FONDAZIONE BRUNO KESSLER
MAGAZINE

Bit armies

May 10, 2023

Silvio Ranise, director of FBK's Center for Cybersecurity and professor of Computer Science at the University of Trento, was among the speakers at #WNF23 and talk about cyber attacks and their effects in the real world. Riccardo Meggiato, consultant in digital forensics and cybersecurity, discussed with him

Moderated by Wired journalist Luca Zorloni, Meggiato and Ranise alternated practical considerations and theoretical distinctions to introduce some key aspects of the evolution of cybersecurity.

First, Meggiato mentioned that today's cyber attacks are the result of increasingly complex strategies that require very long preparation times and consequently a very consistent activity of studying networks by attackers. What in jargon is called the "Cyber kill chain,", i.e. the tracking of the planning steps of an attack, includes a series of preparatory stages that are followed by the actual attack action (so-called delivery) and, if successful, by its effects.

Prompted by the moderator on current events and in particular with reference to the possible use of Chat Gpt to enhance cybercrime, Ranise pointed out that this new technology does allow for the sophistication of attacks, making them more scalable and effective, but he also recalled that the same tools can be used as a remedy. Fortunately, there is more than just the dark side, as the same technologies are available to ethical hackers to perform, for example, "penetration testing," i.e., to simulate attacks and test the vulnerabilities of systems, vulnerabilities that, once explained, can be remediated.

Starting from the question of whether the human being is the weak link in the chain, the speakers pointed out that the psychological/social component is very important and launched a warning: the centrality of cybersecurity in public discourse must not deceive us: although awareness has apparently increased, human errors must be taken into account and above all we must not think that the attacks are not simple solution puzzles

In this context, the issue of competency, stands out, that in the knowledge chain involves several steps from education opportunities offered in high school and furthered with university studies, to training and exposure to research as occurs at FBK. Much more widespread skills and awareness are critical. This implies an issue of cybersecurity culture that averts new "horror stories" generated by careless configuration. If, for example, a system administrator puts a service on the Internet," Ranise commented, "paying attention only to efficiency and scalability while not taking care of

security, he or she will significantly increase the risk of attacks. That is why basic and advanced skills, e.g., on theoretical and applied cryptography, need to be created widely among the widest possible range of Information Technology (IT) experts.

For cryptography in particular, both theoretical and applied skills must be developed. Indeed, there is a huge imbalance between the “algorithm on paper” and its implementation. The example given is that of using it with the wrong parameters, which makes using such techniques pointless and provides a false sense of protection. Thus, having education opportunities between college and work becomes increasingly useful, as companies need people with cybersecurity skills who can apply them in all contexts.

Further complicating the picture is the introduction of quantum computing that could crumble the protection offered by the cryptographic techniques currently used to ensure the confidentiality, integrity and authenticity of data exchanged over the Internet.
On this aspect, taking into consideration the complexity of the situation and the need for coordination among various global players to gradually reach shared standards, Ranise reassured the audience by saying that it will still take a few years to have quantum computers capable of decrypting according to new logic.

Cryptography used everywhere today is based on the difficulty of solving a mathematical problem (which takes years). Theoretically, the new quantum computers will be able to solve the same questions in minutes or even seconds, e.g., by unearthing encryption keys or by affecting integrity, i.e., by allowing attackers to change the characteristics of operations without leaving marks, as if they had actually been produced by the successfully attacked owners.

The international cybersecurity research community is involved in a huge social effort to make algorithms more and more robust. For this reason, we are starting to talk of crypto agility, i.e. the ability to replace cryptographic algorithms as quickly as possible while safeguarding security. In particular, businesses will need to move from a reactive approach to a poractive one, considering update planning as an inescapable aspect.

In closing, Ranise mentioned SERICS, a cybersecurity initiative that combines the contributions of research and businesses thanks to the substantial resources made available by the PNRR and that promises to give our country system a quantum leap by focusing on an interdisciplinary approach to improve cloud, digital identity, awareness and compliance in accordance with rules coming from other sectors that are themselves rapidly evolving such as privacy and AI.

On the same day of the festival, Sunday, May 7, 2023, the Workshop “Cybersecurity is not just stuff for nerds,” was held, that featured FBK-Cybersecurity Center researcher Matteo Rizzi, along with Elisa Rapetti from Edi onlus and Carmelo Ferrante from digitalforensics.it

The three speakers gave a fresco of cyber risks in particular with regard to minors, focusing especially on child grooming – manipulative technique to create an emotional-sexual relationship, consisting of 5 phases: friendship, risk assessment, building a relationship of trust, exclusivity phase (isolating the victim is the violence in grooming, based on control and humiliation), and finally sexualized relationship (with photos to blackmail and/or force offline dating).

In Italy, it has been a crime since 2012. It does not need to involve offline encounters for it to be considered a criminal offence, the only attempt is enough. 424 cases were reported in 2022. The rate is growing and the number of unreported ocurrences due to guilt or shame for trusting a stranger, is substantial. The starting age is around 9 years old, and video games and social networks are the most frequent channels. The situation signals the importance of conducting education actions both on social media and emotional relationships and sexuality.

In terms of prevention, much can be done. Rizzi focused on the issue of digital footprint, i.e. how many footprints we leave when we surf the Web. Through simple examples on email use or online reviews, he showed how much precise information can be gleaned about a person’s location and their likely personal details, spending capacity inferred from posts, assumed lifestyles, and other contextual inputs. Triangulation of available data underlies these heuristics. On top of this, metadata, e.g. photos taken, which provide additional valuable data.

Fortunately, GDPR protects European citizens, but caution is never enough. Among the useful tips pointed out by experts, in addition to being aware of the active accounts and apps that have access to our data that we use on a daily basis through our smartphones, it is important to consider Cybersecurity as a set of common sense rules to maintain a sufficient level of “digital hygiene.” We can carefully monitor what we have subscribed to and what services we give our children access to, view our content as if we were other users so we can understand what others see; separating work email from personal email, adopting multi-factor authentication are some of the ways to do it.

PERMALINK

https://magazine.fbk.eu/en/news/bit-armies/

TAGS

- #cyberbulling
- #cybersecurity
- #digitalization
- #fondazioneserics
- #pnrr
- #prevention

RELATED MEDIA

- VIDEO registrazione dell'evento: https://www.linkedin.com/video/live/urn:li:ugcPost:7060962220569993216/?actorCompanyId=243693
- Fondazione SERICS (PNRR - cybersecurity) : https://serics.eu/

AUTHORS

- Giancarlo Sciascia