hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.16, NO. 01

SOCIAL ENGINEERING ATTACKS

SOCIAL ENGINEERING TECHNIQUES
USING MALICIOUS DOCUMENTS AND APT TACTICS

INTERVIEW WITH CHRISTOPHER HADNAGY
AUTHOR OF HUMAN HACKING

INTRICACIES OF DELIVERING EFFECTIVE
SOCIAL ENGINEERING ATTACK SIMULATIONS

ANALYZE MALWARE USING OPEN SOURCE TOOLS

AND MORE...

Dear readers,

2021 is finally here! To brighten this month up, we prepared something completely new! This issue is dedicated to Social Engineering Attacks. Let's dive into the content!

We start off with A Practical Introduction to Social Engineering Attacks, in which the author is going to show you how hackers can take advantage of human error and what are the most popular social engineering attack techniques.

Then we're going to drift off to Social Engineering Attacks Techniques Using Malicious Documents and APT Tactics. The title speaks for itself - this article will guide you through various attack techniques with an APT scenario. Later we're going to take a look at How Social Networks are Directly Connected With the Improper Application of Social Engineering that'll help you understand how to use social engineering attacks in social networks, who may be the target of such attacks, and how to protect yourself against them.

We also prepared two absolute gems for you! First is an interview with Christopher Hadnagy - the world's leading social engineer and an author of Human Hacking, an amazing book about using social engineering techniques in everyday life. Second one is Login to Hell, a history of Alberto Daniel Hill - first hacker sent to Uruguay prison for a cybersecurity-related crime. Both articles are very different, but extremely interesting and we hope they're gonna excite you as much as they excited us!

You may also want to take a look at Intricacies of Delivering Effective Social Engineering Attack Simulations, a detailed analysis of social engineering attack simulations.

Later on we have Social Engineering - Frenemy or Foe, in which Syed Peer will introduce you to the topic of social engineering techniques in social media and will teach you how to stay safe during your activities in the depths of the internet.

For those of you who haven't had enough of malware, we prepared Analyze Malware Using Open Source Tools - a very detailed guide to malware analysis with examples and presentation of open source tools' usage - and ARP Cache Poisoning with Ettercap.

Last but not least we have Why do I Want to be a Blockchain Developer?, a part 1 of the introduction to blockchain development with examples of useful apps.

Once again, we wish you all the best for the upcoming year. We hope that with this edition your start in 2021 will be more bright and enjoyable. We would also like to send gratitude to our contributors, reviewers and proofreaders.

Thank you and see you next month!

Hakin9 Editorial Team

Contents

Intricacies of delivering effective Social Engineering Attack Simulations

by Terence Teo, Miguel Tan

Social Engineering - Frenemy or Foe

by Syed Peer

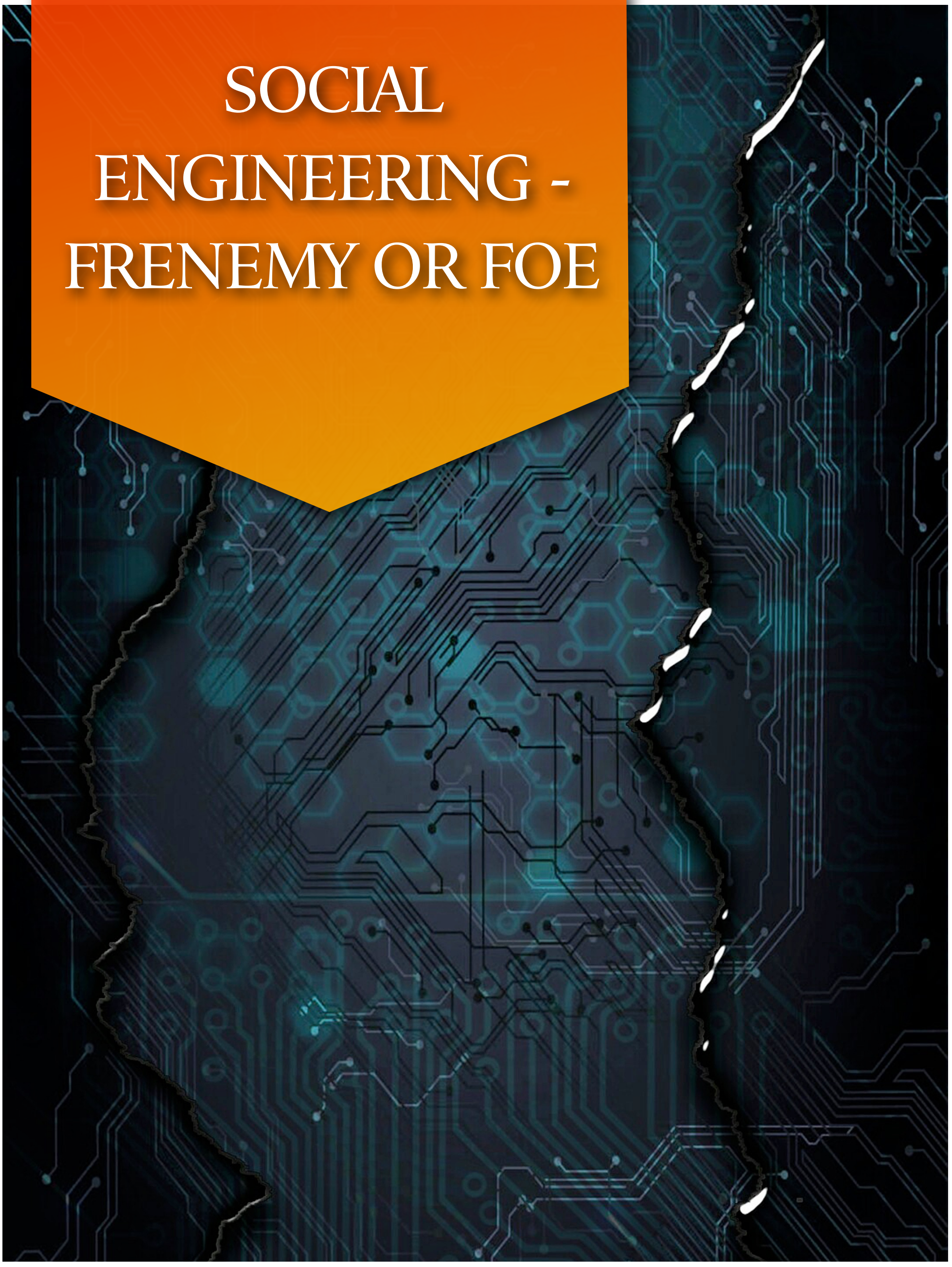
Analyze malware using open source tools

by Adrian Rodriguez Garcia

Login To HELL: The nightmares of an information security professional in South America

by Alberto Daniel Hill

SOCIAL ENGINEERING - FRENEMY OR FOE



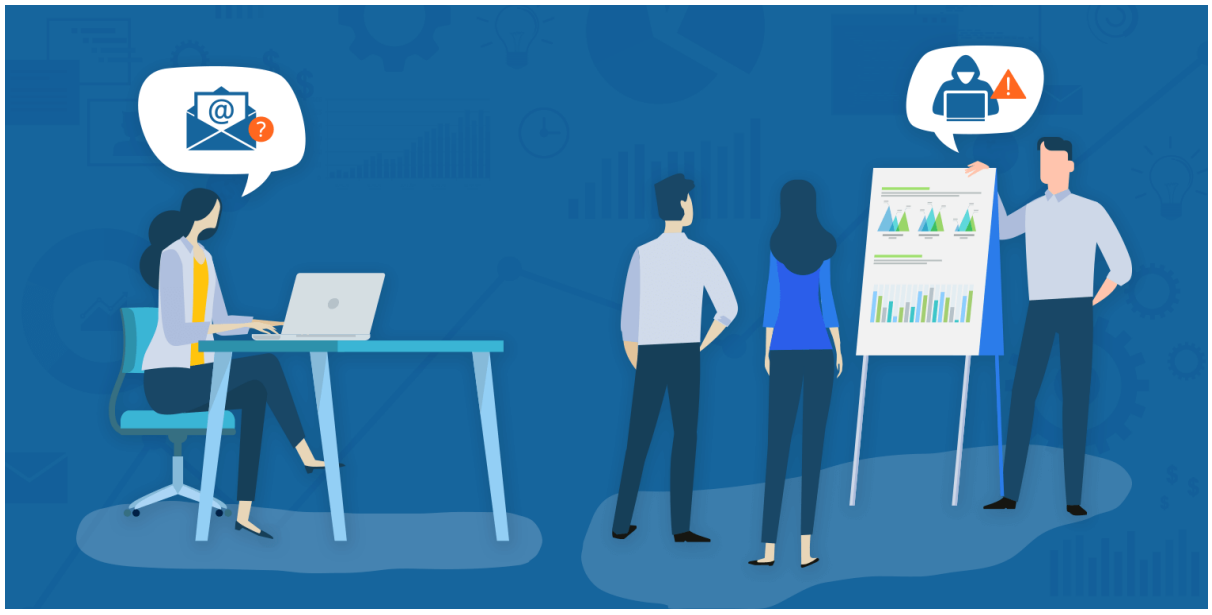
SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering and Cyber Security teams.

Introduction

As we hurtle towards mass internet adoption across the globe at ever accelerating speeds and a mobile device in every pocket, we all must take stock of how much our lives have been changed forever by the digital revolution around us.

From shopping to travel, to work from home during the pandemic, the new "us" is a whole new breed of digital citizen than the days of our parents. The seductive promise of the new web is that everything is so easily within our reach, from our groceries to movie tickets to flight bookings to birthdays and anniversaries. In this rush to get on the bus and start making those all-important connections with family and friends and other netizens, a slew of social media platforms has wet our appetite for connecting, recording, approving, celebrating, aggrandizing and sharing every small detail of our otherwise mundane lives.



And there's the rub.

Social Engineering Defined

As defined by Wikipedia, *"In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information."* Social Engineering has become the Swiss army knife of malware builders and the architects of corporate breaches online.

The modern web and social platforms in particular provide the perfect window into our lives, but are only effective so far as we allow them to be. A fun weekend exercise for young and old alike is just to type your name into the Google Search field and watch all the references that come back to you in an instant. It can be an eye-opening experience that so much information about ourselves (both the good and the bad) is actually out there for the general public to see.

It is not uncommon to have netizens signed up to a half a dozen social media platforms or more. Though "Sharing is caring" is the new mantra online (or so we are told by the marketers), it is important to be cautious and careful in how much an individual is totally invested in social media and what all they are sharing online. Quite often, people will provide too much information online about themselves and their activities. Although their information may be segmented across multiple different platforms, it still provides any able-bodied hacker enough information (patched together across platforms) to triangulate the data and arrive at the most important information about an individual. So much information is already online through the public county records, tax filings, etc., that anyone could easily be forgiven for thinking that more self-harm is not really possible. Unfortunately, for the majority of us, the reality is quite different.

How It Happens

To breach any system, humans are often the weakest link as far as security is involved. Being emotional creatures given to likes and dislikes, daily mood swings and tastes and biases that can be exploited easily, they are typically the first line of attack. A single lapse in security protocol due to lack of knowledge or training and failure to follow simple safety instructions can lead to errors that can cost the individual and organization dearly.

The typical compromise begins with a number of logical steps that are easily documented.

- **Identification:** The first step is to identify the “value” target. This will be the person who is part of an organization and may have sufficient system access and permissions to make their identity worth hijacking or compromising. An example may be a newly hired IT Technician or Desktop Support person.

- **Preparation:** Once the hacker has identified a "value" target the next step is really the initial reconnaissance phase (information gathering) where the target is staked out and the would-be hacker rifles through the target’s digital footprint across several social media posts or group forums looking for an entry point or weakness. A careless project detail disclosed, a co-worker’s bridge game booking or a corporate initiative important enough to elicit a response when framed correctly are all red flags ready for exploitation by the aspiring hacker. Club affiliations, weekly jogging partners, the immediate boss, senior co-worker or an upcoming work anniversary are all valuable data points that the hacker can gain traction from in future interactions online with the target. The idea is always to harvest enough information to be able to manipulate the target at a later date.

- **Infiltration:** The initial contact may happen through an innocent enough "friend request" or "like" and this may act as an important staging ground for opening a future conversation. The "value target" may not even be the primary target in many cases. He or she may simply be a low-level employee active on Twitter or Facebook or elsewhere but is easy enough to convince to download software wrapped as an update or critical patch. Hackers always hope that trawling your connections list will provide a treasure trove of additional valuable information on other higher ups within the organization who may have the necessary admin permissions to conduct their work.

- **Exploitation:** With up to 300 billion emails being sent per day, the next step is typically a targeted “spear phishing” phase by email to hook the “value” target in order to elicit a response with some confidential information (such as credentials) or to quietly deliver a payload disguised as an attachment or link that is primed for a known vulnerability on your corporate systems. The sender address is often spoofed to resemble a trusted organization (bank, school, fitness club) or one of the trusted contacts in your social network. Alternatively, the recipient may be urgently directed via a link (typically a shortened URL) to a malicious website that has been readied ahead of time, on a single visit to drop the offending malware onto the visitor’s system. This is where corporate employee awareness programs (that really should be mandated everywhere) are worth their weight in gold in order to educate staff and prevent such future foreseeable breaches.

☑ **Execution:** Once systems have been breached “the rest is history” as they say and you can search the web for more complete information on all the different companies who have been compromised on account of a careless employee or two and their data scrambled or scrubbed or exfiltrated to another external site.

Basic Dos and Don'ts

Here are a few guidelines for anyone planning to share information through their social media accounts posts or to group forums, etc.

1. In the old Yellow Pages ads, your fingers did the walking but now they are doing the talking and all too much of it. Always remember your record online is permanent once your fingers leave the keyboard. Data you provide, innocently or inadvertently, is set in stone and may never really be erased - ONLY marked for deletion in the future. This pseudo deletion simply "hides" the data from the current view.

2. Be wary of sharing your travel plans ahead of time with the world on social media. It's nice to read you're having a fun time on your desert island holiday or company retreat but never give exact dates or times for when you plan to travel or be out of town for extended periods. It's just like handing your house keys to total strangers.

3. Every comment you make, every selfie you fake, every "like" you take - the machines will be watching you. Be careful in your words and diplomatic in your approach. As taught at school, look both ways before crossing the digital divide to commit your words to immortality. These can come back to hurt you later. Better to practice self-discipline now than have regrets later.

4. Never disclose personal identifiable information as defined by the GDPR (General Data Protection Regulation) in any of your posts. This would include your Social Security Number, date of birth, address, bank account details, driver’s license, medical records or any other especially identifiable datum that points straight back to you and makes triangulation easier for the hackers. Identity fraud remains a rampant scourge online and is unknowingly facilitated by users themselves exposing critical information on their social media posts.

5. Avoid unnecessary unknown “friend” and “connections” requests from otherwise total strangers. This may seem hard initially when you are trying to grow your network but resisting the urge is possible although a little painful. The larger the surface area exposed of your online profile and interactions the more potential damage could be done later by hackers.

6. Shop ‘til you drop may be a mantra of the consumption society but don't post until you roast! Keep conversations cordial, brief and well-mannered always. It's all too easy to find yourself venting and ranting in front of total strangers. All conversations have a half-life of forever online so be careful with not disclosing too much of yourself or what triggers you, or those looking for your hot buttons will come looking for you. Additionally, recruiters and your bosses may be alerted to your posts so there can be a danger of job-related consequences to follow.

Conclusion

All is not lost though, and I hope I haven't rained on your social parade.

Take a few moments occasionally to understand what you are trying to get out of all the social media platforms you have joined. It really is a two-way street both giving and taking. It may be that you are already over reaching and over posting and stretched out too thin to make any reasonable conversation or impact. Now may be a good time to take stock and close out unnecessary accounts and maintain only a few very essential ones.

References:

- Wikipedia: https://en.wikipedia.org/wiki/Social_engineering