Tinkoff craft Anti-Phishing

Zherelin Pavel

InfraSec Team leader

2022

How we made our Tinkoff Anti-Phishing

- What do we mean by Anti-Phishing?
- Why is it necessary?
- Why did we decide to make our own Anti-Phishing solution?
- What problems we faced?
- What's next?

What do we mean by Anti-Phishing?

- We simulate phishing attacks on **employees**
- We train employees how not to fall for anti-phishing next time
- We take special measures if an employee cannot be trained

Is it necessary? After all, we have SOC!

- Any automatic means (mail filtering, blacklists, attachment analysis, etc.) can be bypassed
- Phishing can be very targeted and almost invisible
- You can make very tight technical restrictions, but it will be difficult for people to do their job

There are commercial solutions on the market!

OFF ONE 2022

PROS

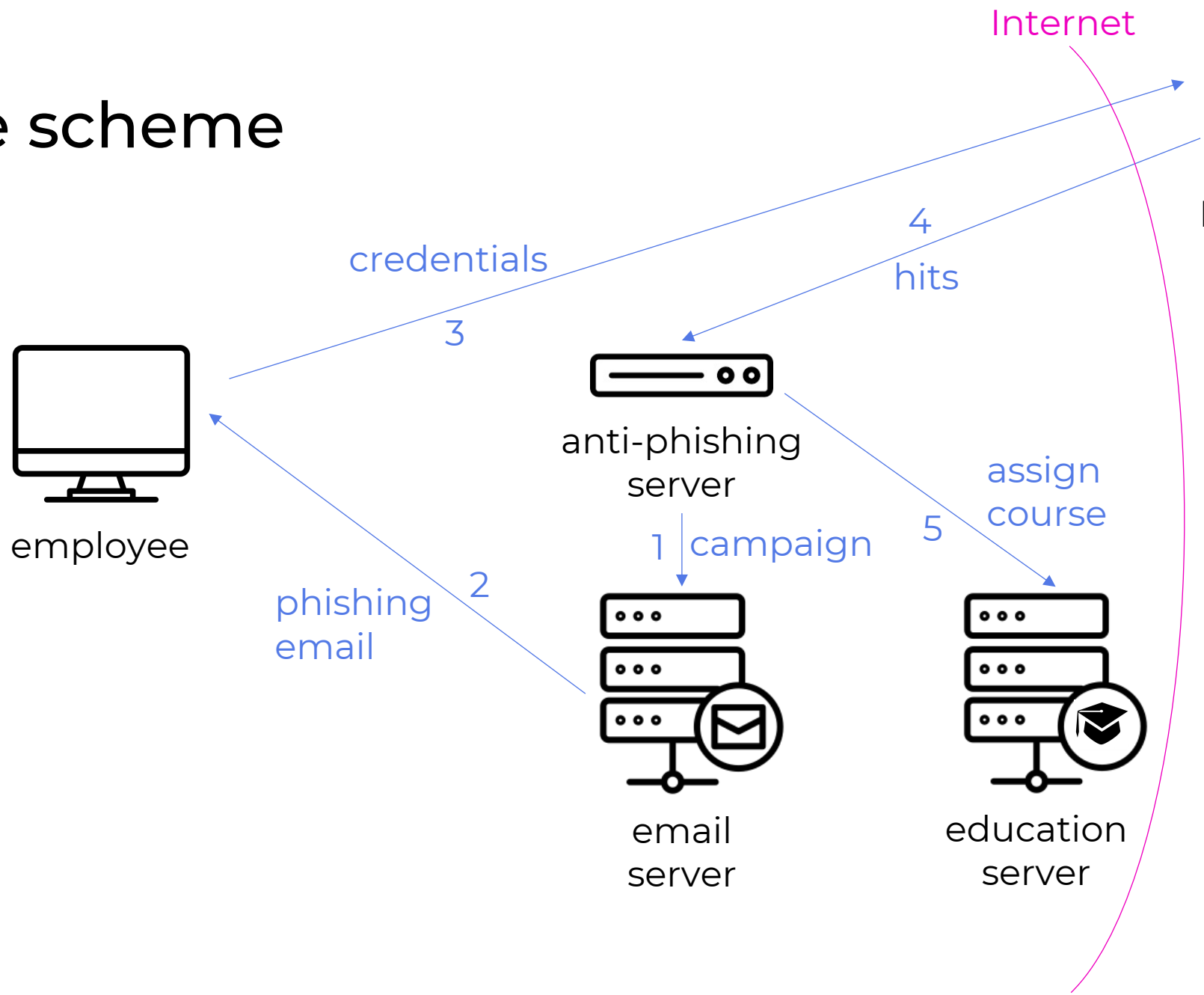
- No need to spend resources on development
- Can get started quickly
- You can use ready-made templates, rather than invent
- Contain sophisticated attacks with advanced "phishing" sites

There are commercial solutions on the market!

CONS

- Licensed by employees, expensive for large organizations
- You need to export data to a third-party system (often to the cloud)
- Emphasis on increasing the effectiveness of the attacks, and not on subsequent work with people
- Difficult to integrate with already implemented systems (for example, with corporate educational portals)

The scheme


Internet
WWW
phishing website
credentials
3
4
hits
employee
anti-phishing server
1
campaign
assign course
5
phishing email
2
email server
education server

Email

From: Контроль рабочего времени <skrv@[redacted]>
Sent: Wednesday, July 8, 2020 11:19 PM
To: [redacted]
Subject: [ВАЖНО] Контроль начала рабочего дня и общего времени работы на удаленке

Уважаемые коллеги!

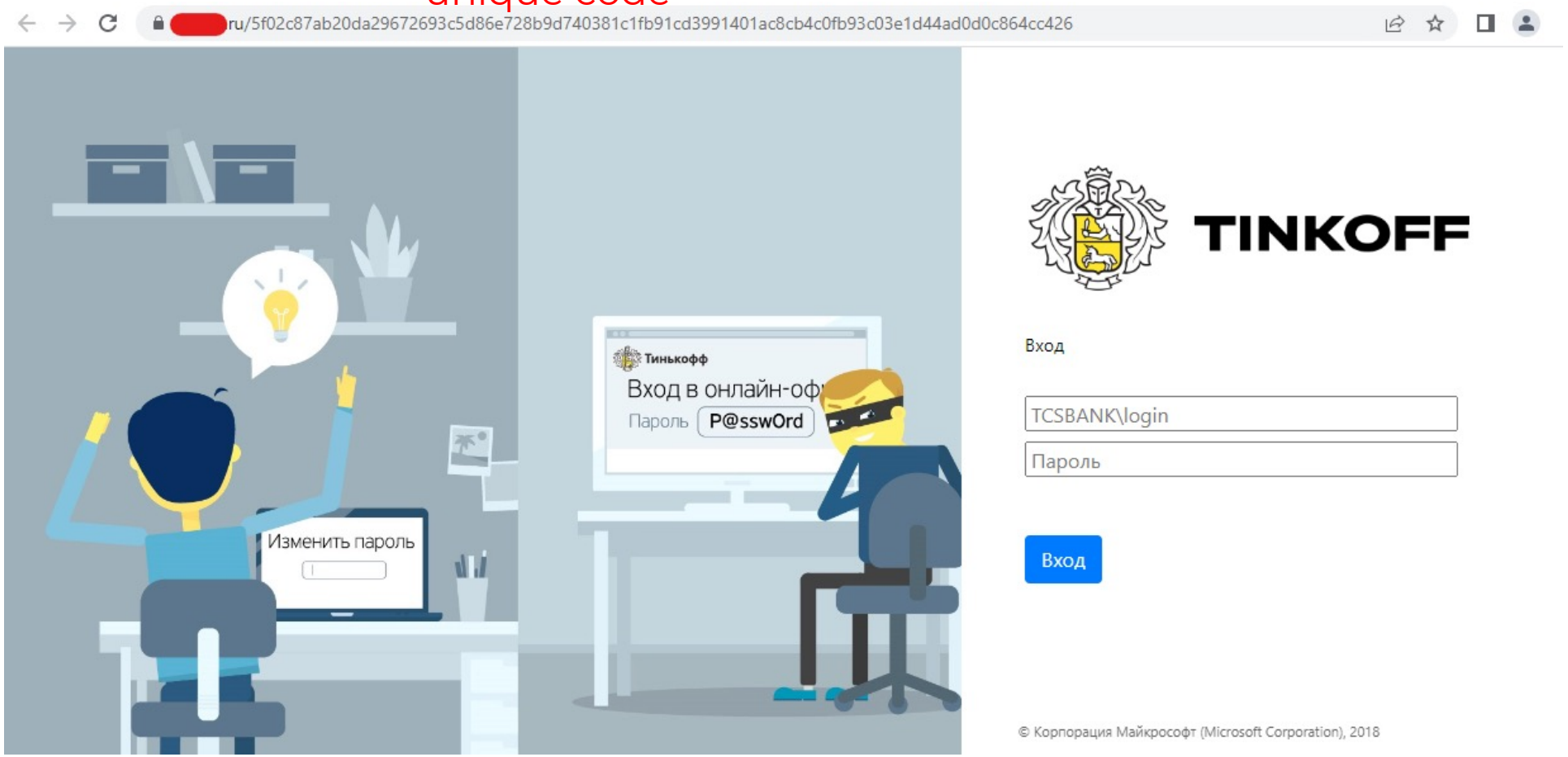
Несмотря на то, что большая часть компании работает сейчас на удаленке, режим работы продолжает регулироваться трудовым договором. Он определяет требования к началу концу рабочего дня, а также к количеству отработанных часов в день.
Когда мы работали в офисе, эти данные брались из СКУД, сейчас аналогичные данные собираются из логов VPN. Вот почему крайне важно начинать рабочий день (т.е. подключаться к VPN) не позже времени обозначенного в трудовом договоре.
Уточнить или изменить время начало трудового дня, а также посмотреть персональный отчет о количестве отработанных часов за последние три недели можно в Личном кабинете. **Проверьте свои показатели!**
Обращаем внимание, что к сотрудникам систематически не выполняющим нормы по отработке времени (отмечено красным в отчете) могут быть применены меры дисциплинарного воздействия вплоть до увольнения.

С уважением,
Илья Крапивин

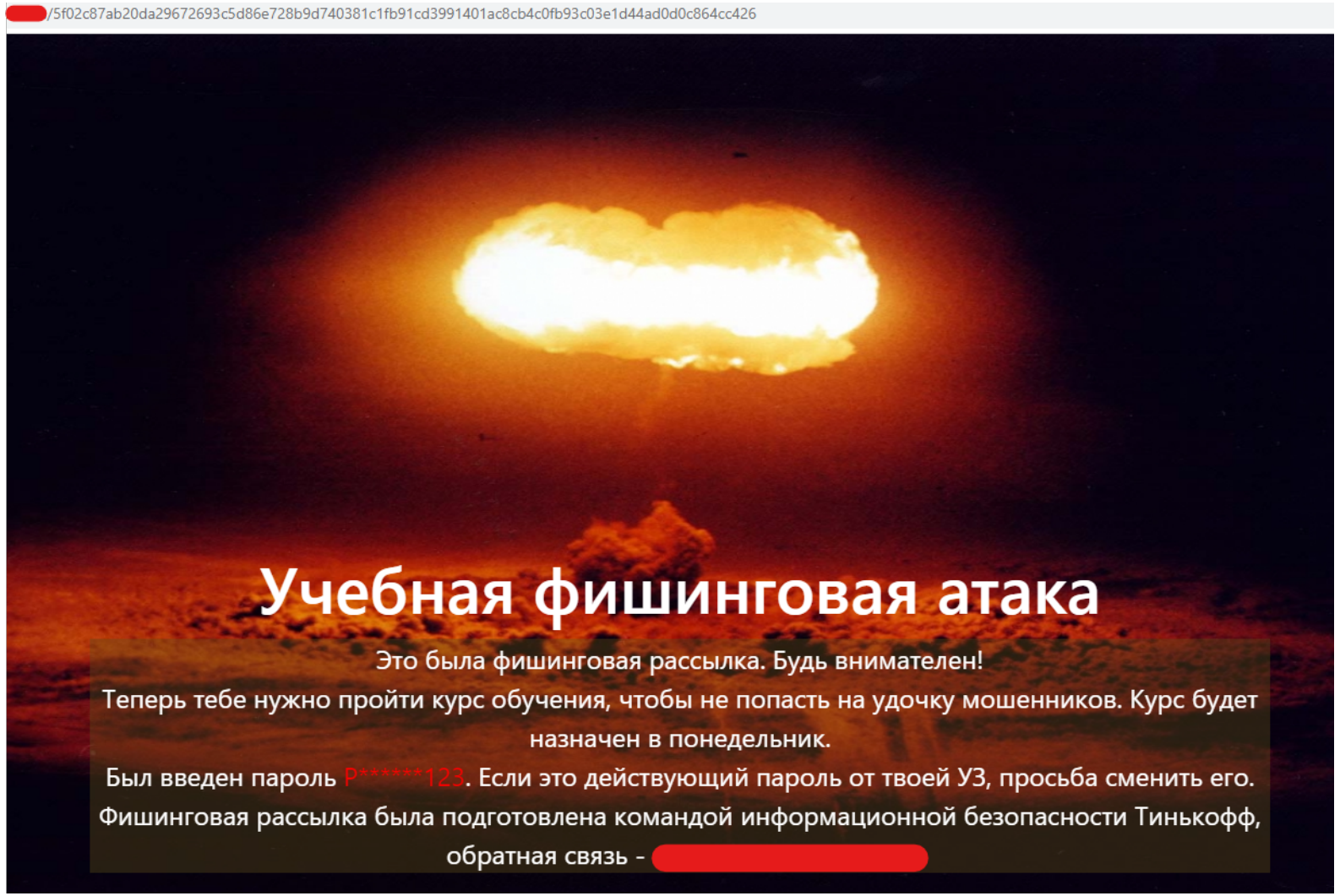
Руководитель службы контроля рабочего времени
Тел.: +7 (495) 648 1000 (вн. [redacted])
www.tinkoff.ru

Website on a domain with a typo

unique code



Boom!


[redacted]/5f02c87ab20da29672693c5d86e728b9d740381c1fb91cd3991401ac8cb4c0fb93c03e1d44ad0d0c864cc426
Учебная фишинговая атака
Это была фишинговая рассылка. Будь внимателен!
Теперь тебе нужно пройти курс обучения, чтобы не попасть на удочку мошенников. Курс будет назначен в понедельник.
Был введен пароль P******123. Если это действующий пароль от твоей УЗ, просьба сменить его.
Фишинговая рассылка была подготовлена командой информационной безопасности Тинькофф, обратная связь - [redacted]

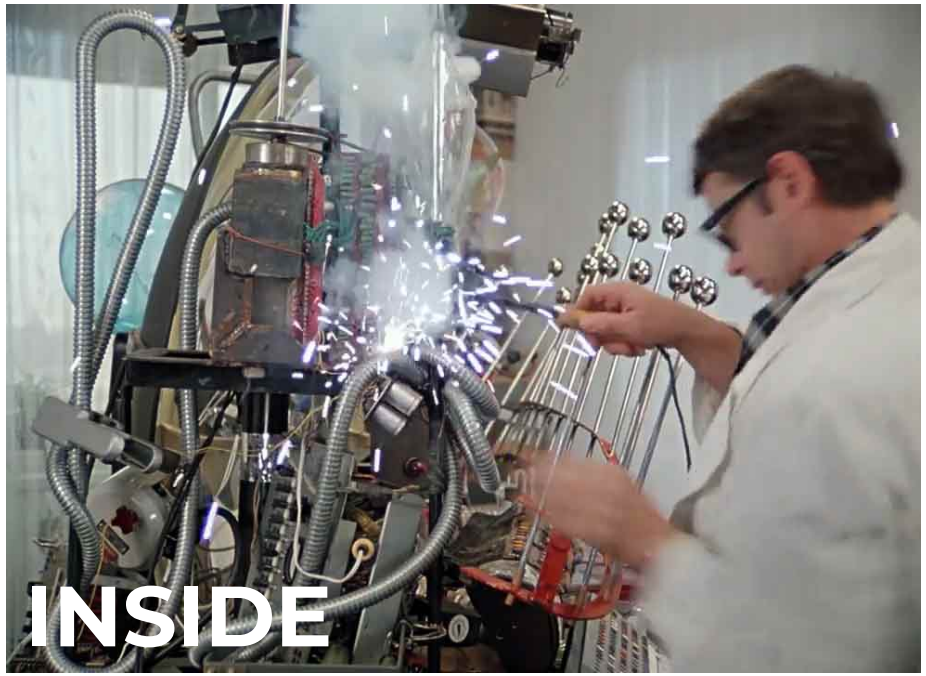
What's inside?

Hosting

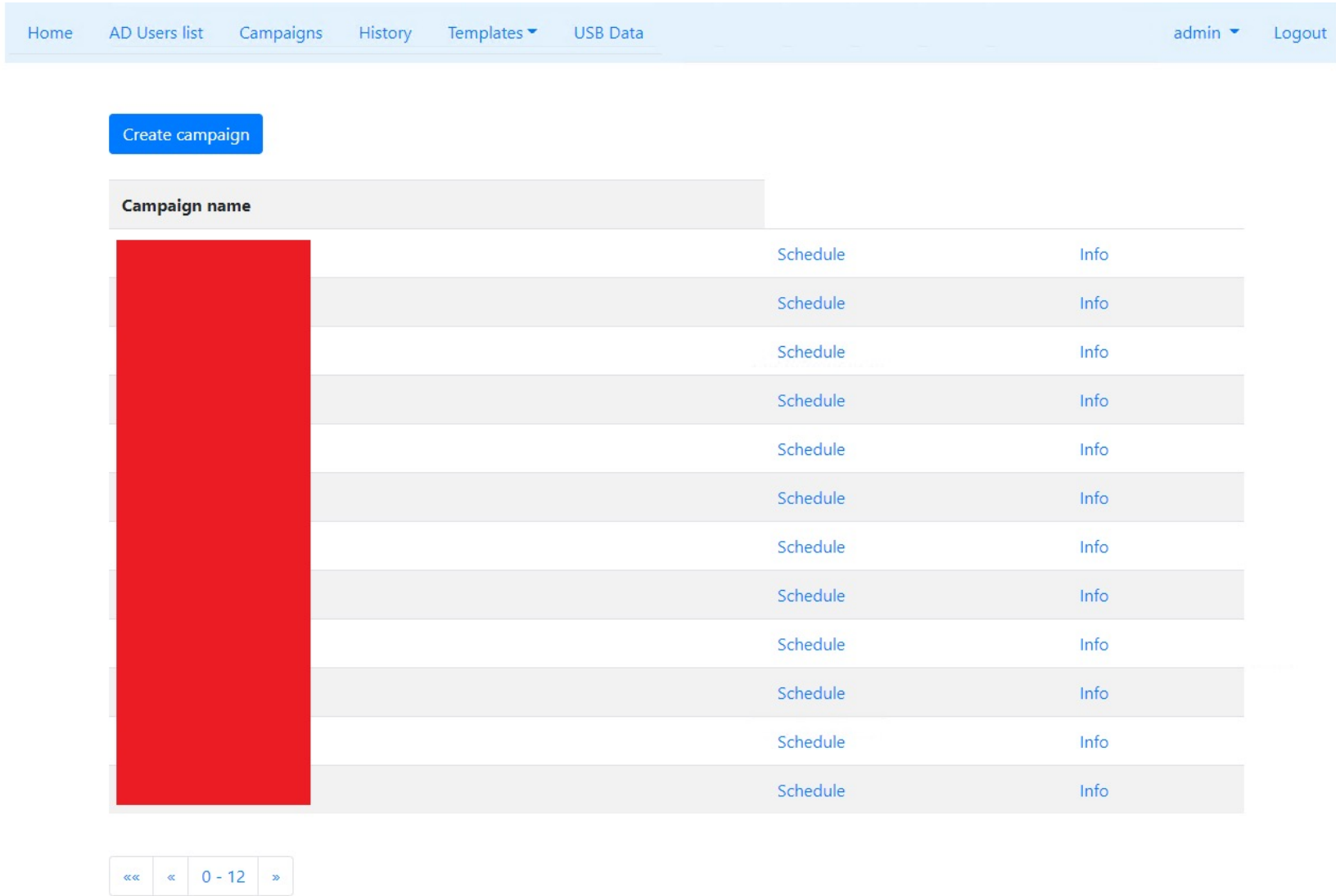
- Phishing Web-site in Public Cloud
- Anti-Phishing Server in Docker/Kubernetes (on-prem)

Stack

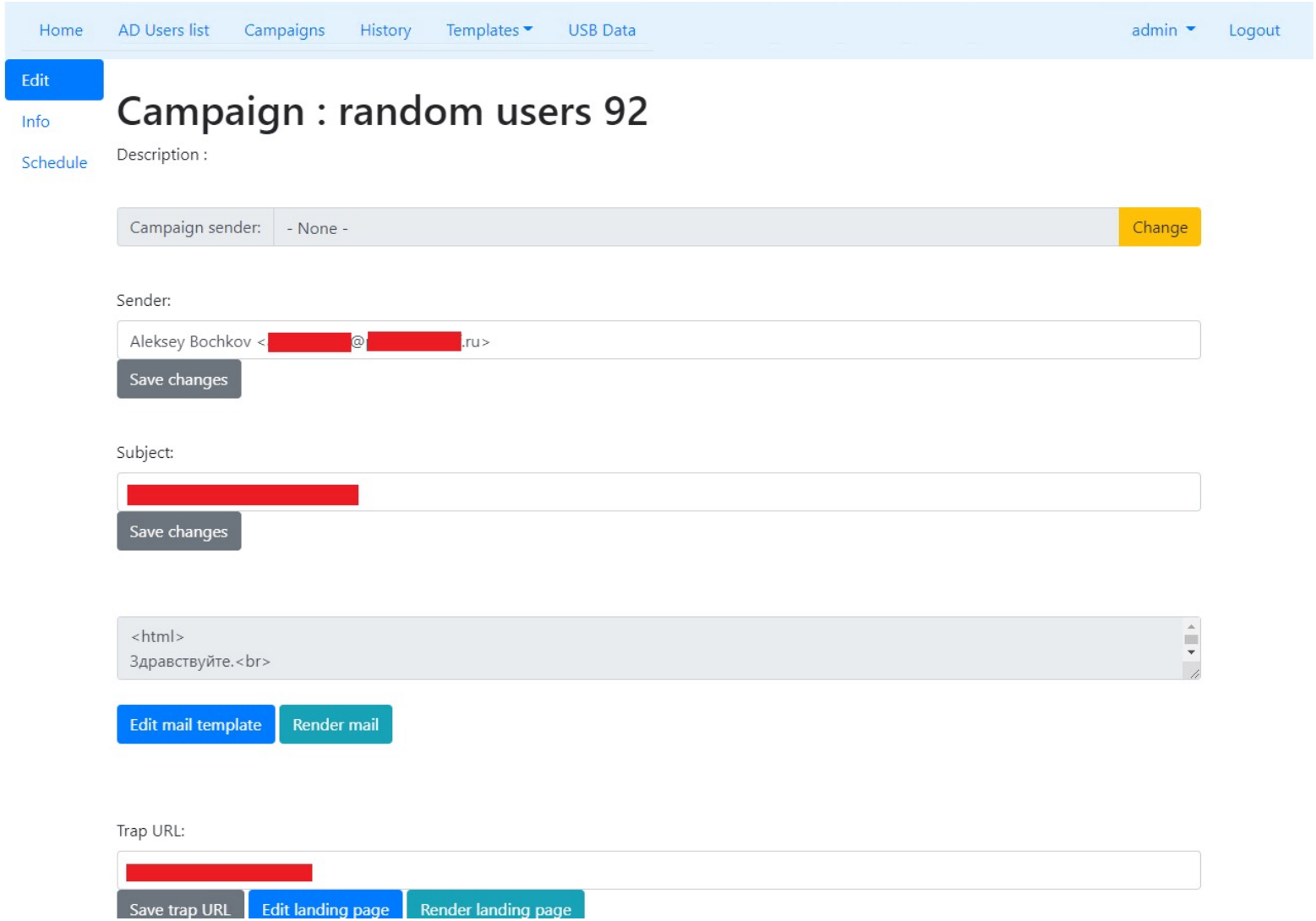
- Python
- Flask
- MongoDB



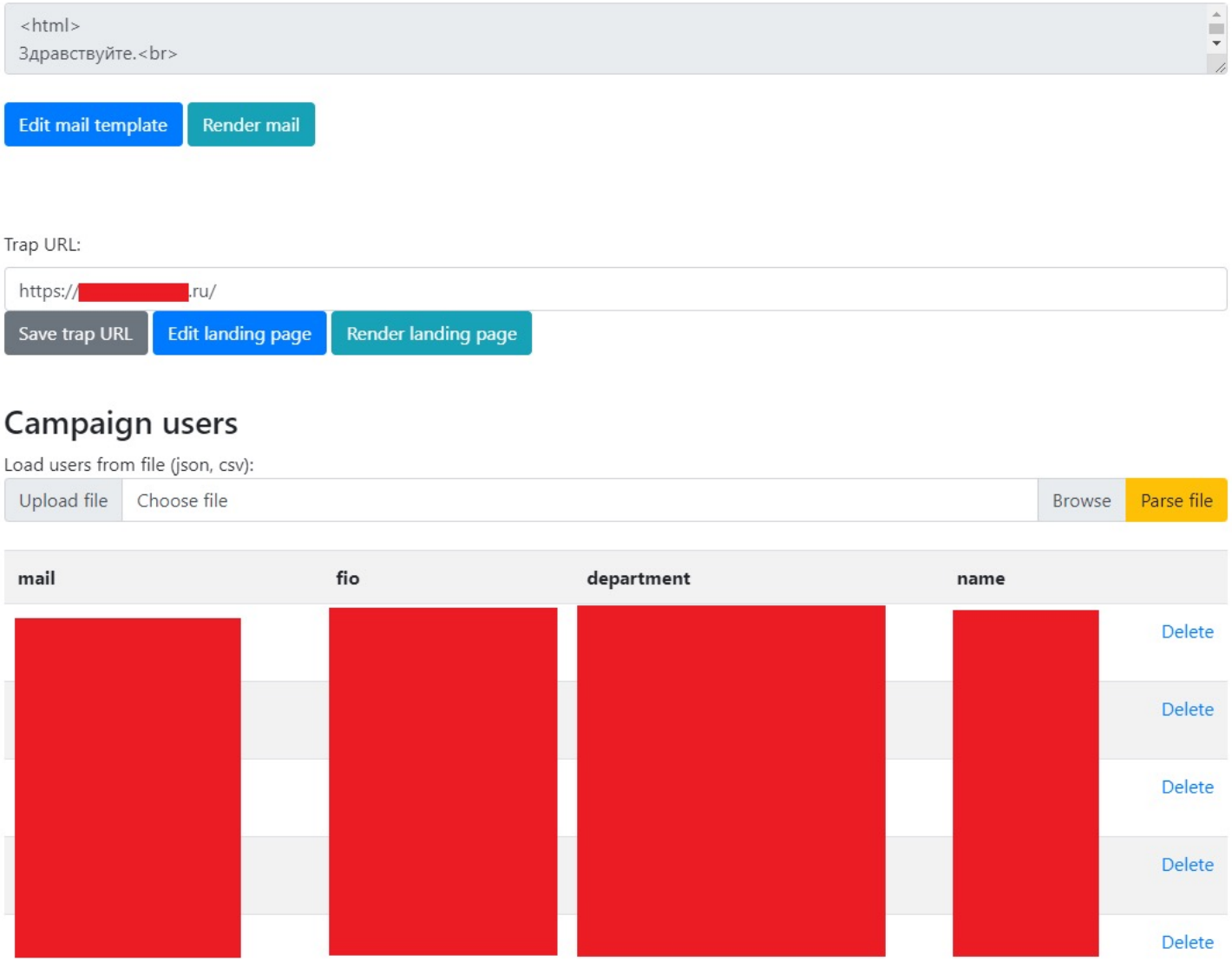
Campaigns


Home
AD Users list
Campaigns
History
Templates
USB Data
admin
Logout
Create campaign
Campaign name
Schedule
Info
«« « 0 - 12 »

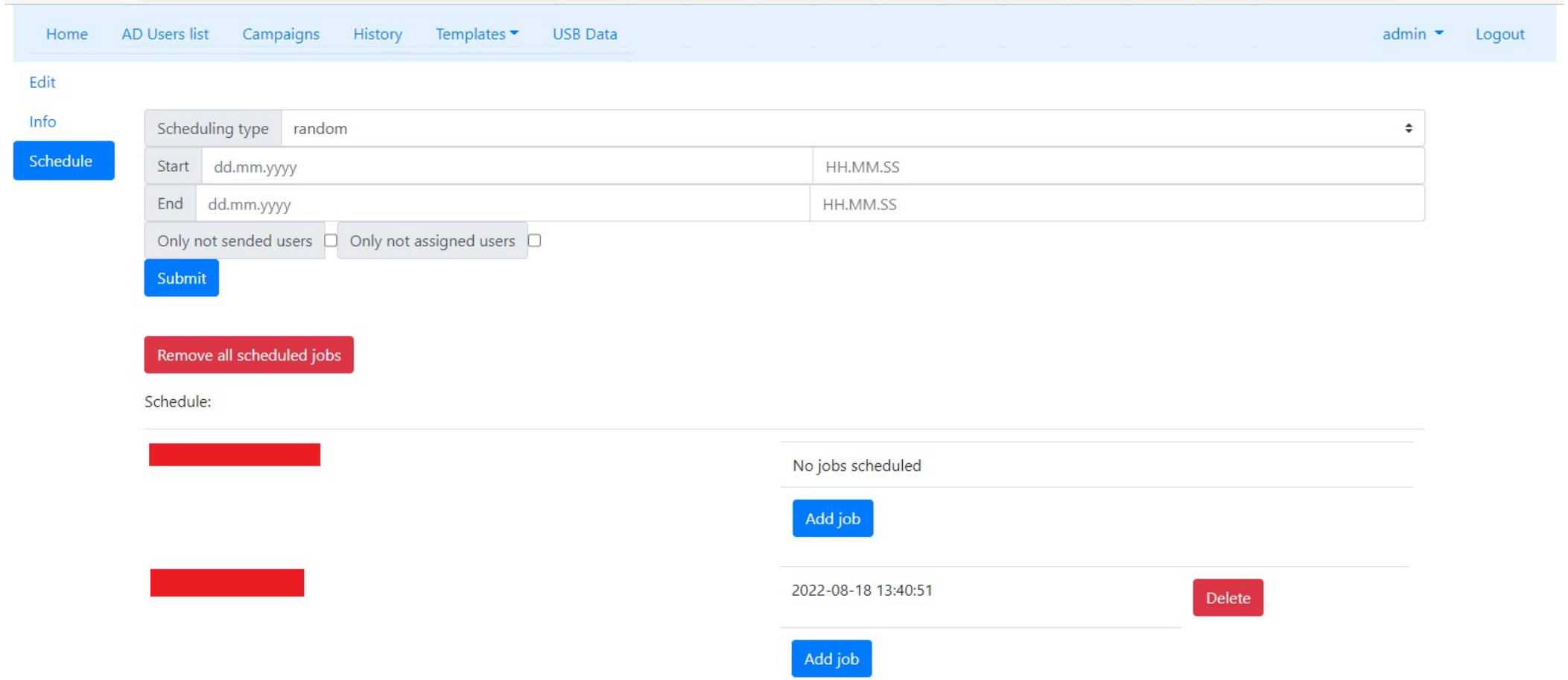
Campaign: email and link to phishing site



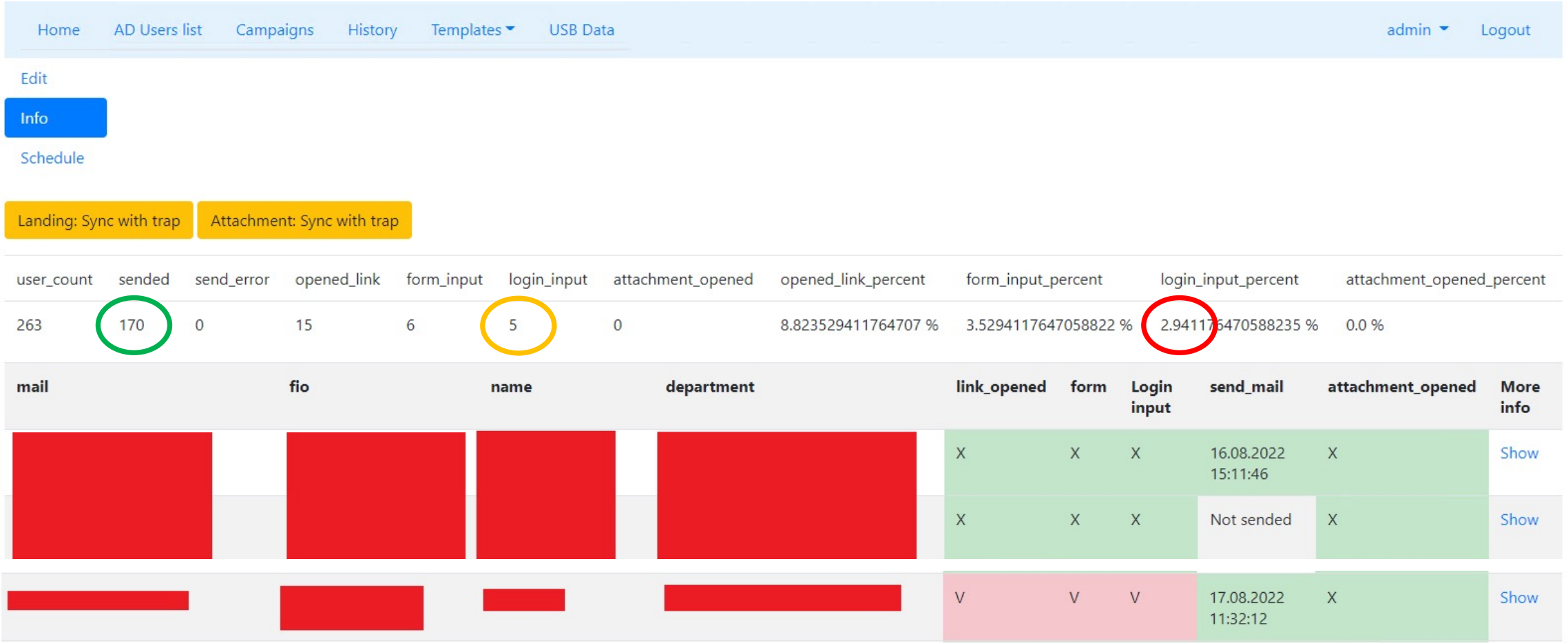
Campaign: users



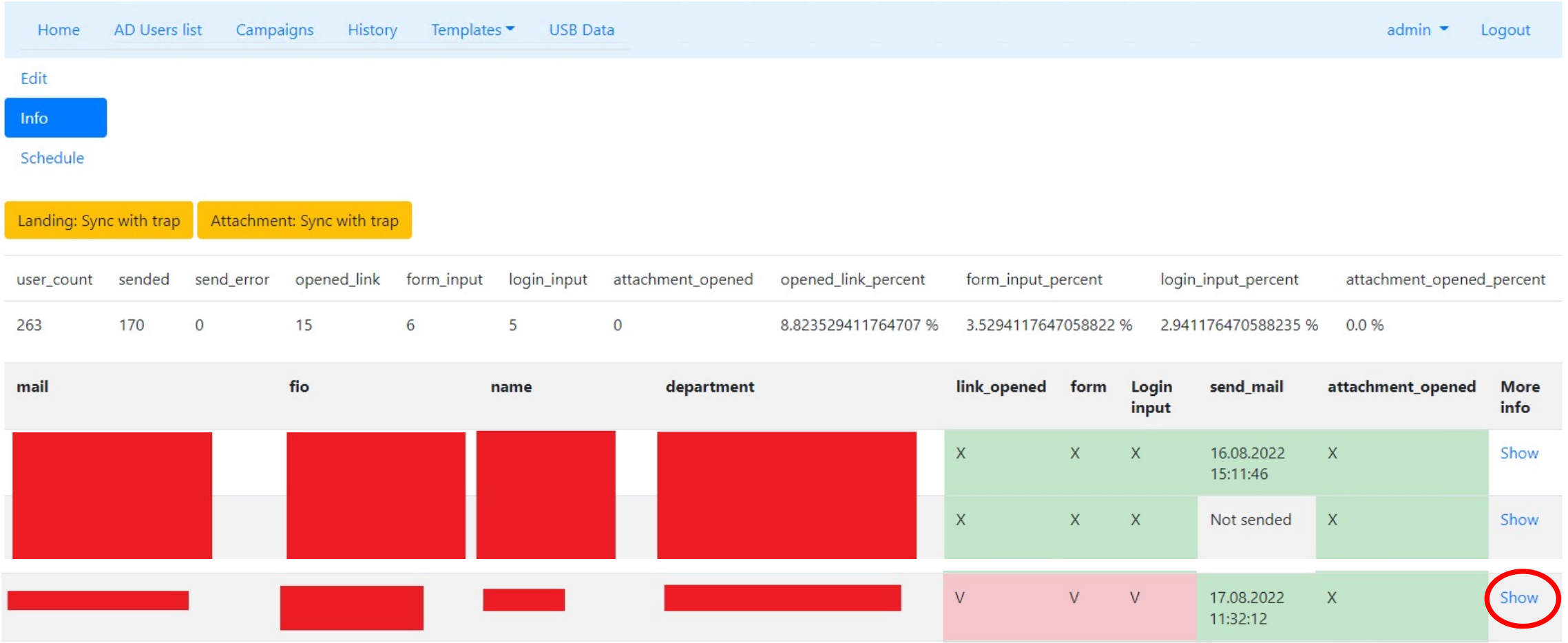
Campaign: scheduler



Campaign: current results



Campaign: current results



Home | AD Users list | Campaigns | History | Templates | USB Data | admin | Logout

Edit

Info

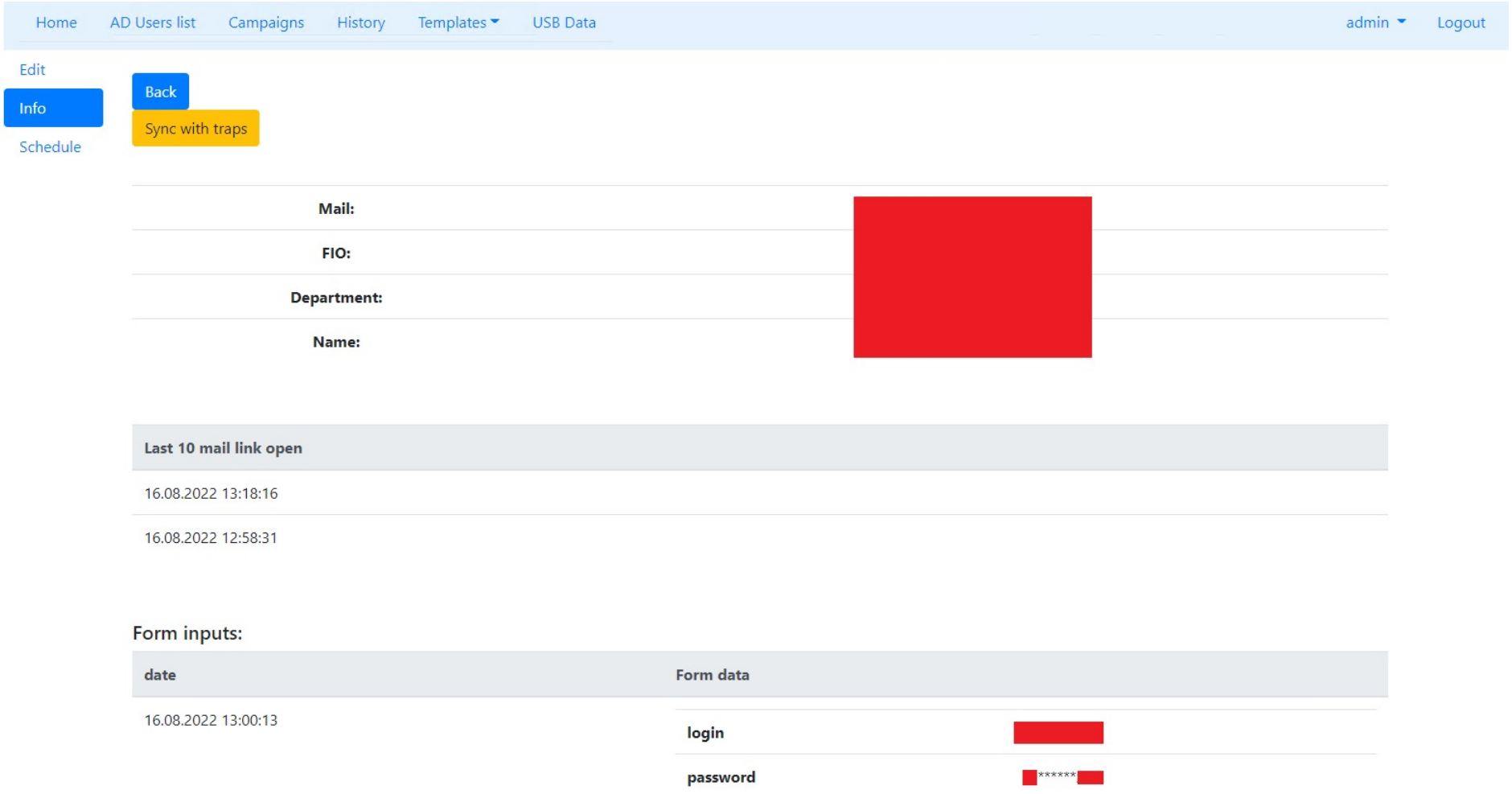
Schedule

Landing: Sync with trap | Attachment: Sync with trap

user_count	sended	send_error	opened_link	form_input	login_input	attachment_opened	opened_link_percent	form_input_percent	login_input_percent	attachment_opened_percent
263	170	0	15	6	5	0	8.823529411764707 %	3.5294117647058822 %	2.941176470588235 %	0.0 %

mail	fio	name	department	link_opened	form	Login input	send_mail	attachment_opened	More info
[redacted]	[redacted]	[redacted]	[redacted]	X	X	X	16.08.2022 15:11:46	X	Show
				X	X	X	Not sended	X	Show
[redacted]	[redacted]	[redacted]	[redacted]	V	V	V	17.08.2022 11:32:12	X	Show

Campaign: compromised employee



Adding a new template

- Come up with a text that should motivate employees to click on the link and enter their credentials
- Approve the idea with HR
- Buy a new domain name (if necessary)
- Set up the appearance for the **form** on the phishing site, the **text** of the email
- Alert SOC about new template
- Set up a campaign

HR Approval Issues

- No communication on behalf of HR or existing departments
- It is advisable not to use resources similar to startup projects of the company
- "Sensitive topics" are forbidden:
  - Everything about salaries
  - "Free lunches for remote workers"

Highly effective templates

- "Remote Employee Entry Control System"
- Requests from "colleagues" to urgently look at tasks
- Messages from "system administrators" (expanding the size of the mailbox, your mailbox is blocked, etc.)

Our statistics

- First campaign: 06.2020
- Over 23598 users have received emails at least once
- Usually about 40% of employees fall into the trap (except for "unsuccessful" templates); 25% average
- An information security course is assigned to employees who have fallen into the trap

Re-sending

- Over 7682 re-sendings with different template
- On average 8.6% fall into the trap again and get one more information security course

What to do with users who are not able to learn?

Processing untrainable employees: TOPs

- Engaging executives
  - Department statistics
  - Email template for Executives
    - Take the assigned courses
    - Threat of restrictions

Processing untrainable employees: restrictions

- Restriction on working with e-mail
  - To receive emails from external senders - create a request to the first line of support
  - The first line of support validates that the email is normal

What are our plans?

- Frontend redesign
- Convenient deployment and configuration independent of the Tinkoff infrastructure
- Integration with business metrics regarding employees

ON FF ONE 2022

Questions?
Want to try it yourself?

a.leonov1@tinkoff.ru
t.me/leonov_av

The presentation used footage from the films of Leonid Gaidai: "Kidnapping, Caucasian Style" (1967), "Operation Y and Shurik's Other Adventures" (1965), "Ivan Vasilievich Changes Profession" (1973)