European Cyber-Security Research and Innovation

by Federico Maggi, Stefano Zanero, and Evangelos Markatos

Looking back at the evolution of cyber criminal activities, from the nineties to the present day, we observe interesting trends coming together in what may seem a perfectly orchestrated scene. In parallel with the 'security by design', we recall the importance of reactive security in a field of ever-changing arms races.

From the Morris Worm to Invisible Malware

In 1988 the Morris Worm [1] marked the beginning of the first of three decades of malicious software: malware written by developers to demonstrate their skill. In the early days, it was not uncommon to find reconnaissance traces identifying the author purposely buried in the code.

Around the beginning of the 21st century, something changed. Criminals started to see business opportunities from compromising and remotely controlling machines. Since then, opportunistic, organized and profit-driven attacks have been rising at an extraordinary pace. For the last 10–15 years the cyber criminals' goal has been to infect as many targets as possible in order to create new botnets or increase the power of those already in existence. More powerful botnets meant more profit, which came from stolen information (e.g., credentials, credit cards) or directly from renting out these attack-as-a-service infrastructures. Our analysis in Chapter 11 of the Red Book [2] shows that modern botnets are also extremely resilient, guaranteeing the cyber criminals long lasting supplies of offensive capabilities.

Today, thanks to the increased sophistication of the research and industry countermeasures, we observe a slight reduction of mass-malware attacks, which have become, to some extent, the background noise of the Internet. Meanwhile, new and more powerful actors have appeared on the scene. On the one hand, the criminal organizations are now more powerful than in the past, thanks to the technical and financial resources accumulated over the years. According to our analysis in Chapter 1, the global market of cyber crime has surpassed one trillion US dollars [3], which makes it bigger than the black market of cocaine, heroine and marijuana combined. On the other hand, hacktivists and state-sponsored attackers have skills and access to resources like never before. Our sources estimated that, as of 2012, about 88% of the EU citizens have been directly or indirectly affected by cyber-criminal activities. However, as we analyze thoroughly in Chapter 6, the era of opportunistic attacks seems to be fading, leaving the floor to high-profile persons, critical infrastructures, political activism and strategic espionage, which are now the top priority of both attackers and defenders. Modern malware samples evade automated analysis environments used in industry and research, performing only benign activities up front, stealthily interspersing unnoticeable malicious actions with benign ones.

From Incident Avoidance to Incident Response

The presence of sophisticated threats combined with this tendency to disclose vulnerabilities and an increasing value of the targeted assets obviously leads to higher levels of risk. We foresee two strategies to change this scenario and minimize the risks. The first—and perhaps not very innovative—reaction is to focus on creating less vulnerable systems by, investing in software quality, using safe programming languages, etc., and to address the remaining security bugs by creating tools and methods to find vulnerability and patch systems faster. However, experiences of recent decades have taught us that, despite significant advances in software protection, awareness among vendors, and attack-mitigation techniques, vulnerabilities are continuously being discovered. This is one of the conclusions that we draw in Chapter 4 of the Red Book, which focuses exclusively on software vulnerabilities.

What is the answer? Can we be effective in ensuring our systems' security? Our answer is that innovation in this field needs to adopt a different definition of security. A secure system today is not a perfect system, against which any attack attempt is detected and stopped before damage occurs. Vulnerabilities, attacks and incidents simply cannot be avoided. The skills, motivation, resources and persistence of modern cyber criminals are such that they will get where they want. We need to change the way we deal with the problem.

Current and Future Approaches

Incident response is not a new process, product or service. It is important to note that incident response is perhaps the most human-intensive task in system security after vulnerability research. Modern incident response should go beyond old-school control rooms with thousands of alerts and graphs calling the attention of the overwhelmed analyst. Modern incident response requires (1) extreme adaptability to new tools (e.g., malware), techniques and tactics, which change rapidly, (2) fast access to intelligence data, and (3) deep understanding of the threat scenario. Gone are the days of large, complex all-in-one security dashboards, which become immediately obsolete as the cyber criminals learn to adapt.

To complement the detailed system security research roadmap given in the Red Book, we conclude by recalling the importance of effective incident response as one of the drivers that will foster the next decade of industry and research innovation.

Link:

The SysSec Consortium: http://www.syssec-project.eu/

References:

[1] E. H. Spafford: "The Internet Worm Program: An Analysis", Purdue Technical Report CSD-TR-823, 1988, http://spaf.cerias.purdue.edu/tech-reps/823.pdf

[2] The SysSec Consortium: "The Red Book. Roadmap for Systems Security Research", http://www.red-book.eu/

[3] N. Kroes: "Internet security: everyone's responsibility", Feb. 2012, http://europa.eu/rapid/press-release_SPEECH-12-68_en.htm.

Please contact:

Federico Maggi, Politecnoco di Milano, Italy
E-mail federico.maggi@polimi.it