The Last Call

HoneyCON21

Nacho Brihuega Rodríguez a.k.a n4xh4ck5

ÍNDICE

- Whoami
- Motivation
- Vishing campagins
- References

ÍNDICE

- Whoami
- Motivation
- Vishing campagins
- References

Whoami: Nacho Brihuega

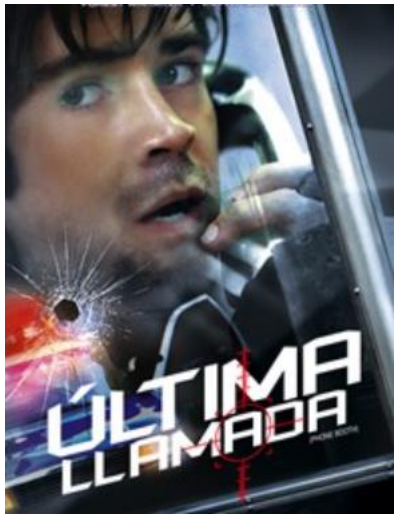
- Red Team in Siemens.
- Trainer in cybersecurity degrees in UCAM and UCLM.
- Co-author in blog “Follow the White Rabbit”.
- OSCP, CRTP, CRTO, CRT&CPSA (CREST).
- @n4xh4ck5

INDEX

- Whoami
- Motivation
- Vishing campagins
- References

MOTIVATION

- Hello, this is Microsoft support and I am calling you….
- Vishing campaigns have increased a lot in the last time.
- The human is the weakest link of security chain.
- Vishing is a technical very common in social engineering campaigns and Red Team engagements.



ÍNDICE

- Whoami
- Motivation
- Vishing campagins
- References

ASPECTS TO CONSIDER

- Why have cybercriminals just carried on performing social engineering campaigns? It Works!
- Unlike phishing or smshing, vishing involves a real person and involves the personal side. In this way, the social engineering principles:
  - Trust. Our few defenses are lowered when we like our interlocutor is aligned with our interests.
  - Reciprocity. If someone offers us something, we tend to offer them something ourselves.
  - A person's first step is to help another person.
  - We feel uncomfortable saying NO.

Vishing Campaign - Types

- Two possible approaches:
  - Vishing such as awareness campaign (Agreement with customer).
  - Vishing such as part of RECON Red Team engagement (free).

Vishing Campaign – Step to step - Definition

- Define the goals of the campaign and short hints. These goals may be focused on:
  - Make the employee does something: click in link, visit website, send email,…
  - Make the employee interacts with the computer: execute commands, disable something,…
  - Make the employee answers questions: Have you got AV in your computer? Could you do remote work?

Vishing Campaign – Step to step – OSINT

- Perform OSINT about the company target in order to disvover:
  - Business activity (energies, telco, fuels, food, …)
  - Affiliated companies (Recently companies adquired and subsites)
  - Main vendors
  - Geolocation headquarters.
  - Try to identify the cybersecurity awareness (blogs, conferences, newsletters,…)
  - Domain/subdomain Discovery in order to find internal websites on focus to employees.

Vishing Campaign – Step to step – Use scenarios

- It recommends to create al least two use scenarios in order to balance between in function campaign progress.
- Two candidates to make the calls. It is desirable that they are of both genders. In this way, it reduces the detection options. There are studies which demonstrate people are more receptive when the caller is of opposite gender.
- It recommends the scenarios are different and as well different intrusive level in order to balance in function sensible identified in employees.

Vishing Campaign – Step to step – Scenarios

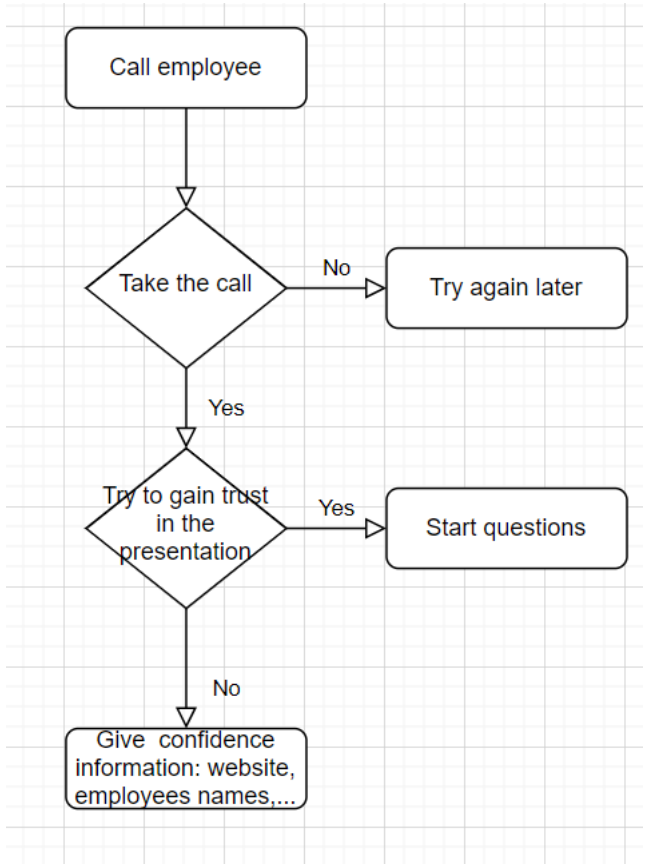
- Scenario 1: The company <TARGET> suffers many phishing campaings and they think some employees have been to download documents attached with dangerous macros. In this way, the company has contracted an external security company to check the awareness of its staff.
- Scenario 2: The company <TARGET> have to pass a regulation certification (ISO, GDPR,…). The company has contracted a external company to check if the employees computers have passed the security requirements.

Vishing Campaign – Step to step – Scenarios

- As attacker:
  - Create company's name credible. It recommends to register a domain and develop a website (2-3 weeks previously in order to be indexed).
  - Prepare an introduction to explain *whoareyou* and the reasons of the call.
  - Prepare the questions where you wish to ask.
  - Use a device which let to change ID call.

Vishing Campaign – Step to step – Scenario

- It recommends using a flow chart to represent the steps of the call in terms of the employe's responses.



Vishing Campaign – Step to step – Scenario- Infraestructure

- Call device:
  - Anonymous:
    - Phone call: Bookmark #31#
    - Skype (60 min free). Disadvantage: untrust.
  - Buy a SIM card to the target country. Disadvantage: It may be reported.
  - App:
    - Fake call: https://play.google.com/store/apps/details?id=com.blogspot.novalabsandroid.fakecallerid&hl=es&gl=US . Not record voice
    - Spoofcard ($): https://www.spoofcard.com/- Let to record voice. In addition, customize your voice to sound like a man or a woman and adding background sounds.

Vishing Campaign – Step to step – Scenario- Infraestructure

- Call device:
  - Websites:
    - https://myphonerobot.com/
    - https://www.spoofmyphone.com/free
    - https://www.spoofbox.com/en/app/spoof-call
    - https://www.covertcalling.com/freecall/
    - http://www.crazycall.net/
    - https://www.bluffmycall.com/
    - https://www.firertc.com/

Vishing Campaign – Step to step – Scenario – Search targets

- Prioritize departments most likely to receive calls: sales, marketing, community manager,… **NEVER** RRHH (they may know everybody).
  - Goals to discover in the searching targets:
    - How much time do they work in the company? Are they external o internal employees? Interns?
    - Tecnologies skills
    - Age
    - Remote work 100%?

Vishing Campaign – Step to step – Scenario – Search targets

- Search employees:
  - Linkedin. People love exposing a lot information (technologies used,…)
  - Find usernames, emails, metadata?
  - Tools/service online:
    - https://github.com/gojhonny/InSpy
    - https://github.com/m4ll0k/Infoga
    - https://hunter.io/
    - https://tools.epieos.com/email.php
    - https://www.emailsherlock.com/
    - https://github.com/alpkeskin/mosint
    - https://github.com/laramies/theHarvester

Vishing Campaign – Step to step – Scenario – Questions

- **Friendly questions:**
  - Are your surnames *smith*?
  - Do you work in the "*legal*" departament?
  - Is your mail XXXXX@company.com? (obtained in the OSINT phase)
- **Easy questions:**
  - How long have you worked in this company?
  - Could you be able to do remote work?
    - How many days could you do remote work?
    - How many days could you go to the headquarters?
  - Have you ever received cybersecurity training?
  - Have you got a corporate mobile phone?
  - Have you got a laptop?

Vishing Campaign – Step to step – Scenario – Questions

- **Technologies questions**:
  - What operative system do you use?
  - What program do you use to open PDF documents?
  - What AV is installed on your computer? which version?
  - How do you connect to corporate tools when you do remote work? Do you use a VPN? What VPN client do you use?
  - How you share documents with your co-workers or customer? Do you use sites such as dropbox or wetransfer?
  - How often do you have to change your password?
  - Do you use a password manager such as keepass?
  - What browser do you use? Which version?
  - Please could you access this URL? Fake URL

Vishing Campaign – Step to step – Scenario – Questions

- **Technologies questions**:
  - How is the password policy? Could you give a password example?
  - Mobile phone
    - What operate system have your mobile phone?
    - How do you download app? Playstore?
    - Which telephone operator do you have?
  - Could you install and use desktop applications such as WhatsApp o Telegram web?
  - Could you explain the VPN connection process? Do you use 2FA?
  - Could you type hostname in your cmd? Explain the process to open cmd.
  - What type of card do you use to access the company? (RFID, HID, none)

Vishing Campaign – Step to step – Last details

- How many employees do you call? 15-20 (max)
- How long should it take? 1-2 days
- What could I do if I was detected? Turn off
- When should it do the calls? At the end of week.

ÍNDICE

REFERENCES:

- https://www.pabloyglesias.com/mundohacker-ingenieria-social/
- https://www.osi.es/es/actualidad/blog/2020/10/14/vishing-la-llamada-del-fraude
- https://www.youtube.com/watch?v=a6oEG1zFPsE
- http://www.euskalhack.org/securitycongress2019/SECTF/EuskalHack_SECTF_2019.pdf
- https://fwhibbit.es/osint-parte-i-todo-lo-que-sabe-google-de-nosotros
- https://fwhibbit.es/reconocimiento-pasivo-en-un-phishing
- https://www.flu-project.com/2021/05/obteniendo-informacion-de-direcciones.html

QUESTIONS?