



Современные атаки социальной инженерии

Александр Павлов

Специалист отдела анализа защищенности,
Информзащита

кибербезопасность
в эпоху перемен

Социальная инженерия — вечная угроза

кибербезопасность
в эпоху перемен

Современные атаки социальной инженерии

Социальная инженерия

— это процесс манипулирования людьми для получения какой-либо конфиденциальной информации или совершения определенных действий

30% - эксплуатация уязвимостей

10% - Ddos атаки **5%** - инсайдерские угрозы и ...

кибербезопасность
в эпоху перемен

б3
информзащита

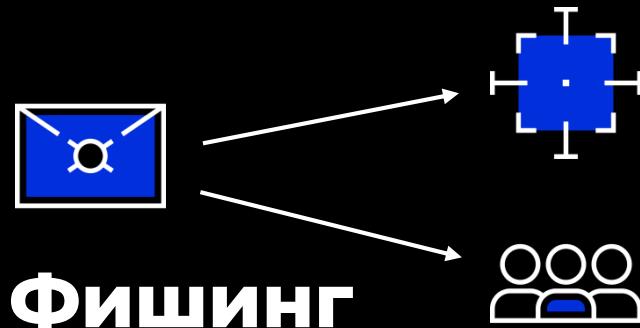


Основные направления социальной инженерии

кибербезопасность
в эпоху перемен

Основные направления

кибербезопасность
в эпоху перемен



Также в контексте проведения социотехнического тестирования на проникновение, мы как красная команда комбинируем фишинг и вишиング, так как подобный формат дает больший импакт в ходе тестирования.

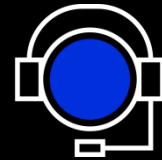
Основные направления

кибербезопасность
в эпоху перемен

Б3
информзащита

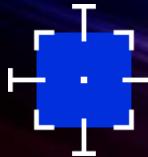


+



Фишинг

Вишинг



В таком формате мы можем заранее обзвонить конкретного человека и выслать ему письмо, либо же наоборот, зависит от контекста проведения атаки.

Основные направления

кибербезопасность
в эпоху перемен



FakeBoss



Whatsapp

Telegram

Viber

При проведении ВЕС-атак исполнители играют роль начальника, руководителя направления и т. д., чтобы заставить подчиненного выполнить какое-то действие. Для правдоподобности используем функциональности того или иного мессенджера, будь то кружок, аудио-сообщения или текст.

DeepFake – настоящее и будущее социальной инженерии

кибербезопасность
в эпоху перемен

Что такое DeepFake

это методика синтеза контента, основанная на машинном обучении и искусственном интеллекте



Полезный
цифровой двойник



Вредный
цифровой двойник

Современные атаки социальной инженерии



Как создается DeepFake

кибербезопасность
в эпоху перемен



01

Сбор
данных

02

Обучение
нейронной
сети

03

Генерация
DeepFake

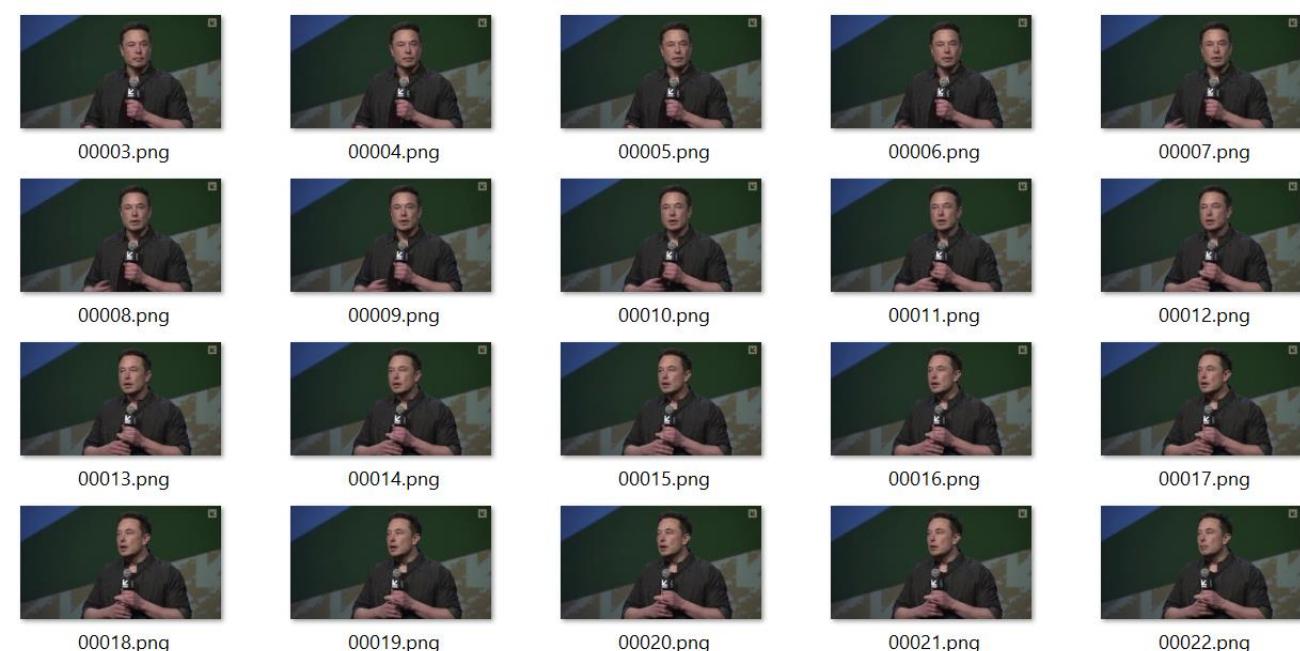
04

Пост-
обработка

05

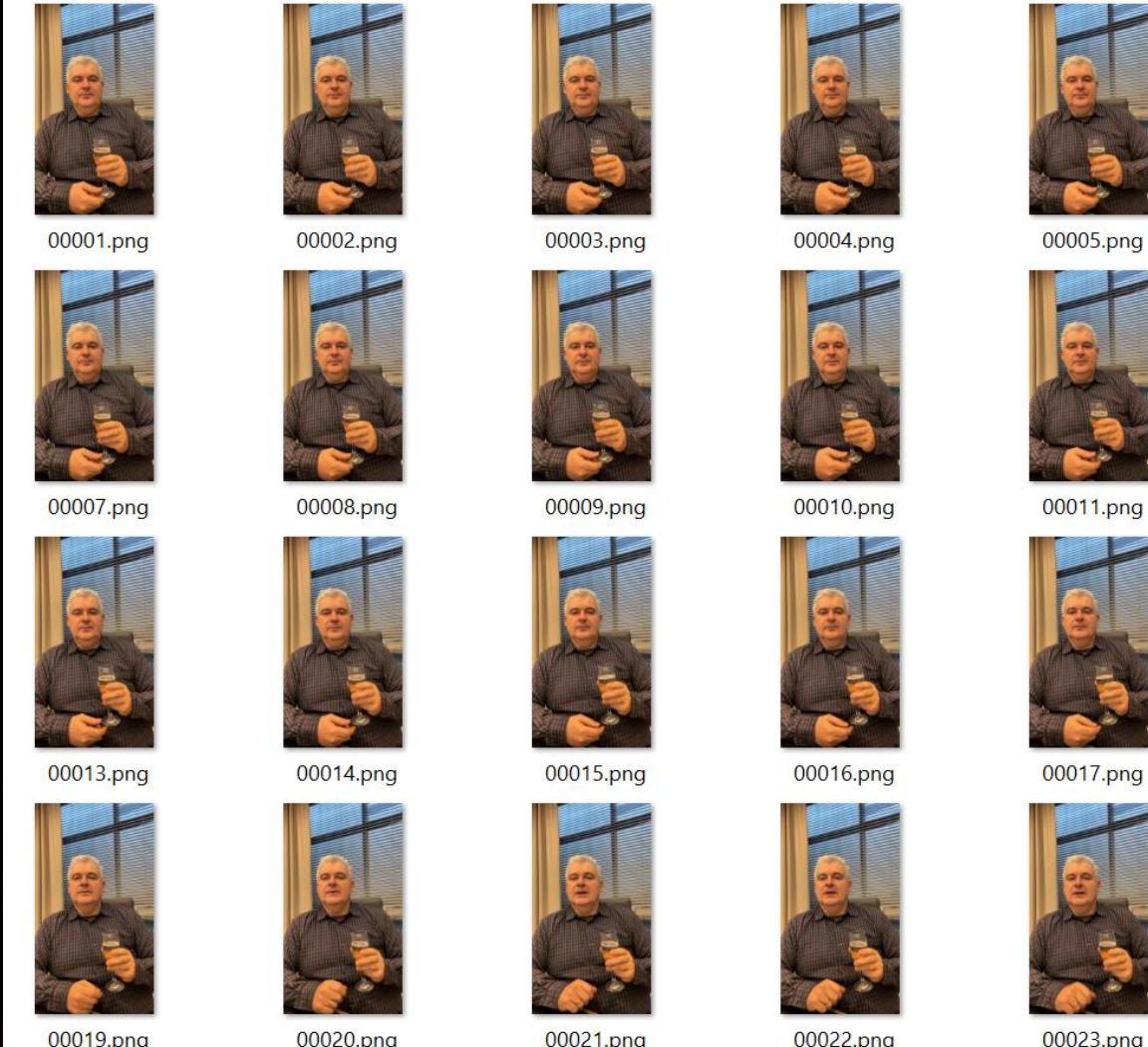
**Deep
Fake**

Сбор данных



destination

Современные атаки социальной инженерии



source

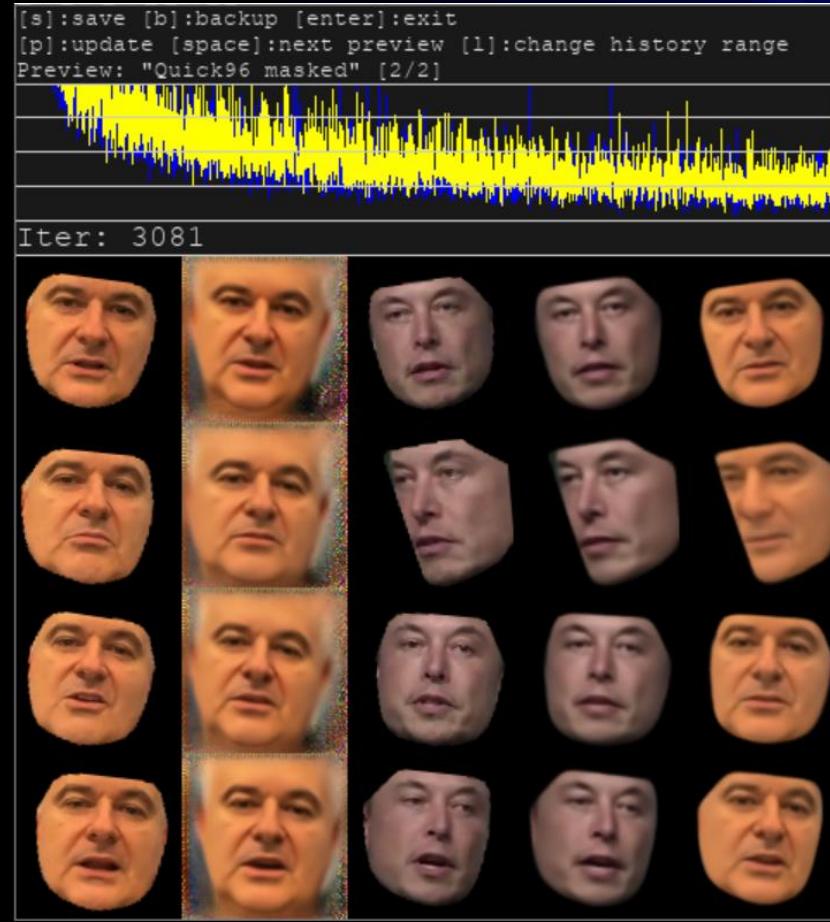
Обучение нейронной сети

кибербезопасность
в эпоху перемен

Б3
информзащита



head



mask

Генерация DeepFake

кибербезопасность
в эпоху перемен



Постобработка

кибербезопасность
в эпоху перемен

Б3
информзащита

```
erode_mask_modifier: 0
blur_mask_modifier: 100
motion_blur_power: 65
output_face_scale: 0
color_transfer_mode: rct
sharpen_mode : None
blursharpen_amount : 0
super_resolution_power: 100
image_denoise_power: 0
bicubic_degrade_power: 0
color_degrade_power: 0
=====
Merging: 20%|#####
MergerConfig 00331.png:
Mode: overlay
mask_mode: learned-prd*learned-dst
erode_mask_modifier: 0
blur_mask_modifier: 100
motion_blur_power: 65
output_face_scale: 0
color_transfer_mode: rct
sharpen_mode : None
blursharpen_amount : 0
super_resolution_power: 100
image_denoise_power: 0
bicubic_degrade_power: 0
color_degrade_power: 0
```



DeepFake

кибербезопасность
в эпоху перемен

б3
информзащита





t.me/imnoturbadboy
tgc - traceback

Современные атаки социальной инженерии

Александр Павлов

Специалист отдела анализа защищенности,
Информзащита

кибербезопасность
в эпоху перемен