



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования

«Дальневосточный федеральный университет»

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ОТЧЕТ

по лабораторной работе № 2

«Проведение фишинговой атаки»

Выполнили студенты гр. М9120-
09.04.01 кибер

_____ Крюков Ю.М

_____ Дрожжина А.П.

_____ Личковаха С. А.

Проверил преподаватель

_____ Зотов С.С.

(оценка)

г. Владивосток

2021

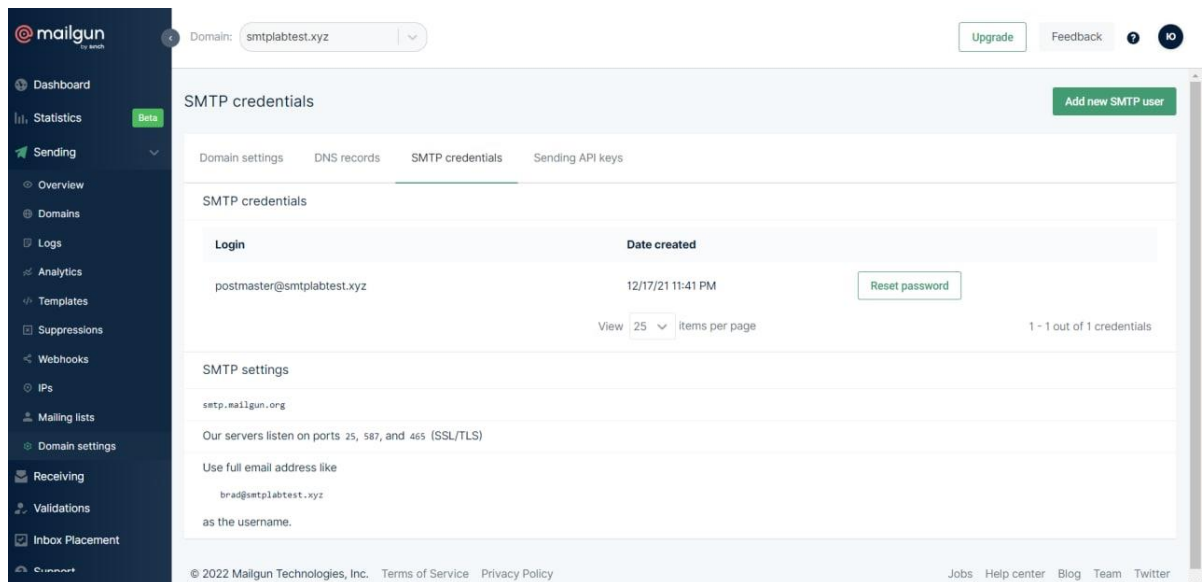


Рисунок 1 - SMTP сервер

Настройка сервера EC2:

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

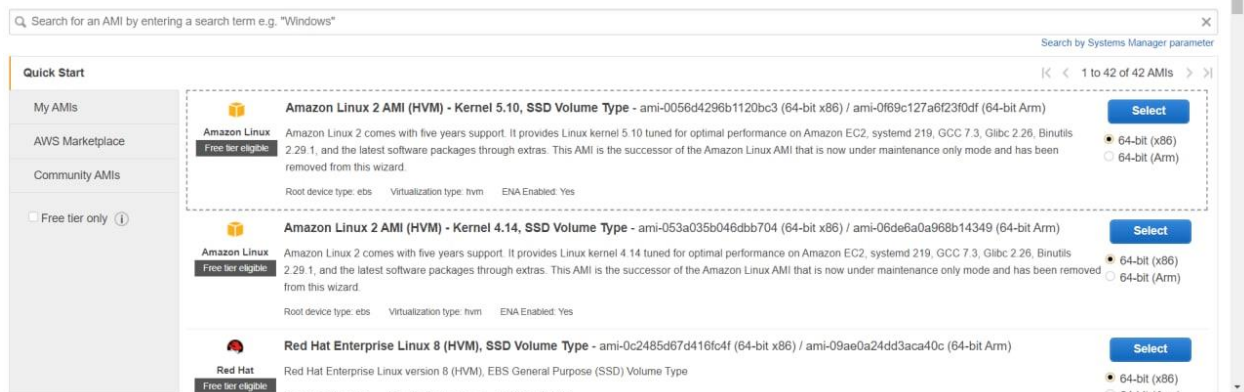


Рисунок 2 – Шаг 1 настройки сервера

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

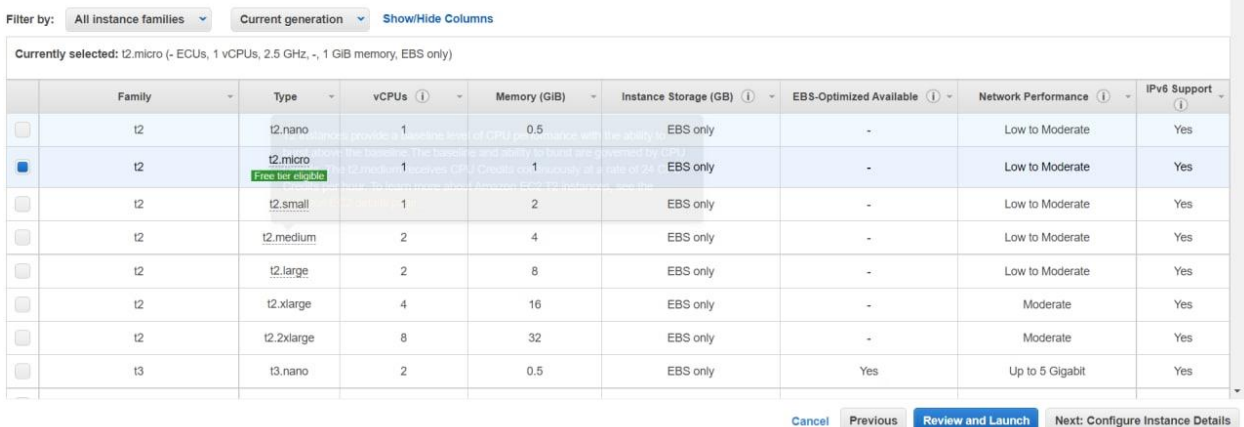


Рисунок 3 – Шаг 2 настройки сервера

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances ⓘ1Launch into Auto Scaling Group ⓘ

Purchasing option ⓘ☐ Request Spot Instances

Network ⓘvpc-07cf1d8655f1da1c7 (default)Create new VPC

Subnet ⓘNo preference (default subnet in any Availability Zone)Create new subnet

Auto-assign Public IP ⓘUse subnet setting (Enable)

Hostname type ⓘUse subnet setting (IP name)

DNS Hostname ⓘ

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group ⓘ☐ Add instance to placement group

Capacity Reservation ⓘOpen

Domain join directory ⓘNo directoryCreate new directory

IAM role ⓘNoneCreate new IAM role

CancelPreviousReview and LaunchNext: Add Storage

Рисунок 4 – Шаг 3 настройки сервера

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/xvda	snap-0dc25ec2d6e1528b3	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Shared file systems ⓘ

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

CancelPreviousReview and LaunchNext: Add Tags

Рисунок 5 – Шаг 4 настройки сервера

awsServicesSearch for services, features, blogs, docs, and more[Alt+S]

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key ⓘ (128 characters maximum)	Value ⓘ (256 characters maximum)	Instances ⓘ	Volumes ⓘ	Network Interfaces ⓘ
Name	Gophish server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
owner	jim.lamb	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
billing	internal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

CancelPreviousReview and LaunchNext: Configure Security Group

Рисунок 6 – Шаг 5 настройки сервера

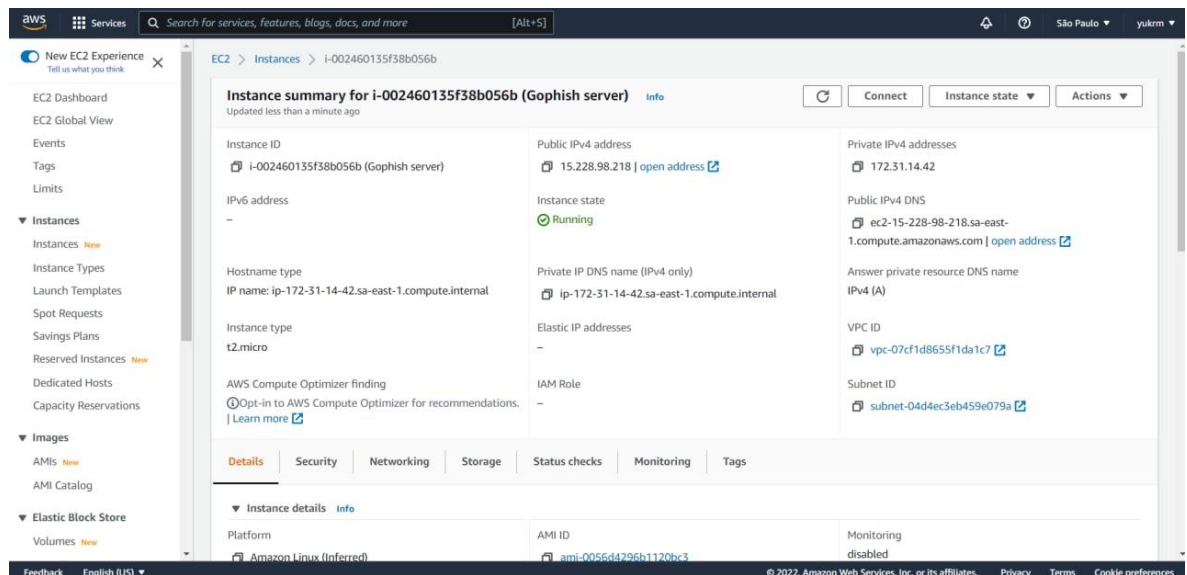


Рисунок 7 - Сервер EC2 с развернутой на нем Linux

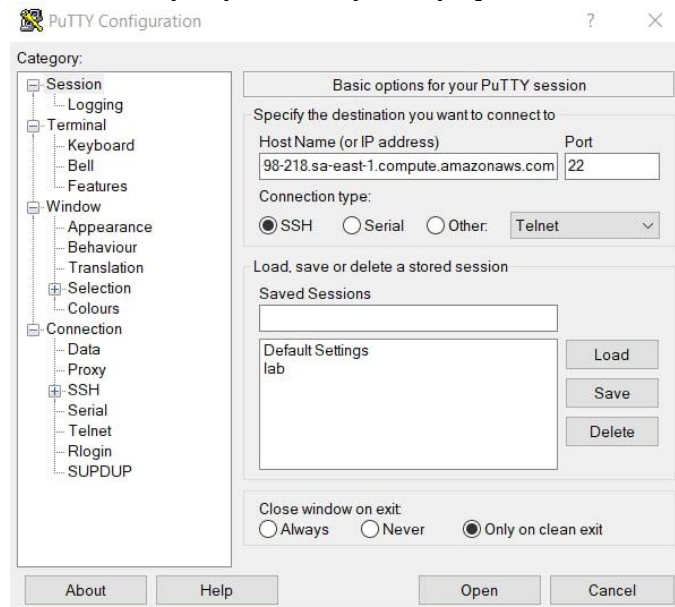


Рисунок 8 - Подключение к виртуальной машине

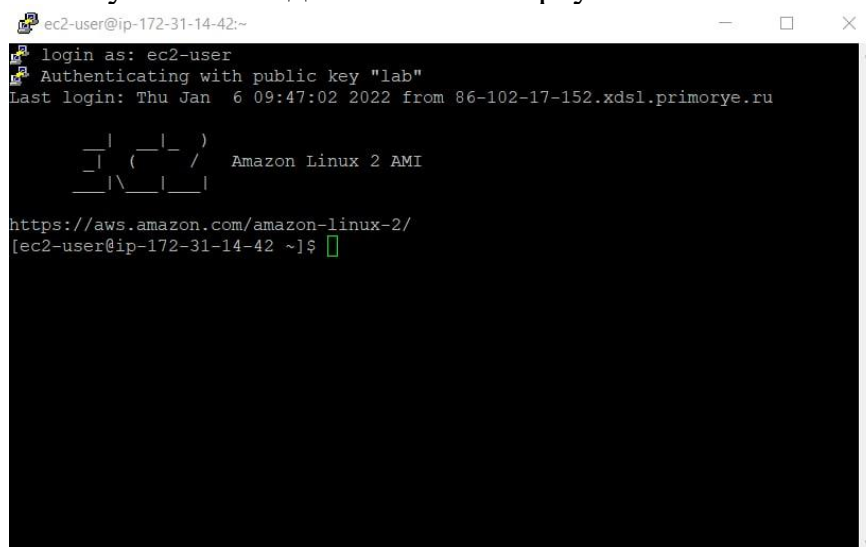


Рисунок 9 – Подтверждение подключения

```
[ec2-user@ip-172-31-14-42 lab]$ sudo ./gophish
time="2022-01-06T09:56:12Z" level=warning msg="No contact address has been configured."
time="2022-01-06T09:56:12Z" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20200730000000
time="2022-01-06T09:56:12Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
time="2022-01-06T09:56:12Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2022-01-06T09:56:12Z" level=info msg="Starting IMAP monitor manager"
time="2022-01-06T09:56:12Z" level=info msg="Starting new IMAP monitor for user admin"
time="2022-01-06T09:56:12Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
```

Рисунок 10 – Запуск Gophish

```
GNU nano 2.9.8 config.json

{
  "admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key"
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",

```

Рисунок 11 – Замена поля listen_url

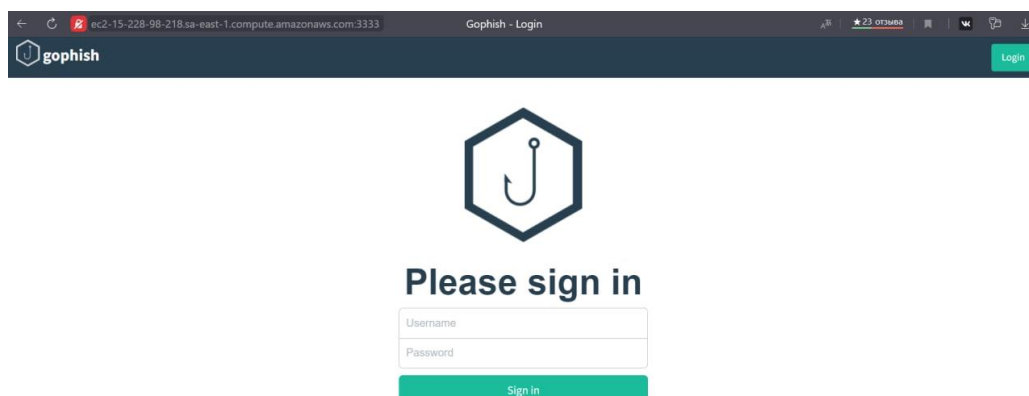


Рисунок 12 – Страница входа в Gophish

New Sending Profile

Name:

lab2

Interface Type:

SMTP

From:

postmaster@smtpplabtest.xyz

Host:

smtp.mailgun.org:587

Username:

postmaster@smtpplabtest.xyz

Password:

.....

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{[.URL]}-gophish

+ Add Custom Header

Show

10

entries

Search:

Header

Value

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Рисунок 13 – Настройка профиля для рассылки

New Landing Page

Name:

 lab2

Import Site

HTML

```
<!DOCTYPE html><html lang="ru"><head>
<base href="https://esa.dvfu.ru/?bu=https%3A%2F%2Fidm.dvfu.ru%2Fmenu%2Fview/">
<meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta charset="UTF-8"/><meta
name="viewport" content="width=device-width, initial-scale=1"/>
<link href="/favicon/apple-touch-icon.png?v=wAXxPe8bK4" rel="apple-touch-
icon"/>
<link href="/favicon/favicon.ico?v=wAXxPe8bK4" rel="shortcut icon"
type="image/x-icon"/>
```

☒ Capture Submitted Data ⓘ
 ☒ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: ⓘ

 https://esa.dvfu.ru/?bu=https%3A%2F%2Fidm.dvfu.ru%2Fmenu%2Fview

Рисунок 14 – Настройка целевой страницы

New Campaign

Name:

lab2

Email Template:

first

Landing Page:

lab2

URL: ?

http://ec2-15-228-98-218.sa-east-1.compute.amazonaws.com

Launch Date

January 8th 2022, 2:23 pm

Send Emails By (Optional) ?

Sending Profile:

lab2

Send Test Email

Groups:

× lab2

Close

Launch Campaign

Рисунок 17 – Создание фишинговой компании

Details

Show 10 entries

First Name	Last Name	Email	Position	Scheduled to send at January 9th 2022, 7:00:00 am	Reported
11	11	santa_ctf@mail.ru		Scheduled	⊗
123	123	sofya-lichkovakha@mail.ru		Scheduled	⊗
22	22	drozhzhina.ap@protonmail.com		Scheduled	⊗
22	22	santa.claus.68@list.ru		Scheduled	⊗
dvfu	dvfu	kriukov.iur@students.dvfu.ru		Scheduled	⊗
dvfu	dvfu	lichkovakha.sa@students.dvfu.ru		Scheduled	⊗
dvfu	dvfu	razumov_ea@students.dvfu.ru		Scheduled	⊗
dvfu.ru	dvfu.ru	cheivelkhut.av@students.dvfu.ru		Scheduled	⊗
dvfu.ru	dvfu.ru	drozhzhina.ap@students.dvfu.ru		Scheduled	⊗
gmail	gmail	annadrozhzhina1998@gmail.com		Scheduled	⊗

Showing 1 to 10 of 20 entries

Previous 1 2 Next



Details

Show 10 entries

First Name	Last Name	Email	Position	Status	Reported
11	11	santa_ctf@mail.ru		Email Sent	⊗
123	123	sofya-lichkovakha@mail.ru		Email Sent	⊗
22	22	drozhzhina.ap@protonmail.com		Email Sent	⊗
22	22	santa.claus.68@list.ru		Email Sent	⊗
dvfu	dvfu	kriukov.iur@students.dvfu.ru		Email Sent	⊗
dvfu	dvfu	lichkovakha.sa@students.dvfu.ru		Email Sent	⊗
dvfu	dvfu	razumov_ea@students.dvfu.ru		Email Sent	⊗
dvfu.ru	dvfu.ru	cheivelkhut.av@students.dvfu.ru		Email Sent	⊗
dvfu.ru	dvfu.ru	drozhzhina.ap@students.dvfu.ru		Email Sent	⊗
gmail	gmail	annadrozhzhina1998@gmail.com		Email Sent	⊗

Showing 1 to 10 of 20 entries

Previous 1 2 Next

Рисунок 18 - Результаты первой рассылки

Отслеживание открытия письма по картинке (пикселю) не делали т.к. из-за этого почти со 100% вероятностью письмо попадает в спам, определить взаимодействовали ли с письмом можно по уведомлению canarytokens.

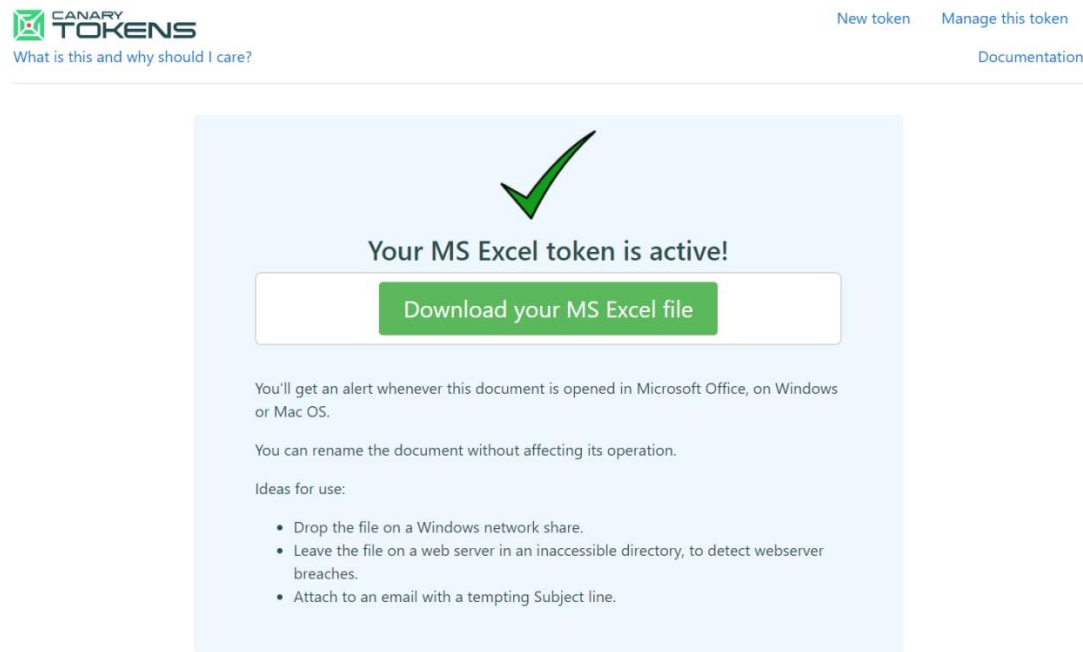


Рисунок 19 - Создание файла canarytokens

После того, как получатели писем открывали таблицу, мы получали информацию о взаимодействии с файлами canarytokens (рис.20). Из этих записей мы можем увидеть IP-адреса, время открытия файла и примерное местоположение.

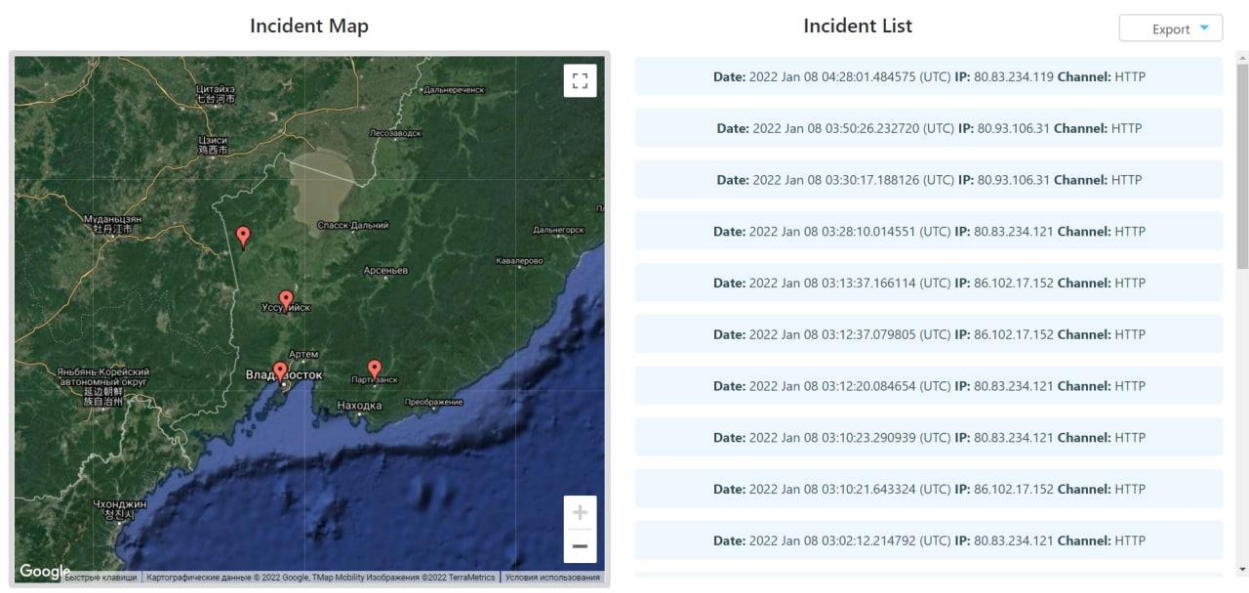


Рисунок 20 - Информация о взаимодействии с файлами canarytokens



Date: 2022 Jan 08 03:12:20.084654 (UTC) IP: 80.83.234.121 Channel: HTTP	
Geo Info	
Country	RU 
City	Pogranichnyy
Region	Primorskiy (Maritime) Krai
Organisation	AS8359 MTS PJSC
Hostname	80.83.234.121.gprs.mrdv.mts.ru
	
Known Exit Node	False
Basic Info	
Memo	Он был чипирован
useragent	Mozilla/4.0 (compatible; ms-office; MSOffice rmj)

Рисунок 21 - Подробная информация о отдельном открытии

Результаты первой рассылки письма со скриптом представлены ниже в таблице 1. Из результатов можно сделать вывод, что с определением фишингового письма лучше всего справился gmail, так как на всех пяти почтах письмо было помещено в спам и было указано о том, что письмо определено как фишинговое. Худшими оказались mail и protonmail, в них письмо прошло проверку и не попало в спам. Почта dvfu отправило письмо в спам на трех аккаунтах из пяти, на двух почему-то проверка прошла. Скриншоты с результатами прихода писем в спам/не спам представлены на рисунках 22–26.

Таблица 1 – Результаты проверки письма на каждой из почт

Почты mail	5 прошло	Почты ДВФУ	3 спам/ 2 прошло
yukrm@mail.ru	прошло	cheivelkhut.av@students.dvfu.ru	спам
sofya-lichkovakha@mail.ru	прошло	drozhzhina.ap@students.dvfu.ru	прошло
drozhzhina.anna@list.ru	прошло	kriukov.iium@students.dvfu.ru	спам
santa.claus.68@list.ru	прошло	lichkovakha.sa@students.dvfu.ru	спам
santa_ctf@mail.ru	прошло	razumov_ea@students.dvfu.ru	прошло
Почты протон	5 прошло	Почты гмаил	5 спам
drozhzhina.ap@protonmail.com	прошло	annadrozhzhina1998@gmail.com	спам
yukrm@protonmail.com	прошло	yukrmm@gmail.com	спам
sofi.lichkovaha@protonmail.com	прошло	petrovasona033@gmail.com	спам
lab2proton@protonmail.com	прошло	adrozina324@gmail.com	спам
fishing221@protonmail.com	прошло	lab220222@gmail.com	спам

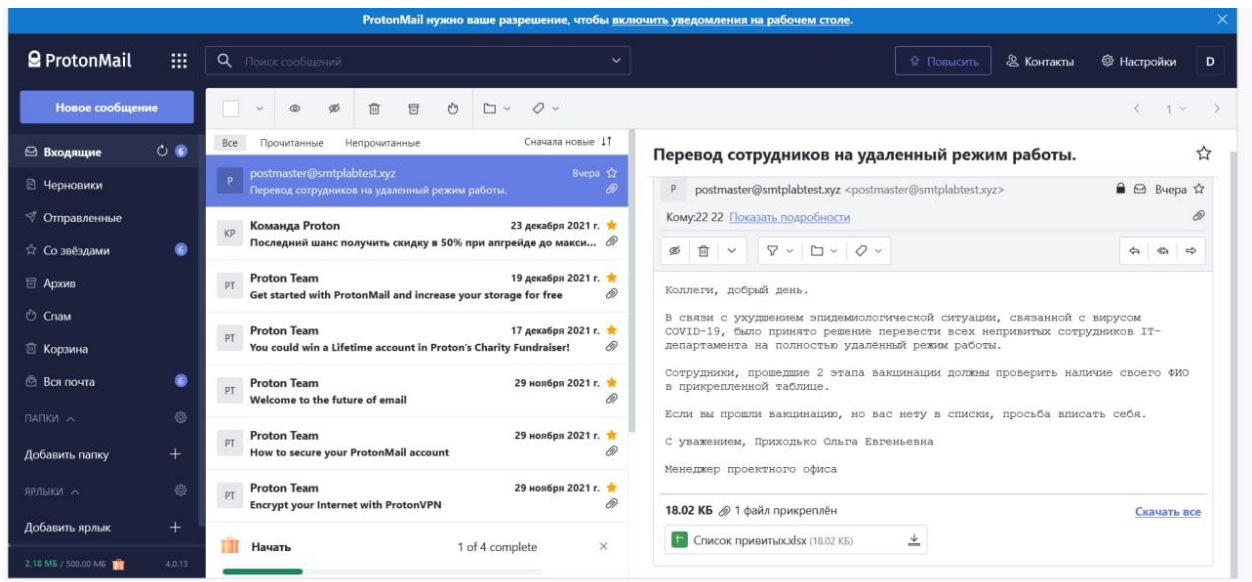


Рисунок 22 – Письмо, прошедшее проверку в protonmail

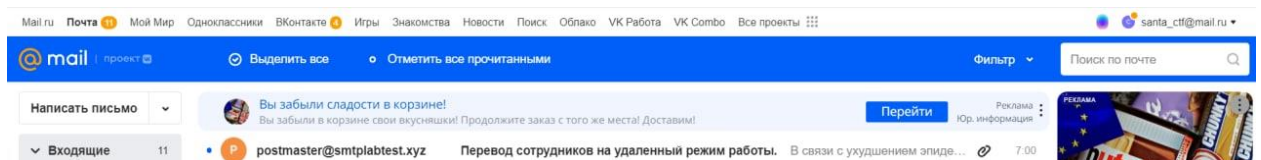


Рисунок 23 – Письмо, прошедшее проверку в mail

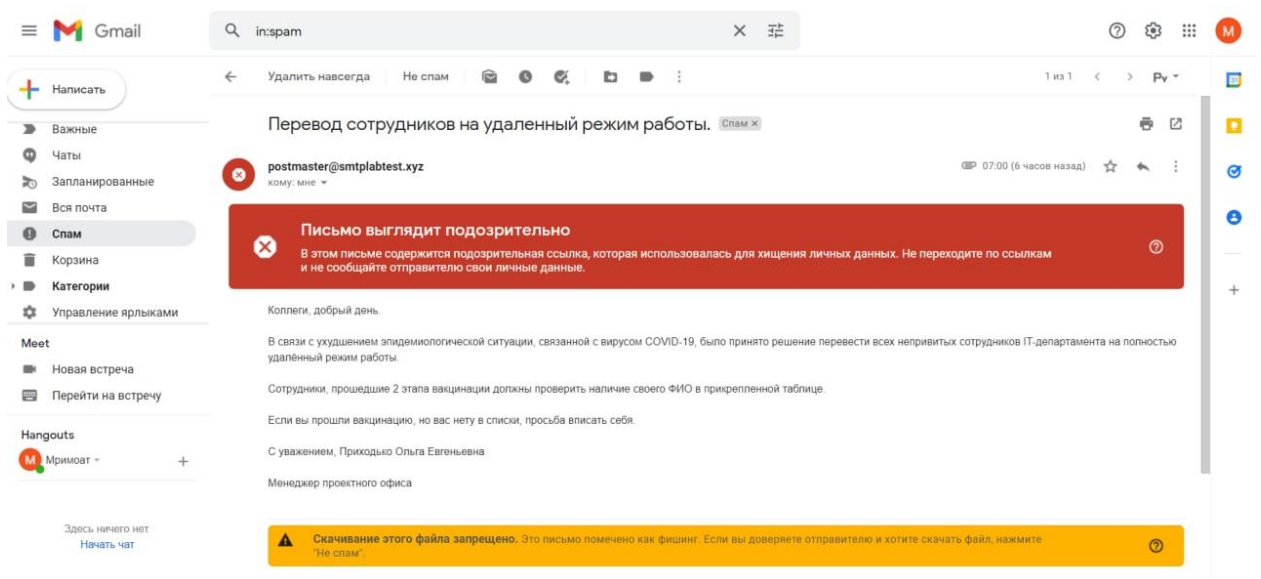


Рисунок 24 – Письмо, непрошедшее проверку в gmail

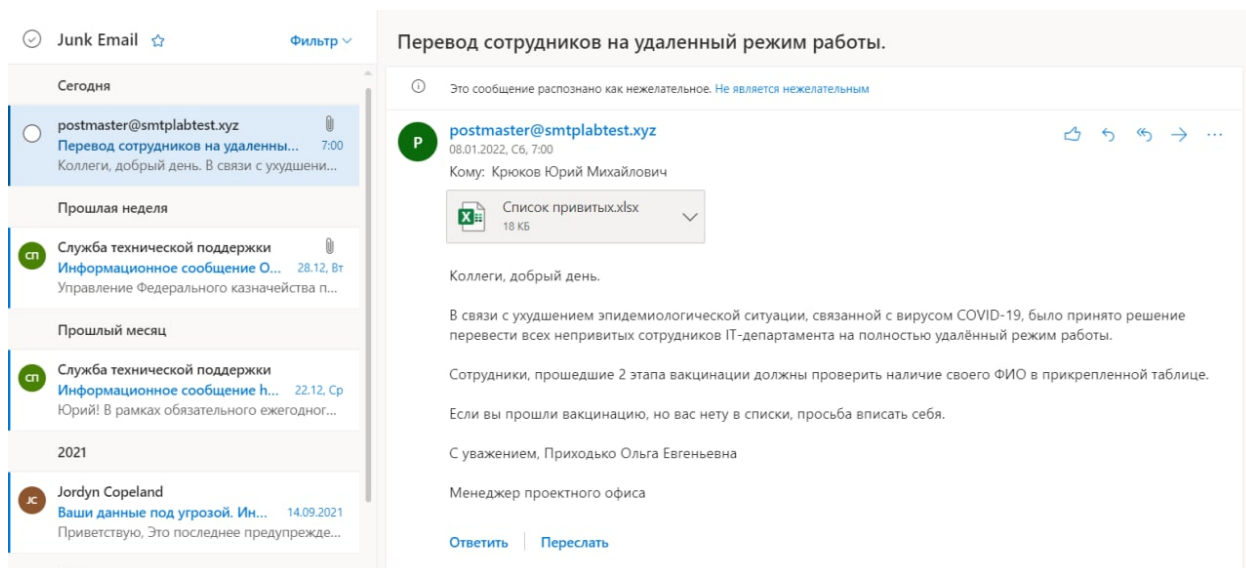


Рисунок 25 – Письмо, непрошедшее проверку в dvfu.ru

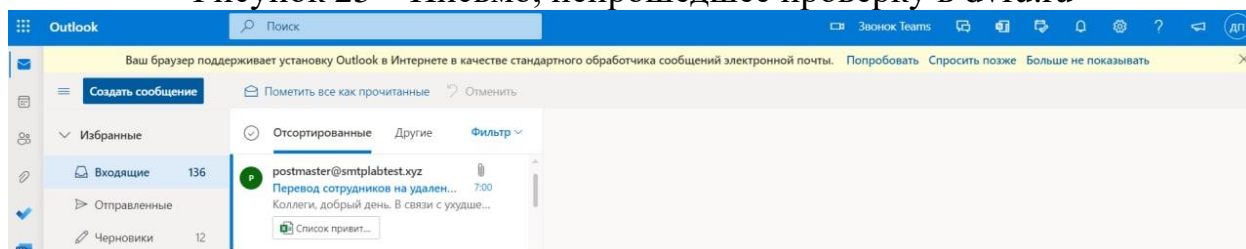


Рисунок 26– Письмо, прошедшее проверку в dvfu.ru

Результаты рассылки второго письма со ссылкой на сайт авторизации ДВФУ представлены ниже в таблице 2. Пример отображения данных по определённой почте представлен на рисунке 27, общие результаты рассылки представлены на рисунке 28. По результатам проверки все осталось также, где прошлые письма прошли проверку, то они прошли и в этот раз, где попали спам, то и в спаме сейчас.

Таблица 2 – Результаты проверки письма на каждой из почт

Почты mail	5 прошло	Логин	Пароль
yukrm@mail.ru	прошло	Kryukov Yuri Mikhailovich	2022,01,09,16,44
sofya-lichkovakha@mail.ru	прошло	Личковаха Софья Алексеевна	2000.01.09.01.15
drozhzhina.anna@list.ru	прошло	Дрожжина Анна Петровна	2022.01.09.09.45
santa.claus.68@list.ru	прошло	Дрожжина Анна Петровна	2022.01.10.00.17
santa_ctf@mail.ru	прошло	Дрожжина Анна Петровна	2021.09.01.18.07

Почты протон	5 прошло		
drozhzhina.ap@protonmail.com	прошло	Дрожжина А.П.	2022.01.10.00.31
yukrm@protonmail.com	прошло	Крюков Ю.М.	2022.01.10.00.36
sofi.lichkovaha@protonmail.com	прошло	-	-
lab2proton@protonmail.com	прошло	Крюков Ю.М.	2022Ю01Ю10Ю00Ю39
fishing221@protonmail.com	Прошло	Крюков Ю.М.	2022Ю01Ю10Ю00Ю41
Почты ДВФУ	3 спам/ 2 прошло		
cheivelkhut.av@students.dvfu.ru	спам	cheivelkhut.anatolij.vas	2022.01.09.11.58
drozhzhina.ap@students.dvfu.ru	прошло	Дрожжина Анна Петровна	2022.01.09.09.43
kriukov.iium@students.dvfu.ru	спам	-	-
lichkovakha.sa@students.dvfu.ru	спам	-	-
razumov_ea@students.dvfu.ru	прошло	Разумов Е.	huymya
Почты гмаил	5 спам		
annadrozhzhina1998@gmail.com	спам	Дрожжина Анна Петровна	2022,01,10,00,22
yukrmm@gmail.com	спам	-	-
petrovasona033@gmail.com	спам	-	-
adrozzina324@gmail.com	спам	Дрожжина Анна Петровна	2022,01,10,00,21
lab220222@gmail.com	спам	Дрожжина Анна Петровна	2022,01,10,00,23

▼

dvfu.ru

dvfu.ru

drozhzhina.ap@students.dvfu.ru

Submitted Data

Timeline for dvfu.ru dvfu.ru

Email: drozhzhina.ap@students.dvfu.ru
Result ID: SawW8pS

- Campaign Created

January 8th 2022 7:18:51 pm
- Email Sent

January 9th 2022 7:00:17 am
- Clicked Link

January 9th 2022 9:42:54 am

 - Apple iPhone (OS Version: 15.1)
 - Safari (Version: 15.1)
- Submitted Data

January 9th 2022 9:44:06 am

 - Apple iPhone (OS Version: 15.1)
 - Safari (Version: 15.1)

Replay Credentials

View Details

Parameter	Value(s)
__original_url	https://esa.dvfu.ru/?bu=https%3A%2F%2Fidm.dvfu.ru%2Fmenu%2Fview/?bu=https%3A%2F%2Fidm.dvfu.ru%2Fmenu%2Fview
_csrf_univer	8D9cnaA4MBQ3FOy-XC96fgOfTucHhozWJuzwytkiDiDHdwr5jXJdQ3FVs7UOeCghe-kYoEnHxKRQ3aiHmPtoQQ==
bu	https://idm.dvfu.ru/menu/view
password	2022.01.09.09.43
username	Дрожжина Анна Петровна

Рисунок 27 – Полный список сведений для почты

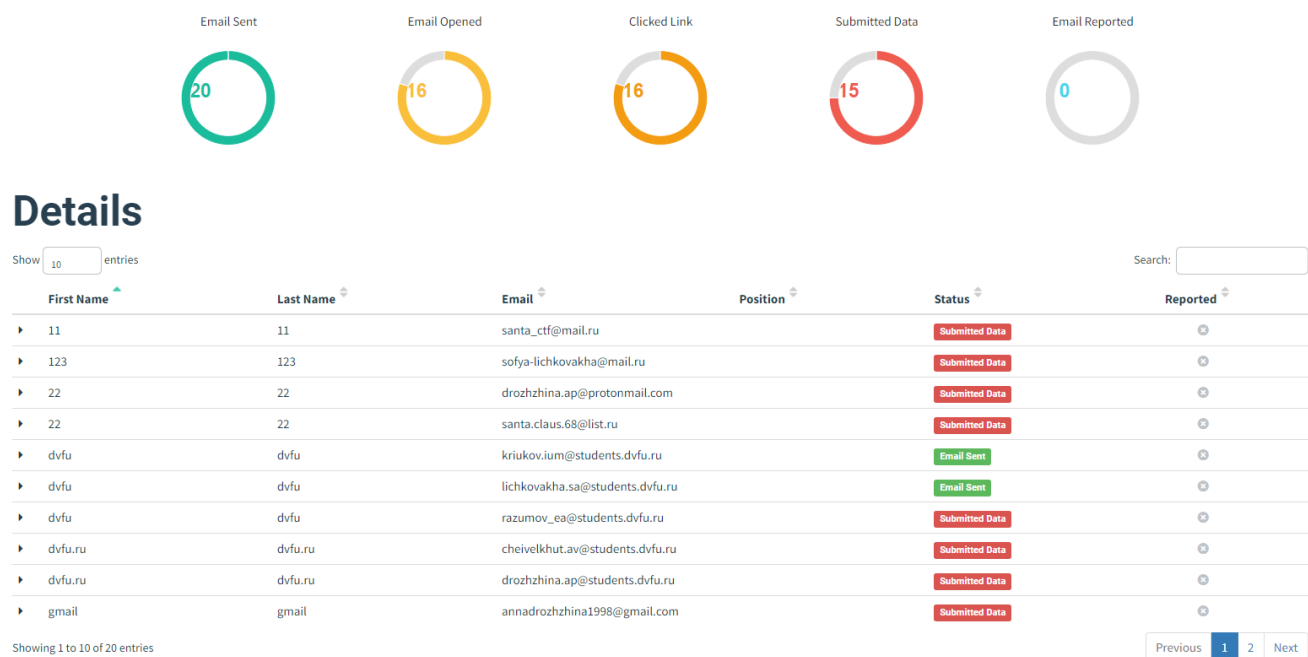


Рисунок 28 - Общие результаты

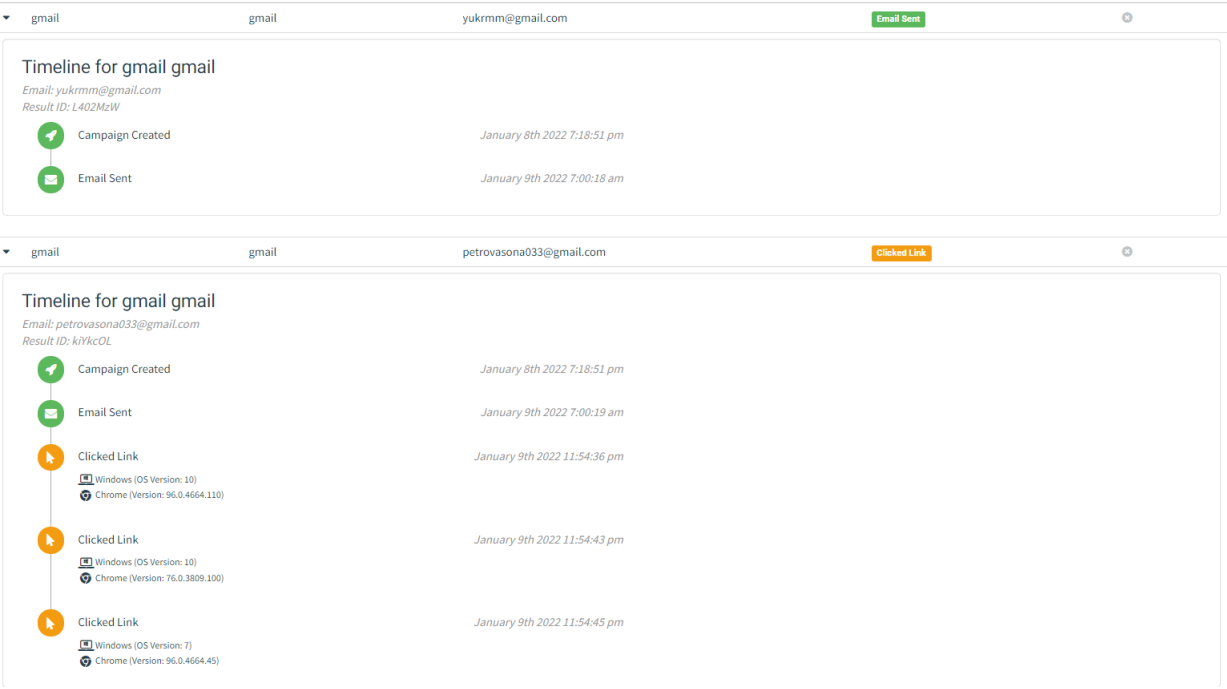


Рисунок 29 – Другие статусы писем