## Proposal: Security Nightmare 2015 – Cloud Attack! by David Kelm (david@it-seal.de)

**Assumptions:** In the described setting the company International Traders Ltd. (ITL) has just a few employees of who we assume to know each other and who are able to communicate easily - none of the involved persons is liable to bribery. Moreover, we assume them to have a safe technical environment. Just placing a Trojan horse or a similar malicious file to obtain the target file is not possible. We further assume that there is just this one **Laptop** to access the VMs and one is able to access FileX just in combination with the correct **login credentials** of **Big**, **Ethan** or **Sydney** (to access VM1). The badges, however, authorize the owner to enter the respective area without restrictions.

> Our attack therefore consists of two parts: Obtain correct **login credentials** and get **physical access** to the **laptop** (since it is in general considered safe).

Since Ethan and Sydney can be assumed to be aware of frauds (as fraud investigator and IT system administrator), we focus on **Big**, who as CEO, is probably less aware and more customer orientated. Because he is concentrating on running the business, Big is susceptible to a **Social Engineering Attack**. Since we have presumably just one try, once we get access to the Laptop, we gather passwords from Big in several attempts.

### Part I - *Gathering login credentials*:

To obtain Big's login credentials there are several options:

1. Call Big and pretend to organize an **Investment-Conference** (creating a background-story, setting-up a webpage), and want to consider him as a keynote speaker. He would be one of the main candidates, therefore we need his CV to place some information on the web and flyer. To do so, he needs to register himself on our Conference-Webpage and uploads the file (led to webpage during call). (GOT E-MAIL, GOT PASSWORD1, GOT CV) Together with the CV information and crawling from social media sites we can do a **personalized password guessing** attack and try to break into an E-Mail or other accounts (may be reused for business purpose). (GOT PASSWORD2)
2. In case we can figure out what the **intranet** looks like we can **clone** the login page. When Big is on travel we can send a spoofed E-Mail in Sydney's name and ask to check some critical issue with a customer. To do so he needs to login with his company-account on our cloned webpage. After submitting he is redirected to the real intranet. (GOT PASSWORD3)
3. Offer to install a **video surveillance** component in the open office (creating a background-story, setting-up a webpage), at a competitive price. We can then use our backdoor access to observe the employees (not just Big) using the Laptop and entering their login data - a technical form of **shoulder surfing**. (GOT PASSWORD4)

Several of these options can be executed since they are all designed not to be identified as attacks. That way we get a good chance of having the correct password for logging into VM1.

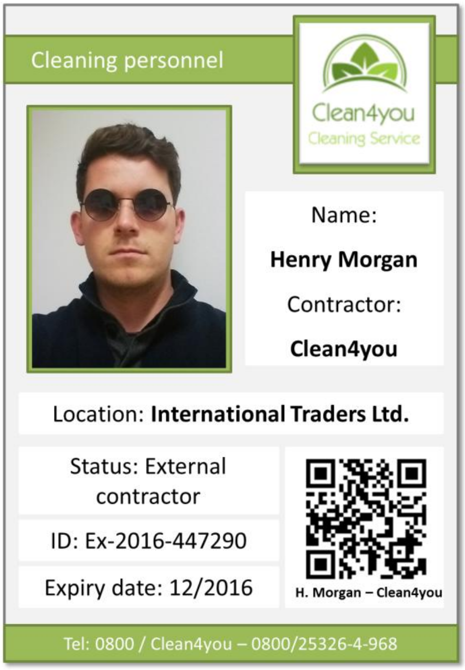
## Part II - Gaining *Laptop Access*:

To gain physical access to the laptop we utilize the business relationship with the **external contractor** (EC). Shortly after obtaining the login credentials (credentials could be changed, if waited to long) we call EC in the afternoon by spoofing Big. We claim not to need Cleo this week (due to some renovation of the OpenOffice) and ask EC to inform Cleo directly. Moreover, we give an alternative phone number for callbacks, since we (Big) are travelling to a conference this week.

Second we call Big by spoofing EC and claim that Cleo is sick for about a week. To satisfy our costumer we will send a replacement Henry. Since he has no badge to access the area and Cleo's badge is not available, Big is asked whether the IT department could grant a temporary badge to be able to enter the building freely.

Once Henry (background-story and costume are prepared) gets his badge he can enter the building, particularly the open office. To access the Laptop, Henry enters the building at night. In case the badge just works in the office hours, Henry comes in late and stays longer, until everybody has left.

Thus, we can achieve access to the Laptop, login and access **FileX** when the room is empty.



Cleaning personnel

Clean4you
Cleaning Service

Name:
Henry Morgan
Contractor:
Clean4you

Location: International Traders Ltd.

Status: External contractor

ID: Ex-2016-447290

Expiry date: 12/2016

H. Morgan – Clean4you

Tel: 0800 / Clean4you – 0800/25326-4-968

**Figure 1: Mockup of the fake identification badge**

***Countermeasures:*** To secure ITL against this attack, one can think of several countermeasures. The most effective one would be to use strong authentication methods as e.g. **two factor authentication** (e.g. biometric). This would even make Option 3 useless when shoulder surfing is employed. Moreover, a **verification/background-check of external personnel** would minimize the threat from this attack vector. Strong mechanisms for frequent password changes or the verification of calls could improve the situation further. Crucial for these measures is also the **education** of all employees, especially the ones who have access to critical information. That way, the **awareness** and knowledge about policies can be strengthened and compliance ensured. Furthermore, it is advised to establish further **physical security mechanisms** to secure the laptop (e.g. to lock it in a safe). Especially overnight a **security firm** could be hired to guard the building.

To discover and track the attack **video surveillance** as well as the use of **logging** mechanisms is advised.

***Outline:*** The described attack scenario is realistic and feasible: it uses simple social engineering techniques that require little technical proficiency and are resilient to software-side security - no deeper hacking knowledge is required. ITL (or a similar company) is extremely vulnerable to this attack if the introductory assumptions are correct. The most comprehensive way to test the vulnerability of ITL is to conduct the attack (or parts) in a real-world simulation - to verify how individuals react and if incident response procedures take effect.