An innovative and comprehensive framework for Social Driven Vulnerability Assessment

20 November 2014
Who are we?

**Enrico Frumento**
(twitter: enricoff)
ICT Security Specialist @ CEFRIEL
Main Activities: unconventional security, phreak, tweak, psychohistorian, ...

**Roberto Puricelli**
(twitter: robywankenoby)
ICT Security Consultant @ CEFRIEL
Main Activities: Social-driven Vulnerability Assessment, Security research, passionate of technology...
Who is CEFRIEL?

Bridging the gap between industries and academia to BOOST INNOVATION

CEFRIEL Unique Value Proposition

Industrial companies

CEFRIEL

Academic universities

RESEARCH INNOVATION MARKET
What will you get?

What is SE today?

How companies react?

How vulnerable are?

Real numbers

...a lot of phun, but no beers
What’s cybercrime today?

From geek-driven to business-driven.
What’s cybercrime today?

Selling is selling!
What do you need to sell cybercriminals products?
Who’s the customer?

“The golden rule for every business man is this: put yourself in your customer’s place.”

— Orison Swett Marden
What’s cybercrime today?

**BOTH** tries to enter, tweaking the person at the door..

**Door-2-door seller**

==

**Modern cybercriminal-seller**
What’s cybersecurity today?

YES A TOTALLY DIFFERENT APPROACH, USING THE SAME TECHNIQUES OF MARKETING...

Viral,

Guerrilla,

Unconventional,

... And of course Social engineering 2.0

So what? Anything new??
What’s cybercrime today?

“ADVERTISING”

ADVERTISING

... DEVELOPERS
SOCIOLOGIST
HCI EXPERTS

PSYCHOLOGIST
SELLERS
MARKETING EXPERTS
SN INFLUENCERS
What is the security team?

Our team includes several competences

- malware expert
- web designer
- web developer
- psychologist
- expert of HCI interaction
- marketing expert
- SN influencer
- legal advisor
SOCIAL ENGINEERING 2.0
The Role of the Human Factor in Hacker Attacks
Characteristics of SE 2.0

- Malware Ecosystem 2.0
- Automatic Social Engineering Attacks (ASE)
- (ab)use of linked-data
- Chat-bot
- (ab)use of psychology, personality profiling systems and cognitive science models
- Mail attack vector
- Economic Drivers
SE became an important part of the malware 2.0 and the main infection strategy
Automation of SE attacks through information collection and mining and through the **sentiment analysis** from Social Networks.
The public bodies and anyone are moving toward the free circulation of data, to the web 3.0. This is the **Linked-Open-Data** or web-of-data. **(ab)using LOD** will facilitate the collection of data to fully contextualize attacks to targets.
**Diffused use of chat-bot**, as in **ASE** attacks to start and maintain conversations with other social networks users and to balance the lack of a real social engineer (mass social engineering attacks)
Professional use of **memetics** and **personality models** of the attacked users, especially of models coming from theories of **cognitive psychology**
Massive use of mails - if compared to other attack vectors - since it doesn’t need talented hackers and it can reach lot of victims at a time (i.e. new forms of spam)
SE 2.0 is since the beginning an investment (no ways doing it for phun), all attacks have one common aim: **making money.**
Characteristics of SE 2.0

USE

vs

ABUSE
(ab)use of psychology and models of cognitive science

Professional use of memetics and personality models of the attacked users, especially of models coming from theories of cognitive psychology

(ab)use of Social Networks

Social Networks are fantastic sources of information about victims, tastes, personalities, profiles, etc. The phase of information collection about the target in a crucial step for each attack.
The first example... RSA

THE case study...

You probably know this email
.. the latest one: Darkhotel attacks

The Darkhotel threat actor compromises selected luxury hotels

After check-in, the executive tries to connect to Wi-Fi

The attackers offer an update for legitimate software:

Now the attackers can use a set of tools to collect data, hunt for cached passwords

and steal login credentials

A high-level business traveller stays in the compromised hotel

The hotel requires the guest's surname and room number at login

The 'welcome packages' are installers for a backdoor

Warning! Trade secrets could be stolen!

What’s in common?

- More than 7 years
- Target business executives
- Drive-by download attack
- Steal data and collect passwords

Social Engineering at the beginning
Problem: It’s not anymore so advanced. “Advanced” only means that the attackers have a (devilish) business plan.
An APT often begins with a Social Engineering attack

• Email is the most used attack vector

• How to build an effective attack?
Spear phishing is the new evil
• A contextualized email is more effective

- How to gather information?
Internet and Social Network allow to retrieve lots of information

- Public information are already available
- Also “active” attacks

OSINT  Target selection  SE attack

- What’s the result?
Advanced Persistent Threat Model

Technological attack can create a backdoor inside the company
• Known vulnerabilities or zero-day attacks

- OSINT
- Target selection
- SE attack
- Ad-hoc tech attack

• What’s next?
Advanced Persistent Threat Model

Inside the network, lateral movement
Difficult to detect slow and punctual attacks

OSINT
Target selection
SE attack
Ad-hoc tech attack
Attack expansion
Advanced Persistent Threat Model

How can we measure that risk?
OUR FRAMEWORK

- Ubiquitous processing
- Peace of mind
- Emotion and context-awareness applications
- Human sensor networks
- Motivation
- Empathy
Our Framework

OSINT
Target selection
SE attack
Ad-hoc tech attack
Attack expansion
Data exfiltration
Our Framework

Passive social information mining

Spear phishing attack simulation

Technological attack simulation

OSINT
Target selection
SE attack
Ad-hoc tech attack
Attack expansion
Data exfiltration
Our Framework

- Setup
- Passive social information mining
- Spear phishing attack simulation
- Technological attack simulation
- Awareness
Since the activities is innovative stakeholders need to:
• share objectives
• define the boundaries

Prior to start the assessment, it is necessary to provide a startup phase
People are the target of the assessment

• A potential attacker has no constraints
• Direct contact with the target (active)
• Don’t care about consequences
• During an assessment need to take care about the users

Ethics vs legal perspective

Only passive scanning
Public sources
Anonymous results
The purpose is to find some evidence regarding the **feasibility of the social engineering attack**

Focus on the company, not on the user

Even if the source are public, lot of information retrieved...

..and it’s just the tip of the iceberg
WEAPONS OF
MASS DISTRACTION
emails of employees possibly attacked

initiatives related to company or employees

templates for building effective attack
evidence related to specific risks
The purpose is to **test the user behavior** when stimulated with social engineering attack.

It begins with emails sent to employees. Target is a sample of employees.

We evaluate two different types of risks:

1. **The user click on the email**
   - Expose to drive by-infection

2. **The user also provides the requested credentials**
   - Lose of a critical company asset
Type of phishing: A SDVA Example

An example of email for a SDVA test
Type of phishing – Example of a website

An example of the related phishing website

Company asset requested (credential)

Both email and website contains clues that allow to identify the risk

Refers to the phishing campaign

70% DISCOUNT

ACME corpora...al to obtain the discounts
Collected information

The assessment track user behaviors
• Anonymity vs result analysis
People often have potentially dangerous behaviors.

Most part of Workstation analyzed include obsolete or unpatched software.
The aim is to **demonstrate the possibility to compromise the company laptop**, knowing its configuration.

Usually through a proof-of-Concept:

- Analyze software configuration
- Correlate with vulnerabilities
- Create a custom exploit payload
IT’S POSSIBLE TO FIND A WAY TO COMPROMISE A WORKSTATION INSIDE THE COMPANY
The assessment should help to *raise awareness inside the company against these threats*

People is the weak point

- Management need to be aware
- Employees need to know

Training and awareness is the only (nowadays) effective countermeasure

..but need to be properly done.
Video
Raise awareness through visual information

Pills
describe correct behaviour

Gamification
Stimulate users to enhance learning
Our experience

In the last five years we performed about **15 SDVA** in big enterprises with thousands of employees, involving about **12000 users**

Given an example of a possible test email

In your opinion, what are the results?
Overall results

- Employees receive the email: 100%
- 34% visit the website
- 21% also insert the credentials
Benchmarking

Credential insertion (% of sample)

Click on email link (% of sample)
Benchmarking

Click on email link
(% of sample)

Credential insertion
(% of sample)

34% 21%

3 emails to obtain one click
5 emails to obtain a valid credential
58% conversion rate click/insertion
Comparison with other studies

- **34%** Average click rate in our research
- **10%** Average click rate in modern phishing
- **2%** Average click rate in Marketing
- **0.01%** Average success in “traditional” phishing

Source: www.proofpoint.com
We measure relative effectiveness per campaign.
User reactions

I inserted the credential, but I don’t receive a confirm

I inserted the credential, but I think it’s phishing and I change the password

This is definitely phishing. Please do something!
User reactions

- 1% of employees signal the phishing
- 6 minutes fastest email to antiphishing
- 20 minutes record on block website

"This is definitely phishing. Please do something!"
We measure relative effectiveness per campaign.

Time analysis - Visits

Success ratio (% of overall success)

Time (minutes)

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

0 10 20 30 40

20 min

Already 50% success before block website

32% Success before first report email

6 min
User characterization

**Age**
- <30 years: 26%
- 30-40 years: 22%
- 40-50 years: 19%
- >50 years: 17%

Younger employees are more exposed
Habits of new generation?

**Role**
- Employee: 23%
- Middle-level: 20%
- Management: 18%

Also managers are vulnerable
Risk is (not enough) lower

**Awareness**
- Awareness: 19%
- No Awareness: 24%

Targeted training mitigate the risk
Behaviour is impacted by awareness
CONCLUSIONS
PEOPLE DON’T KNOW THAT SHARING INFORMATION on social media can BE DANGEROUS...
Companies are exposed to Social-Driven risks and often there is no perception of how extended the risk is.

A social engineering attack with a contextualized hook can be effective.
Lots of employees could become a risk for the enterprise just for a discount on a sandwich .. or a slice of cake.
PERFORMING APT ATTACKS IS BECOMING EXTREMELY SIMPLE, IT MAINLY MEANS HAVING A BUSINESS (DEVILISH) PLAN.

**PS:** no chick was harmed during the preparation of these slides.
THAT’S ALL FOLKS ...