's minitrack emphasizes the role of communication in cybercrime research.

Keywords: cybercrime, ransomware, communication, interdisciplinary, multidisciplinary.

1. Introduction

Organizations and individuals are regularly warned: cybercriminals are out there, right now. They are sending phishing emails in the hopes that some percentage of people click on a malicious link (Hadnagy et al., 2015). They are using network analysis software to probe corporate, government, and consumer devices and networks, seeking out vulnerabilities to exploit. They are exploiting our sense of loneliness through "romance scams," using pictures of beautiful people, sending fawning messages, all with the goal of getting us to send them money (Nurse, 2019). Or, one of them could even be standing right in front of you, smiling, pretending to be a customer or a janitor, but in reality being a social engineer, seeking to gain your confidence in order to convince you to gain access to sensitive documents.

We are warned that cybercriminals come from many different places and backgrounds. Some are mere "script kiddies"—rank amateurs who play with off-the-shelf hacking software (*Meet the Script Kiddies*, 2023). Some are professional organizations, such as the Yahoo Boys of Nigeria, who run massive romance scams (Barragán, 2023). And some are state-sponsored, such as the group dubbed APT43 operating out of North Korea (Gramer & Iyengar, 2023).

And we are also warned: once cybercriminals have access, they might exfiltrate our personal information in order to sell it on dark web "fullz" markets (O'Rourke, 2016). They might install remote access tools (RATs) to enable them persistent access to a network. They expose confidential information in order to shape public discourse during elections (Gehl & Lawson, 2022). Or they might install ransomware on machines, encrypting the data, promising to decrypt the data only after receiving a payout.

But what we don't often get told is what to do *after* a cyberattack is successful. How do we communicate with those affected? With consumers, citizens, investors, publics, or partner organizations? Which members of the organization should speak, and to whom? And—in the case of successful ransomware attacks—how do we communicate with attackers? Should we? More importantly, how do evaluate the effectiveness of these communicative acts?

2. Cybercrime minitrack 2024

Fortunately, this year's Cybercrime minitrack offers answers to these questions. But first, a bit about the Cybercrime minitrack in general. As we wrote in our introduction to last year's minitrack, our goal is to "develop a theoretical and practical understanding of issues related to cybercrime without excluding any methodological approaches" (Harviainen et al., 2023,

URI: https://hdl.handle.net/10125/106890
978-0-9981331-7-1

p. 3609). We encouraged empirical investigations and theoretical insights into the multiple practices and meanings of cybercrime. This year, just as last year, we cast a broad net, seeking to attract the state-of-the-art in cybercrime research.

3. Review of accepted research

And, like last year, we are excited about the results. For HICSS-57, three manuscripts were accepted for presentation and publication. The first paper (Cram, Chan, Yuan & Joo), *Conceal or Communicate?* focuses on the moment when a ransomware attack becomes publicly known, considering patterns of communication from affected organizations. Examining 101 distinct ransomware incident notifications, the authors discover varying transparency in the responses. They conclude with specific recommendations to organizations for this form of crisis communication.

Relatedly, the second paper (Abbatemarco, Salviotti, D'Ignazio & De Rossi), *Understanding Leadership Competencies in Cyber Crisis Management*, examines the extreme pressures faced by leaders of organizations that have been successfully cyberattacked. Drawing on the crisis management literature, the authors focus on the case of the successful NotPetya attack on the shipping company Maersk. The company's response to the attack has been widely hailed as successful; the authors investigate why this was so, abstracting principles from the case for wider application.

The third and final paper (Luu, Jones & Samuel), *The Effects of Dark Triad Traits and Perceived Law Enforcement Competence in Responding to Ransomware Attacks*, draws on survey data to consider the range of responses individuals might take when they are victims of a ransomware attack. The typical responses include paying the attackers, abandoning the data, or communicating with law enforcement. Using the psychological concepts of "dark triad" personality traits, the authors explore how negative personality traits may result in suboptimal outcomes in ransomware responses.

4. Conclusion

The variety of types, methods, and actors involved in cybercrime is immense. So, too, is the complexity of means to respond when organizations and individuals are successfully attacked. Given the scale and scope of cybercrime across the globe, and given how often attackers are successful, knowledge about how to communicate and act during and immediately after a crisis is now a necessary part of the equation. Such communication may happen at many levels of an organization, from leadership to PR offices to individual members. This communication can either be effective in allaying concerns from stakeholders, bringing about a swifter end to the crisis, and helping organizations and individuals move on with their lives, or it can exacerbate the crisis.

We have been warned that it's largely a matter of when, not if, we will endure a successful cyberattack. In that case, researchers will have to increasingly focus on developing theories, tools, and practices for successful responses to these events.

5. Funding

This research was undertaken thanks in part to funding from the Canada First Research Excellence Fund; the Polish National Science Center (Narodowe Centrum Nauki) grant 2021/43/B/HS6/00710; and the Kone Foundation grant for Kadulta labraan.

6. References

Barragán, C. (2023, June 24). The Romance Scammer on My Sofa. *The Atavist Magazine*.

Gehl, R. W., & Lawson, S. T. (2022). *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Create a New Form of Manipulative Communication*. MIT Press.

Gramer, R., & Iyengar, R. (2023, April 17). How North Korea's Hackers Bankroll Its Quest for the Bomb. *Foreign Policy*.

Hadnagy, C., Fincher, M., & Dreeke, R. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. Wiley.

Harviainen, J. T., Siuda, P., Hamari, J., & Gehl, R. W. (2023). Understanding and Moving Forward Research on Online Crime: Introduction to Cybercrime Minitrack. In B. X. Tung (Ed.), *Proceedings of the 56th Annual Hawaii International Conference on System Sciences, HICSS 2023* (pp. 3609–3610).

Meet the Script Kiddies: Teenage hackers who make or break our world. (2023, May 26). *Euronews*.

Nurse, J. R. C. (2019). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *The Oxford Handbook of Cyberpsychology* (p. 0). Oxford University Press.

O'Rourke, M. (2016). The Costs of Low-Tech Hacking. *Risk Management*, 63(7), 40.