МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информационной безопасности

Лабораторная работа №2

Выполнили студенты гр. М9120-09.04.02ИБКФС

Ефременко И.В.,
Медведев Н.В

Старший преподаватель

С.С. Зотов

зачтено / не зачтено

г. Владивосток
2022

Установка gophish:

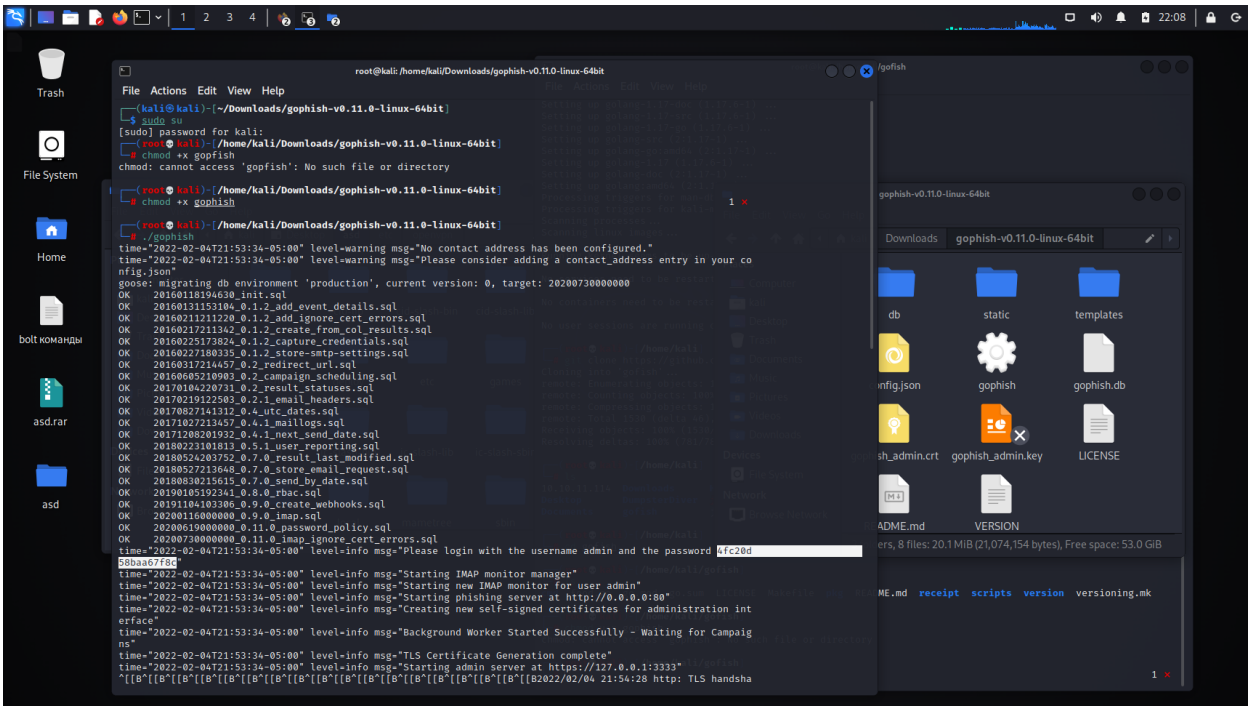


Рисунок 1 gophish

Сервис заработал и мы попали на главную страницу localhost.

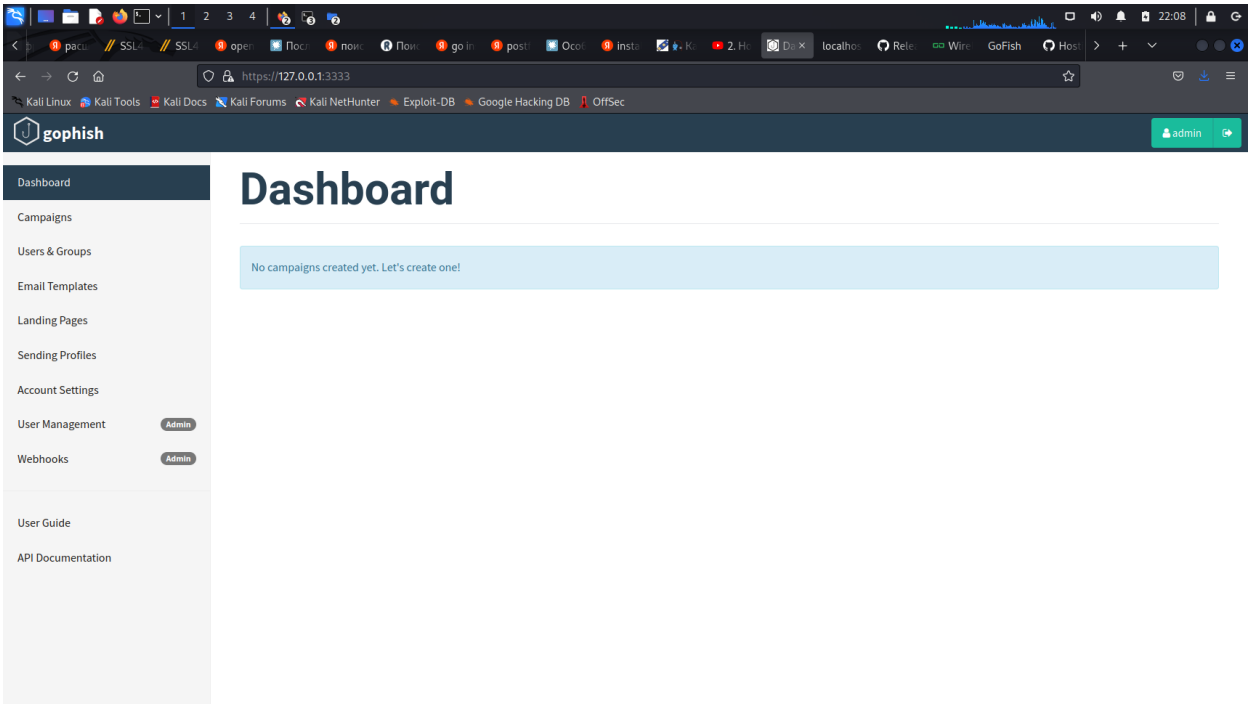


Рисунок 2 localhost

Произвели покупку домена:

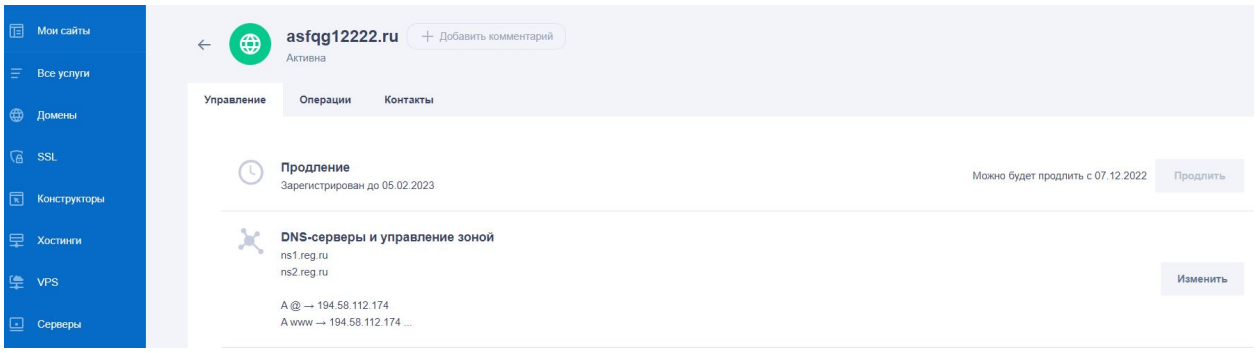


Рисунок 3 Домен на REG.ru

После создали письмо с, прилагающемуся к нему, файлу. Содержание данного письма представляет собой обычное приглашение на ИТ мероприятие.

Уважаемые студенты,

Уведомляем вас о том, что ФГБОУ ВО «Уральский государственный педагогический университет» при поддержке ФГАУ «Ресурсный молодежный центр», АНО «Россия — страна возможностей». Министерства образования и молодежной политики Свердловской области реализует проект «Всероссийский педагогический хакатон «HackEducation 2.0».

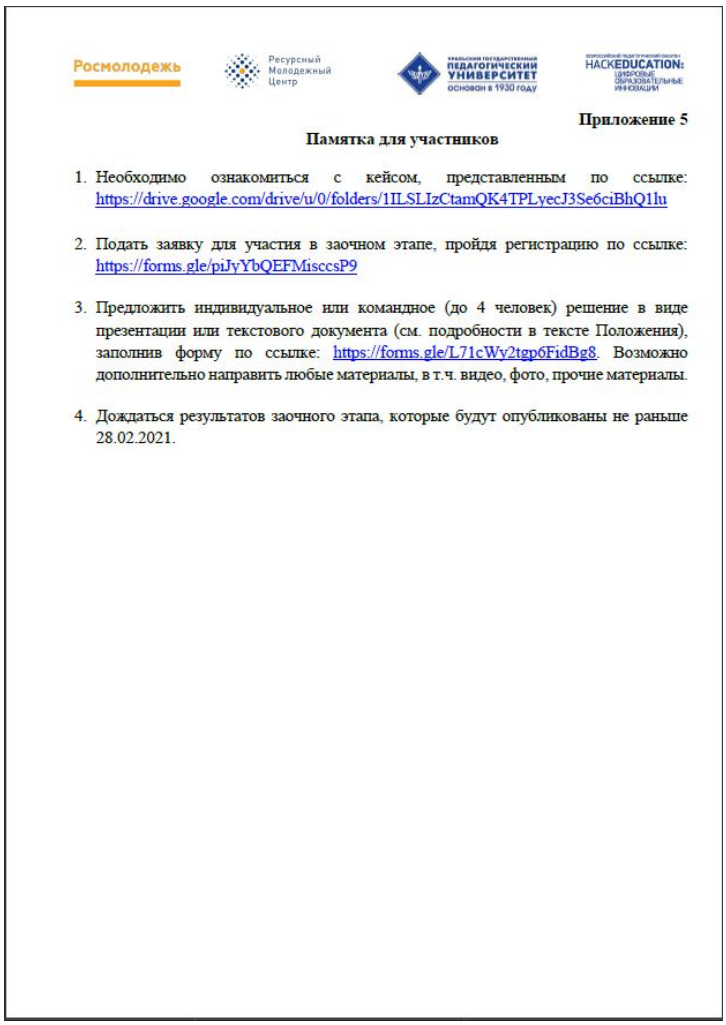
HackEducation 2.0 - педагогический хакатон для IT-разработчиков и педагогов в возрасте от 18 до 30 лет. Направлен на формирования условий взаимодействия для решения актуальных проблем и задач модернизации системы отечественного образования.

Хакатон представляет собой соревнование объединенных студенческих команд и включает в себя 2 этапа, в рамках которых необходимо представить собственную технологическую идею образовательного цифрового продукта, а также разработать прототип на основе идеи и презентовать его на публичной защите. Команды примут участие в лекциях от экспертов, менторских сессиях, партнерских активностях и мероприятиях.

В прикрепленный файлах вы можете ознакомиться с положением и памяткой для участников.

Более подробная информация по ссылке - https://vk.com/hackeducation

Рисунок 4 Текст письма



Росмолодежь

Ресурсный Молодежный Центр

ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ основан в 1930 году

HACKEDUCATION: ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ ИННОВАЦИИ

Приложение 5

Памятка для участников

1. Необходимо ознакомиться с кейсом, представленным по ссылке: https://drive.google.com/drive/u/0/folders/1ILSLIzCtamQK4TPLyecJ3Se6ciBhQ1lu
2. Подать заявку для участия в заочном этапе, пройдя регистрацию по ссылке: https://forms.gle/piJyYbQEFMisccsP9
3. Предложить индивидуальное или командное (до 4 человек) решение в виде презентации или текстового документа (см. подробности в тексте Положения), заполнив форму по ссылке: https://forms.gle/L71cWy2tgp6FidBg8. Возможно дополнительно направить любые материалы, в т.ч. видео, фото, прочие материалы.
4. Дождаться результатов заочного этапа, которые будут опубликованы не раньше 28.02.2021.

Рисунок 5 Файл в закрепе

Данный файл необходимо было сконвертировать через canarytoken, создав тем самым скрипт, который отошлёт нам информацию о запущенной системе. Конвертирование показано на рис 6., а его срабатывание на рис. 11.

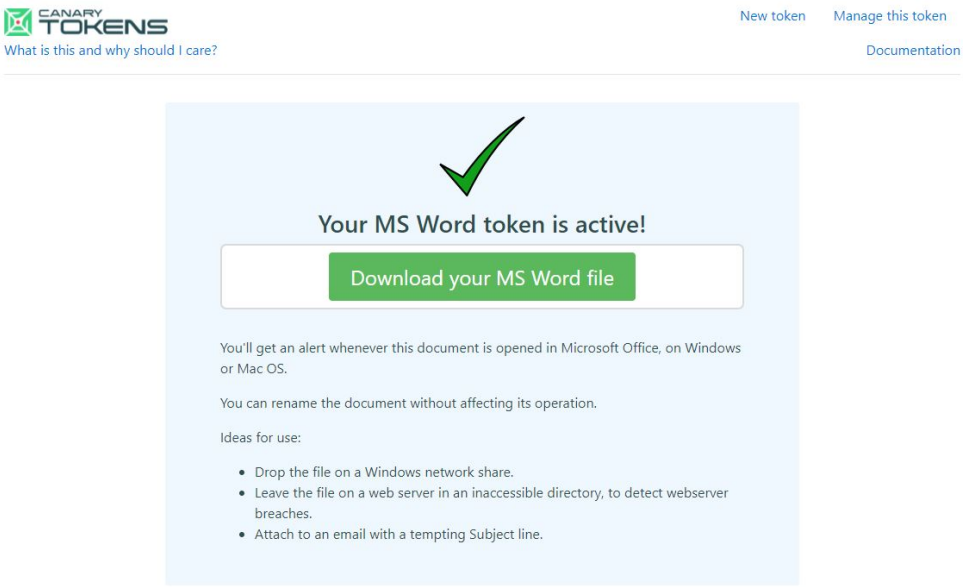


Рисунок 6 Создание токена

Далее была произведена настройка отправителя и сообщения в gobhish, после чего предприняли попытку выслать тестовый email.

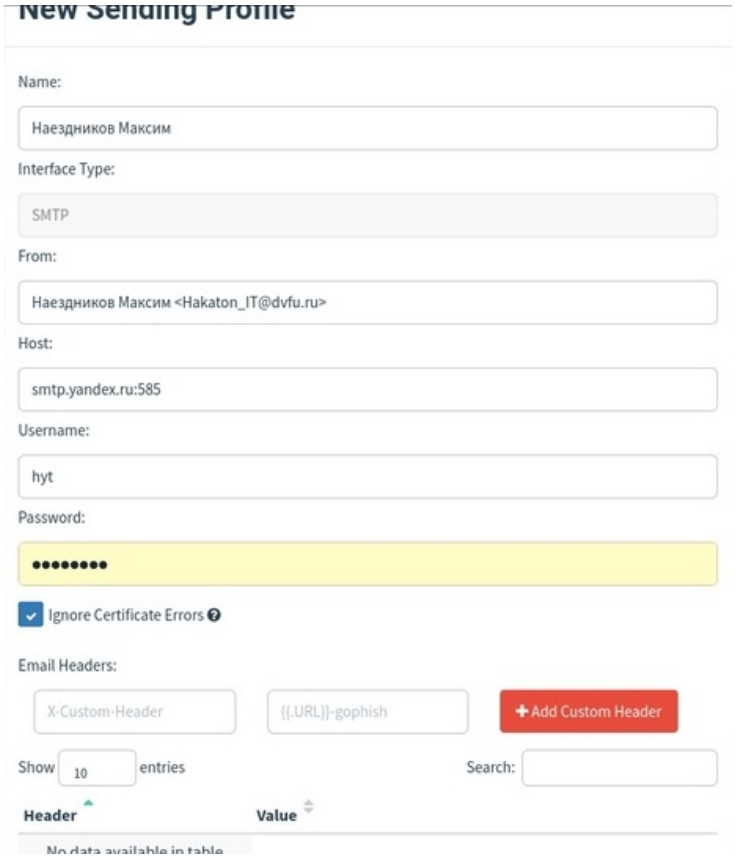


Рисунок 7 Отправитель

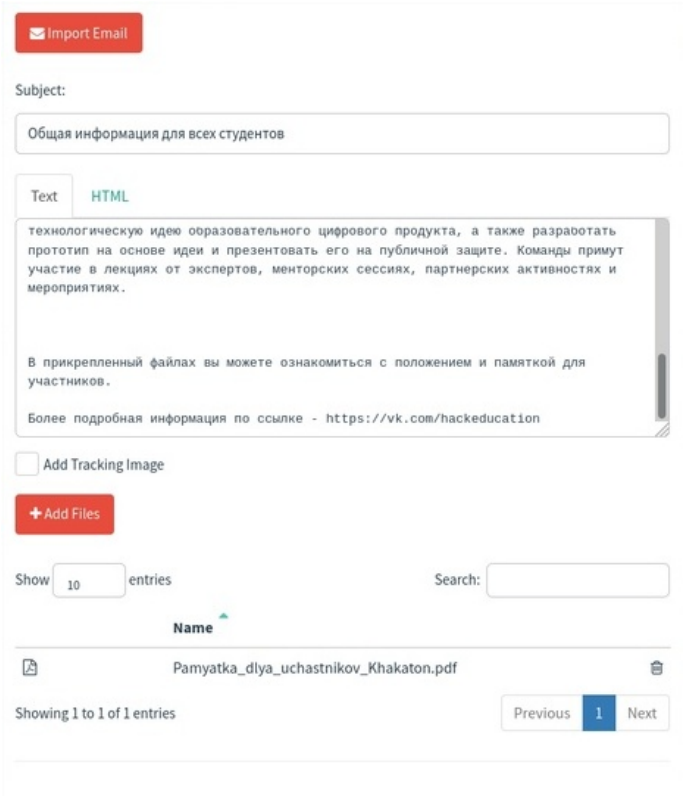
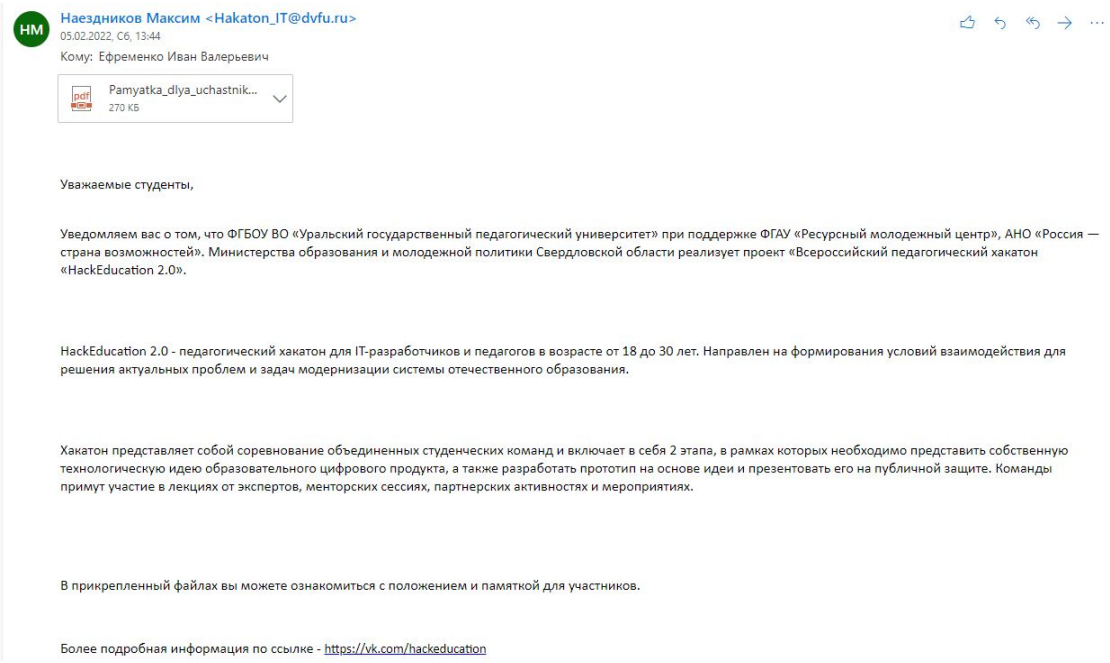


Рисунок 8 Сообщение

Данное сообщение пришло, но сразу же улетело в спам.



НМ Наездников Максим <Hakaton_IT@dvfu.ru>
05.02.2022, Сб, 13:44
Кому: Ефременко Иван Валерьевич

Pamyatka_dlya_uchastnik...
270 КБ

Уважаемые студенты,

Уведомляем вас о том, что ФГБОУ ВО «Уральский государственный педагогический университет» при поддержке ФГАУ «Ресурсный молодежный центр», АНО «Россия — страна возможностей». Министерства образования и молодежной политики Свердловской области реализует проект «Всероссийский педагогический хакатон «HackEducation 2.0».

HackEducation 2.0 - педагогический хакатон для IT-разработчиков и педагогов в возрасте от 18 до 30 лет. Направлен на формирования условий взаимодействия для решения актуальных проблем и задач модернизации системы отечественного образования.

Хакатон представляет собой соревнование объединенных студенческих команд и включает в себя 2 этапа, в рамках которых необходимо представить собственную технологическую идею образовательного цифрового продукта, а также разработать прототип на основе идеи и презентовать его на публичной защите. Команды примут участие в лекциях от экспертов, менторских сессиях, партнерских активностях и мероприятиях.

В прикрепленный файлах вы можете ознакомиться с положением и памяткой для участников.

Более подробная информация по ссылке - https://vk.com/hackeducation

Рисунок 9 Сообщение

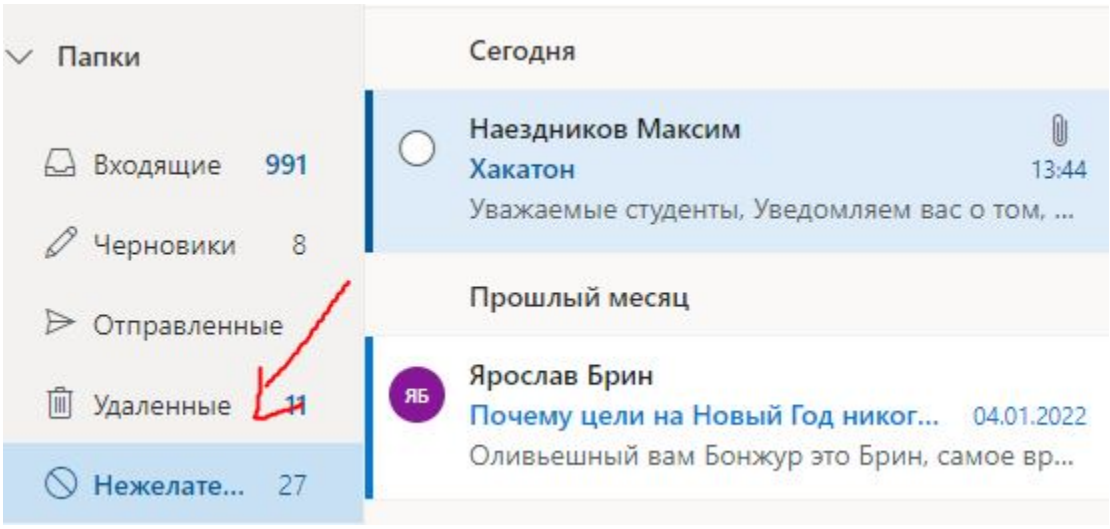
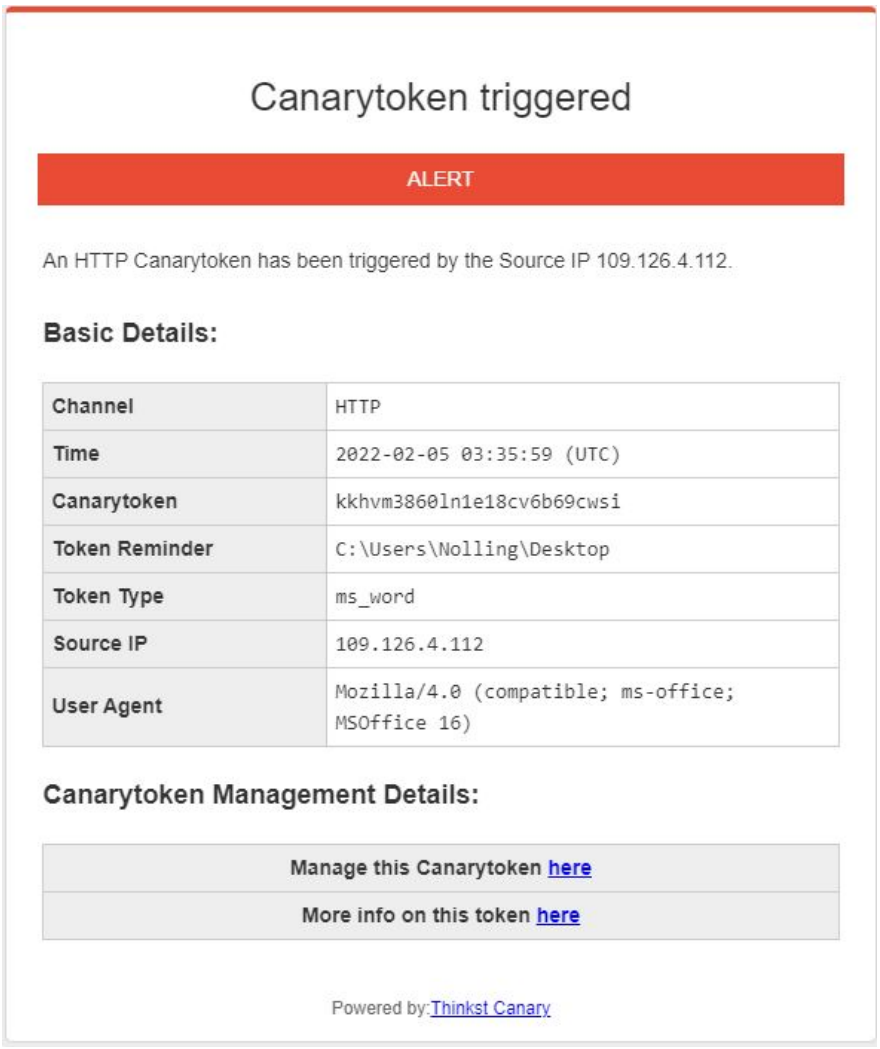


Рисунок 10 Спам

При открытии файла, срабатывает триггер, созданный на canarytoken.



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 109.126.4.112.

Basic Details:

Channel	HTTP
Time	2022-02-05 03:35:59 (UTC)
Canarytoken	kkhvm3860ln1e18cv6b69cwsi
Token Reminder	C:\Users\Nolling\Desktop
Token Type	ms_word
Source IP	109.126.4.112
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Powered by: Thinkst Canary

Рисунок 11 Его срабатывание