Computer-Security-Oriented Escape Room

Erwan Beguin, Solal Besnard, Adrien Cros, Barbara Joannes, Ombeline Leclerc-Istria, Alexa Noel, Nicolas Roels, Faical Taleb, Jean Thongphan, Eric Alata, et al.

Computer security oriented escape room

Erwan Béguin, Solal Besnard, Adrien Cros, Barbara Joannes, Ombeline Leclerc-Istria, Alexa Noël, Nicolas Roels, Faïçal Taleb, Jean Thongphan, Eric Alata, Vincent Nicomette
INSA Toulouse/LAAS-CNRS
Université de Toulouse, CNRS, INSA, Toulouse, France

***Abstract*— New types of attacks are developed daily targeting companies. If employees are not aware of the consequences and tactics of such attacks, they are not protecting their company. Current teaching methods, such as lectures and videos, may not prepare participants for real life situations. To raise awareness about computer security, two escape rooms were developed by teachers and students of INSA Toulouse, with different approaches for the same goal: raising awareness. Players learn how to reduce risks of being a computer attack victim during hour-long real-life simulations. Choosing strong passwords and spotting fishing emails are just a few of the habits our escape room scenarios can instill in participants to mitigate the damage of hacks and social engineering attacks.**

I. Context and motivation

Current society displays an increase in reliance on computer systems and the Internet with new technologies changing our way of living and working. This surge in new technologies makes cyber security a main concern for both users and companies. Yet many people are still not aware of the risks they are subject to. This problem is especially noticeable with the increased adoption of Internet of Things and smart devices [1,2]

On another hand, more and more attacks target human flaws and errors: social engineering attacks [6]. These attacks mostly target employees who are not always proficient in computer science but use it daily at work.

The fact that such attacks, such as phishing, are still successful nowadays shows that education regarding computer security is not yet effective. Also the Mirai botnet [3] showed that default passwords on devices are not getting stronger and are as easy to find as they were in 1988 by the famous Internet Worm [4]. Educating users is thus as important as educating programmers who create such vulnerable software and devices.

II. Benefits of using an escape game as a teaching tool

Raising awareness about a subject is usually done via conferences, videos or lectures. However, the participant is most of the time passive and does not always remember the advice given nor how to apply them once at home or at work. The use of game methodology emerged in the professional context in the last few years with gamification and a rise in the use of educational games. Game methodology involves the student in an active role, brings a sense of progress and achievement, and thus is observed to increase interest and motivation compared to traditional teaching methods [5].

Escape games, or escape rooms, are games in which a team of players is trapped in a room and have to solve series of enigmas and riddles to achieve a goal, usually escaping of the room, within an hour. These games can be great learning tools because they combine the fun of games and the satisfaction of accomplishing a goal. Contrary to regular learning methods, in escape games, the player is not passive but active. More importantly, the player will already have performed a number of computer security related actions making it easier for her to repeat these actions in her day to day life. The room should be as realistic as possible to create an environment that the participants will identify with. The goal is to create enigmas that resemble situations lived almost daily by the players, mainly in their work environment. Lastly, escape rooms bring some creativity and diversity to computer security awareness efforts. So far, games have rarely been used to raise awareness or teach skills that enable to turn awareness into everyday security decisions.

Briefing and debriefing are very important parts of the game too. The goals must be defined beforehand. At the end of the game, game masters should have a detailed debrief with the players to ensure the goals have been reached and explain any enigma that has not been solved.

III. Room creation

Enigmas need to be created combining technical aspects, social engineering and physical elements such as confidential documents and personal belongings. Furthermore, the room should be as realistic as possible so players understand that computer security manipulations done during the game can be repeated at home or at the work place.

For each enigma, a descriptive sheet was written. This sheet included the enigmas description, its solution, the elements required to solve the enigma, the useful clues brought for the next enigmas, tips to give players if needed and which computer security aspect was related to the enigma. Once every enigma sheet was completed, it was time to organize enigmas in a logical order depending on the scenario. To do so, an organizational chart was created linking enigmas to one another and to objects in the room. Enigmas were organized in a non-linear way for various reasons. It stimulates team work, forcing players to communicate with each other. It also avoids

boredom as solving an enigma does not always lead to another one directly. Of course, in some scenarios, a more linear enigma organization may be more suitable.

Lastly, a detailed plan of the room was drawn. Each object was carefully placed in a location depending on it relation to other objects or enigmas. The goal was to recreate a work environment so that players would identify with the space and the objects within it. Here is part of the room plan for one of the scenarios detailed further.

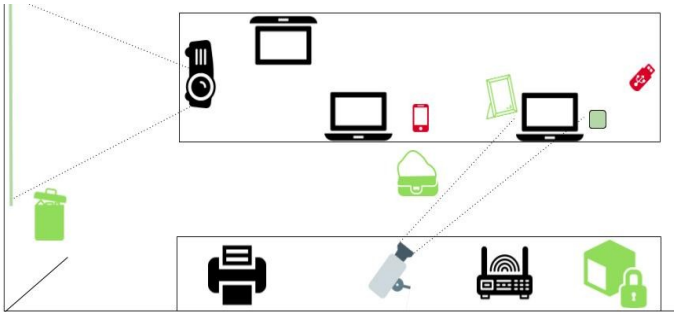

Fig. 2. Part of a room plan showing computers, a phone, a USB key, a smart camera, a router, a locked box, a printer, a projector and other objects.

We expect to make the relevant documents (the enigma descriptive sheet, the logical order organizational chart and the detailed room plan) available to interested researchers at a password-protected site [8]. The researchers can email the authors to obtain the password.

IV. Different scenarios

We created two escape rooms with different approaches but with the same objective - teach participants how to protect themselves from computer attacks.

A. Defense scenario

For the defense room, the idea is to get participants to patch vulnerabilities in the room for an hour. The room is designed as an open space: there are four to five computers, a white board, a video projector, a router, a security camera, paper documents and closed drawers and boxes. Each one of the four participants plays the role of an employee working in this open space. Before the game begins, they are all given a sheet with some of their accounts' password and details about their character. The scenario is the following: the company has received a threat from a hacker and they have an hour to secure the company to reduce the risks of a successful attack.

There are many vulnerabilities to correct including weak passwords, computers left on and unlocked, sensible information left on a white board, etc. There are also some traps from the "hacker" like an infected USB key [7] and a few spear phishing emails with malicious links or attachments. The players earn points for each vulnerability corrected and loose points if they fall into a trap. To further motivate them during the hour-long game, it was decided to add a second objective: identify the threatening hacker.

As not all successful computer attacks are very technical, social engineering attacks protection mechanisms were included in the game, through the presence in the room of a smartphone which is used by the players to communicate with someone pretending to be the company's network manager.

B. Attack scenario

For the attack room, the functioning principle is simple: participants will take the role of a hacker team which has to attack a company in order to retrieve a document for a third-party. To reach their goal, they will need to exploit a series of vulnerabilities in the premises of the targeted company. Like in the defense scenario, action takes place in an open space office, with a lot of office supplies, but this time there are two different rooms separated by a locked door. In this scenario, the purpose is to make participants identify, then use vulnerabilities so that they realize how unsafe those security breaches may be. This way is less direct and intuitive than in the defense room, but it is very interesting to see how people learn in different cases.

The sequence of enigma follows a linear guideline: players need to solve each enigma before the next one, but there is also information gathering and physical search in parallel to keep a lot of dynamism. This kind of sequence is necessary because participants need to be guided, if there are too many enigmas in parallel, they might not understand what prerequisites they need to go further in the scenario. The game is designed to reproduce privilege escalation; players have to access the secretary's computer then the accountant one to finally reach the administrator's desktop which is in the locked room.

Along the game, participants will have to exploit exposed breaches to progress towards the final step. Those vulnerabilities are linked to user safety problems because the main purpose of this escape room is to train and raise awareness among users with an average computer science level. Many enigmas highlight negligent or non-adapted behavior more than technical or specialized content. A broad range of security items, from physical safety to social engineering passing by information exposure, are found in the room. Each item is realistic and rooted in reality, to allow people to easily identify the room with their work and link the simulation they are playing with real world situations.

V. Feedback

After each game the participants completed a survey to evaluate the knowledge and skills learned during the game. We also collected unstructured feedback. Participants were students and professionals from various specialties.

A. Feedback on the defense scenario

The defense scenario has been played by nine teams of four players, making a total of thirty-six participants so far. It was intended to diversify as much as possible the players' background in order to have different ages and fields of expertise. All were very positive about the experience and confirmed that they learned a lot more during the game than they would have during an hour-long lecture. For example, risks of social engineering attacks and of accessing the Internet with administrator's account were a new knowledge for many partciaipants.

When finding the USB key in the room, attitudes diverged depending on how far along in the game the players were. If found at the beginning, participants were more hesitant and careful before taking a decision - good or bad. But if the USB key was discovered close to the end of the hour, it was inserted in a computer almost right away. This attitude illustrates than upon stress and pressure, humans are more likely to make mistakes and take irrational decisions. This is a typical human flaw that attackers use in social engineering attacks along with curiosity.

During the decision-making process, it was often observed that a single individual's doubt changes the rest of the group's opinion. For instance, while having a phone conversation with the attacker, if a player thought it was not such a good idea to reveal the password, the team ended up not revealing it. This behavior illustrates that it is possible to bring awareness to a large group of people by informing a few members of the group about the risks and good security habits to adopt.

Results of the surveys taken after the game were analyzed and here are some notable statistics. Regarding smart devices, all participants were convinced that Internet connected surveillance cameras could be vulnerable and present risks for companies but half did not think that other smart objects can be too. Smart devices are increasingly present in our society, both in our personal life and at work. However, few people think about securing these objects that are as vulnerable, if not more, than other electronic devices, such as computers or routers.

Looking at the survey results, it can be understood that all players knew about the importance of not leaving a computer on and unlocked without surveillance. Yet, very few groups turned off the computer, which was left on and unlocked in the defense room. This phenomenon can be observed in companies. Employees know they must lock their computer each time they leave their desk - no matter for how long they are away - but a lot of them still fail to do it most of the time (we don't know if they forget or if they choose to not follow the security guidance). Our escape room was purposely designed to help motivate or instill locking habits.

B. Feedback on the attack scenario

For now, the attack scenario has been played by five teams of two to three players, making a total of fourteen participants. Just like the defense scenario, it was intended to diversify as much as possible the players' background in order to have different ages and fields of expertise for example. So far, the players were pupils, students or professionals, and were ten to fifty-five years old. All the players agreed that they learned a lot while playing. Computer science students confirmed that it was easier to remember bad behaviors after exploiting them as a "bad guy". On the other hand, non-specialists were glad to get introduced to good practices thanks to a game. They admitted they would never have attended an hour-long lecture about security, because they do not feel concerned.

Player feedback allowed us to analyze the players and collect statistics about their behavior and their computer security knowledge before and after the game. We noticed that players tend to forget the objective during the game. When they arrive in the room, they try to break into the computers without really knowing why, and usually lose a lot of time. Participants told us that, at the beginning of the game, they were so focused on technical aspects and the current enigma that they almost forgot they were in a game.

Also, in the attack scenario there are employees' personal objects lying around, such as a jacket and a purse. One of the teams needed a lot of time to find out this was part of the game. Every player was convinced the jacket belonged to another teammate. It took them thirty minutes to realize they could interact with it. This behavior illustrates that often people think it is safe to leave their belongings in a room, and forget than an attacker could break into their office to steal sensitive information about their company or themselves.

One of the most important statistics is that sixty percent of non-computer scientists were convinced that they could not be victim of social engineering attacks. Most of them thought it happens to others and they could easily recognize that kind of attack. At the end of the game, the question was asked again, and luckily all the players realized how easy it was to fake an identity. It was important that this aspect was included in the scenario because of the increasing presence of social engineering attacks, such as phishing or impersonation scam.

VI. Conclusion and perspectives

Overall, participants were happy to have taken part in these escape games and their feedback was always positive and rewarding. Every player learned something by playing in these rooms and confirmed it was an interesting and effective teaching tool.

However, both rooms can still be improved. More tests are planned to finalize the scenarios and software. Currently, it is still necessary to have a game master in the room to check that there are no technical difficulties and make sure players stick to the game. For the defense room, points could be given automatically depending on the players' actions rather than manually.

References

[1] K. Zhao and L.Ge, "A survey on the Internet of Things Security", in Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security (CIS), pp 663-667, December 2013, doiieeecomputersociety.org/10.1109/CIS.2013.145

[2] Kaspersky Lab, "The state of Industrial Cybersecurity 2018", https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

[3] Manos Antonakakis and Tim April and Michael Bailey and Matt Bernhard and Elie Bursztein and Jaime Cochran and Zakir Durumeric and J. Alex Halderman and Luca Invernizzi and Michalis Kallitsis and Deepak Kumar and Chaz Lever and Zane Ma and Joshua Mason and Damian Menscher and Chad Seaman and Nick Sullivan and Kurt Thomas and Yi Zhou}, "Understanding the Mirai Botnet", in Proceedings of the 26th USENIX Security Symposium, pp 1093-1110, Vancouver, BC, 2017, USENIX Association.

[4] J.A. Rochlis, M. W. Eichin, "With microscope and tweezers; the worm from MIT's perspective",

Communications of the ACM, Volume 32, Issue 6, pp 689-698, June 1989
[5] The Guardian, “Get me out of here! The addictive thrill of escape games”, https://www.theguardian.com/lifeandstyle/201nov/09/puzzle-games-escape-live-birmingham, November 2015
[6] G.L. Orgill, G.W. Romney, M.G. Bailey, P.M. Orgill, “The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems”, in Proceesings of the 5th Conference on Information Technology Education (CITCS’04), pp 177-181, Salt Lake City, UT, USA, October 28, 2004.
[7] Matthew Tischer and Zakir Durumeric and Sam Foster and Sunny Duan and Alec Mori and Elie Bursztein and Michael Bailey, “Users Really Do Plug in USB Drives They Find”, in Proceedings of the 2016 IEEE Symposium on Security and Privacy, 22-26 May 2016, do 10.1109/SP.2016.26.
[8] https://www.Laas.fr/~nicomett/Escape_Room

Appendix

This should go to the sidebar :
Survey:

1. *To remember all my passwords:*
    a. *I write them on hidden post-it or in a notebook.*
    b. *I use mnemonic phrases that I am able to remember.*
    c. *I use the same strong password for all my accounts.*
    d. *I use easy to remember password like “NameOfChild+BirthDay” or I leave defaultpasswords like “admin” or “1234”.*
    e. *I use a password manager software that automatically fill my ids and passwords.*
    f. *I configure my accounts on auto login.*

2. *If I leave my workstation 3 minutes for a coffee, there is no risk if I do not lock my computer*
    a. *True.*
    b. *False.*

3. *When I leave a meeting room*
    a. *I wipe the whiteboard.*
    b. *I turn off or lock all the computers.*
    c. *I can leave my jacket and my bag as I will come back just after lunch.*
    d. *I throw away in the bin the useless documents.*

4. *I found a USB key on the ground of my company’s lobby*
    a. *I plug it on my computer to find out who is the key owner to return it.*
    b. *I give it to the IT centre of my company.*
    c. *I give it to my colleague that is better than me with computer.*

5. *I received an email from a colleague on his personal email address. He sent me a link to download a software that can be useful to me. He attached the software specifications on a PDF file.*
    a. *I click directly on the link and download the software. This is exactly what I needed!*
    b. *I call him to see if this email is indeed from him because he usually writes me from his professional email address.*
    c. *I open the PDF file to know a bit more about this before clicking on the link.*
    d. *I transfer the email to another colleague to know his opinion about this software.*

6. *On Internet and on social networks, what I publish is only visible by my friends.*
    a. *True.*
    b. *False.*
7. *My email inbox protected by a strong password is a good way to store confidential and personal information.*
    a. *True.*
    b. *False.*

8. *The connected objects that can represent a vulnerability for a company are:*
    a. *Surveillance camera accessible from the outside via Wi-fi.*
    b. *The boss’s smart watch connected to his smartphone via Bluetooth*
    c. *The personal smartphone of a technical manager.*
    d. *The smart TV in the meeting room.*

9. *Which situation doesn’t represent a risk for the company (several responses possible) :*
    a. *Open the door to someone saying he has forgotten his badge.*
    b. *Give their login and password on the phone to the IT centre.*
    c. *Bring his own food for lunch.*
    d. *Have the same phone for work and personal life.*

10. *Which Wi-fi router configuration is the most secured?*
    a. *WPA2.*
    b. *WPA.*
    c. *WEP.*

11. *My personal belongings (agenda, ID…) can represent a risk for me if an ill-intentioned person find them.*
    a. *True.*
    b. *False.*