TECH SCAMS: A ONE-TO-ONE ANALYSIS WITH SCAMMERS

As Part of the King's Undergraduate Research Fellowship

Riccardo Gugliermini, Dr Guillermo Suarez de Tangil[1], Javier Carrillo Mondéjar[2]

Faculty of Natural, Mathematical & Engineering Sciences, King's College London, London WC2R 2LS

1. *IMDEA Networks Institute and Cybersecurity Group, King´s College London, London WC2R 2LS*
2. *Universidad de Castilla-La Mancha, C/ Altagracia, 50, 13071 Ciudad Real*

Introduction

Over the last two decades, the Internet has been taking an enormous part in people lives, who have been storing every kind of data in them, even very confidential one (a trite example could be baking details). Unfortunately, when their devices connect to the Internet, they become exposed to several threats of many different types. One of these is known as "*tech support scam*", where a scammer makes the user believe there are some issues with their personal devices and then acts as a support technician to gain control of the victim's computer.

Objective

This research aims to build a software tool that gathers information about tech scams in order to build a deep level analysis. To achieve this, it connects users to real scammers (via a simulated real-life environment) and let them gain control of the devices.

Method

The type of scam took into consideration in the research is tech support scamming. It happens when a scammer impersonates a tech support assistant. A user usually gets notified that their device has some issues (such as malware infection) and then is given some contact details to tech support to get help to resolve the problem. Consequently, the user calls the tech support (which are scammers). Over the call, the scammers ask the victim to download some software so that they can take remote control of the personal computer. Once got it, they are then able to infect the device with malicious software.

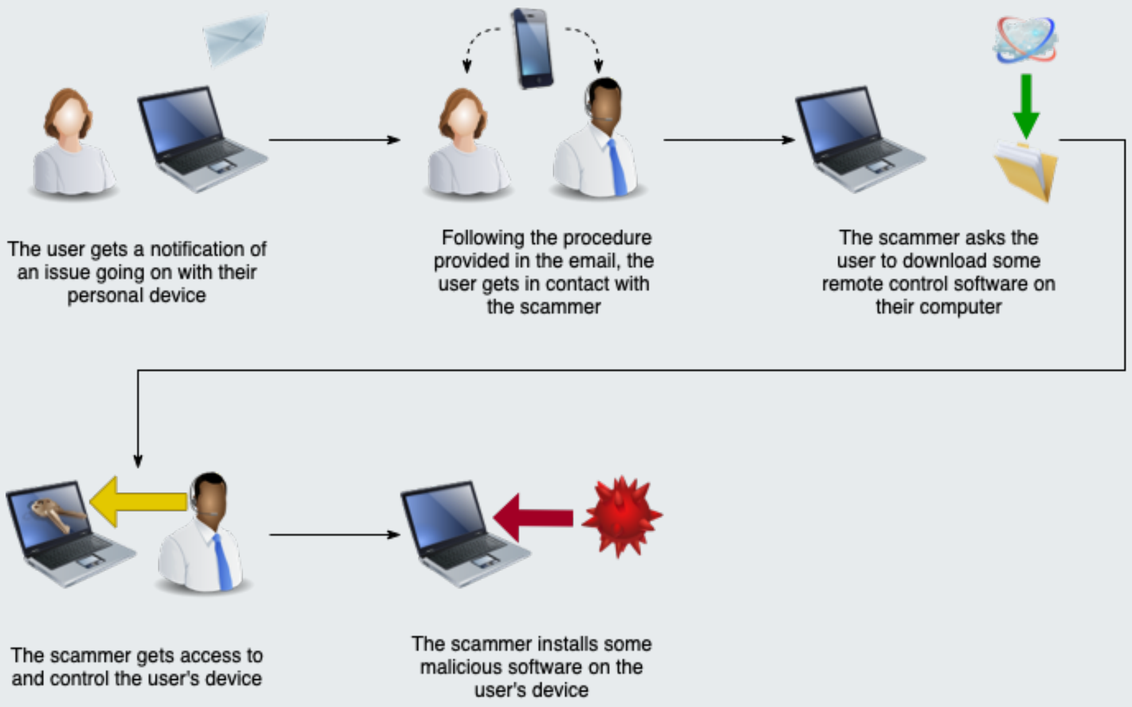

Fig 1: A sample illustration of the scamming process

The tool to be developed by this research needs to simulate a real-life machine, where the user allows scammers to get control of the machine by installing software the scammers ask them to install. Therefore, while the user follows instructions from the scammer over the phone and scammers control the device, this tool monitors the machine from different views.

Results

The scam-analysis tool adopts virtual machines to simulate real-life scenarios and operate in a safe environment. The use of virtual machines is essential to prevent malware to cause damage for the reason that the risk of getting infected by malware is very high. Oracle VirtualBox[1] and its API were used for the purpose of this research.

Furthermore, the creation of real-life scenarios is easier with virtual machines. Virtual machines allow making the scammers believe they are operating on real devices with real users. Three different real-life scenarios have been initially set up during this research (*Fig 2*).

After that, two python scripts were developed. The first one manages the virtual machine with the integration of *pyvbox*[2], a VirtualBox library for Python. The script is firstly supposed to prepare the virtual machine and set up the environment. The initial operations in sequence are:

- virtual machine start up;
- snapshot recovering;
- screen-recording;
- network traffic capture.

Following the initial setup, the machine is ready and a scammer can be called in order to make them take control of it, while the machine screen is being recorded and the network traffic captured.

Once the scammer has finished taking control with remote administration software[2], the script manages to shut the machine down and save a snapshot.

Remote Administration Tool
Team Viewer
LogMeIn Rescue
CITRIX GoToAssist

Tab. 1: List of software to access personal devices (used by scammers to gain control)

When the virtual machine is eventually down, another python script takes place. This one compares the virtual machine filesystem before and after scammers have operated.

Finally, the script produces a report which logs all the files that were created, edited, and deleted during the scamming operation.

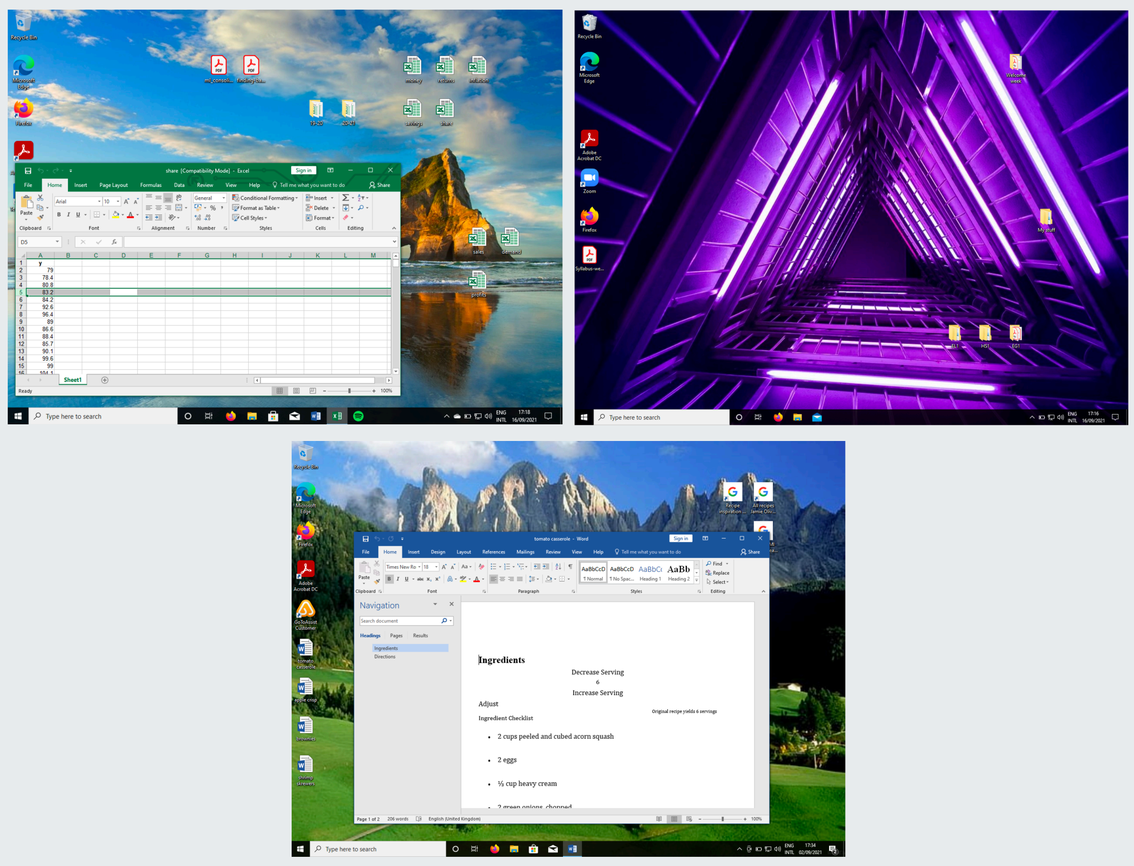

Fig 2: Screenshots of real-life environments set up in the virtual machine

Discussion

Online scams keep growing day by day, and they are becoming more and more dangerous. The effect these scams have on victims could be catastrophic for the reason that users store the most sensitive data on their devices and, once a user gives total control of their devices to scammers, the ladder ones can access the user's most private information (such as online banking details, websites passwords, and others).

The core of the problem is that messages and e-mail that lead to scams are becoming more accurate, and it is many times hard to identify a potential scam message from a safe and real one.

Conclusion

This research provides a tool that can identify and classify scams. This can become helpful when users receive potential scam messages, so that they can compare the message they received with the ones analysed by the tool and possibly avoid to get scammed.

1. Oracle Corporation, *Oracle VM VirtualBox*, Version 6.1.26, available at: www.download.virtualbox.org/virtualbox/6.1.26/UserManual.pdf
2. Michael Dorman, *pyvbox 1.2.0 vbox 5.1.1 documentation*, 2013, available at: www.pyvbox.readthedocs.io/en/latest/index.html
3. N. Miramirkhani, O. Starov, N. Nikiforakis, *Dial One for Scam: A Large-Scale Analysis of Technical Support Scams*, Cornell University, March 2017, available at: www.arxiv.org/abs/1607.06891