Thinking Like They Do: An Inside Look at Cybercriminal Operations

Gianluca Stringhini, University College London

The cybercrime landscape has evolved considerably in the last 15 years. What once was a business ran by hobbyists in their basements is today a large ecosystem with a real economy and different actors that are very specialized and interact with each other in a complex economy. A cybercriminal who wants to set up his operation nowadays has to interact with multiple specialized entities, each responsible for one component required for the success of the illicit operations. For example, a cybercriminal willing to send spam to victims around the globe will need to acquire a list of victim email addresses from a specialized harvester, rent a botnet – which is a network of infected computers – from another specialized crook, and finally will need to join a spam affiliate programme and include a link to an illegal market site on his spam emails. He will then receive a cut out of the money that his victims actually spent to buy goods on the affiliate market.

Despite cybercrime being a major problem, the cybercriminal ecosystem described above is still not well understood by the research community. A good understanding of the actors involved in this economy, as well as of the problems that they face and of the key aspects that make their operations successful is of fundamental importance to develop mitigation techniques that can actually send cybercriminals out of business. In this talk, I will provide an overview of our efforts in understanding the underground economy linked to spamming botnets, performed over the last four years. I will first describe our efforts in taking down the Cutwail spamming botnet, in conjunction with law enforcement and companies [2]. I will then present the insights that we obtained by analyzing the data collected during the takedown: by analyzing the historical data contained on the botnet command and control servers we were able to learn about important aspects of the botnet, as well as key differentiators that distinguish successful spammers from the ones that did not make any money [1]. Finally, I will describe our measurement study aimed at tracking the relationships between the different specialized actors in the spam landscape: email harvesters, botmasters, and spammers [4]. I will then discuss what our observations teach us, and how we can leverage them to develop more effective mitigation techniques [3, 5].

References

[1] J. Iedemska, G. Stringhini, R. Kemmerer, C. Kruegel, and G. Vigna. The Tricks of the Trade: What Makes Spam Campaigns Successful? In *International Workshop on Cyber Crime*, 2014.

[2] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2011.

[3] G. Stringhini, M. Egele, A. Zarras, T. Holz, C. Kruegel, and G. Vigna. B@BEL: Leveraging Email Delivery for Spam Mitigation. In *USENIX Security Symposium*, 2012.

[4] G. Stringhini, O. Hohlfeld, C. Kruegel, and G. Vigna. The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*, pages 353–364. ACM, 2014.

[5] G. Stringhini, T. Holz, B. Stone-Gross, C. Kruegel, and G. Vigna. BotMagnifier: Locating Spammers on the Internet. In *USENIX Security Symposium*, 2011.