JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 15 (2020) 164-167
Received: 24 November 2019
Accepted: 10 December 2019

Analysis of the vulnerability of IT system users to a phishing attack

Analiza podatności użytkowników systemów informatycznych na atak phishingowy

Szymon Grzebielec*

Department of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract

This article presents an analysis of users' vulnerability to phishing attacks. The study was carried out using a self-prepared attack. A phishing attack was carried out on a group of 100 people. The subjects were divided into two groups of 50 people. The first group was attacked from a private, trusted account. The second group was attacked from a foreign email address. The attacked people were asked to complete the survey, its results and conclusions are presented in this article.

Keywords: network security; network attacks; phishing

Streszczenie

W niniejszym artykule przedstawiono analizę podatności użytkowników na atak phishingowy. Badania dokonano za pomocą samodzielnie przygotowanego ataku. Atak phishingowy przeprowadzono na grupie 100 osób. Badanych podzielono na dwie grupy po 50 osób. Pierwszą grupę zaatakowano z prywatnego, zaufanego konta. Drugą grupę natomiast zaatakowano z obcego adresu e-mail. Zaatakowane osoby poproszono o wypełnienie ankiety, jej wyniki oraz wnioski przedstawiono w niniejszym artykule.

Słowa kluczowe: bezpieczeństwo sieci; ataki sieciowe; phishing

*Corresponding author

Email address: szymon.grzebielec@live.com (S. Grzebielec)

1. Wstęp

W obecnych czasach można zauważyć szybki rozwój technologiczny oraz postępujący proces informatyzacji. Dotyczy to zarówno prywatnych przedsiębiorstw jak i administracji publicznej. Systemy teleinformatyczne są używane głównie do gromadzenia, przechowywania i przetwarzania danych. Ich szybkie i komfortowe użytkowanie jest możliwe między innymi za sprawą Internetu.

Rozwój Internetu oznacza, między innymi, że coraz większa liczba komputerów jest na stałe lub czasowo przyłączona do tejże sieci globalnej [1, 2]. Daje to określone korzyści, ale stwarza również i zagrożenia, których każdy użytkownik powinien być świadomy. Jednym z nieodłącznych ryzyk, które wiąże się z używaniem internetu jest możliwość naruszenia prywatności przez innych użytkowników sieci, którzy nie byli do tego uprawnieni. Zdobycie uprawnień do działania w określonym systemie komputerowym pracującym w sieci bez upoważnienia ze strony jego właściciela nosi nazwę „ataku".

Istnieje wiele rodzajów ataków sieciowych. Mogą być to ataki pasywne oraz aktywne [3]. Do najpopularniejszych z nich należą SQL Injection, phishing, broken authentication and session management czy DDoS attack [4].

Według danych CERT Polska ok. 280 tys. komputerów dziennie jest atakowanych przez hakerów na różne sposoby [5]. W związku z tak częstym zagrożeniem kradzieży danych zasadne jest badanie najpopularniejszych ataków, ich możliwości oraz świadomości użytkowników i ich podatności na próby kradzieży danych.

1.1. Phishing

Słowo phishing często jest tłumaczone jako łowienie haseł, co pochodzi od angielskiego zwrotu password harvesting fishing. Phishing jest formą ataku opartą na oszukaniu ofiary. Do powodzenia ataku niezbędna jest znajomość inżynierii społecznej. Napastnik używa socjotechniki aby nakłonić atakowaną osobę do wykonania pewnych działań. Zazwyczaj chodzi o zalogowanie się z podanego linku lub pobranie złośliwego oprogramowania. W taki sposób wyłudzane są dane osobowe, loginy i hasła do kont bankowych, portali społecznościowych, komunikatorów internetowych czy informacje dotyczące kart kredytowych [3]. Zwykle atakujący udają kogoś innego. Mogą udawać znajomych lub kogoś z rodziny ale także przedstawicieli prywatnych firm lub instytucji państwowych. Ataki phishingowe można podzielić na trzy typy. Są to spear phishing, clone phishing oraz whaling.

Spear phishing jest to atak skierowany konkretnie pod wybraną osobę, grupę ludzi czy przedsiębiorstwo. Przed dokonaniem ataku napastnik zbiera jak najwięcej informacji dotyczących swojej ofiary [6, 7].

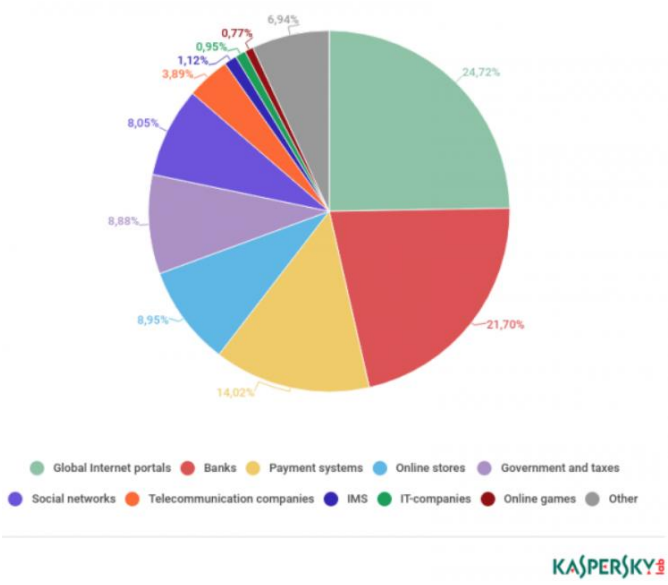
Clone Phishing jest takim rodzajem ataku phishingowego, w którym dostarczona, legalna wiadomość e-mail posiadająca załącznik lub link zostaje skopiowana. Skopiowana wiadomość jest używana do ataku a załącznik lub link zostaje zastąpiony złośliwym oprogramowaniem [8].

Whaling(ang. wielorybnictwo) jest to atak phishingowy spersonalizowany pod kadrę kierowniczą, managerów czy szefów firm lub korporacji. Zwykle jest to wiadomość e-mail

od osoby podszywającej się pod instytucję państwową czy kancelarię prawniczą [9].

Jedną z form phishingu jest przygotowanie strony internetowej imitującej inną stronę WWW na przykład banku lub portalu społecznościowego. Napastnik umieszcza na takiej stronie skrypt który przechwytuje dane logowania a następnie wysyła je na serwer lub adres e-mail atakującego.

Brak świadomości czym jest phishing, jak działa oraz brak umiejętności obrony przed tego typu atakiem może skutkować utratą wielu ważnych danych co z kolei może prowadzić do utraty pieniędzy. Według informacji udostępnionych na stronie www.prnews.pl tylko 36,7% badanych wie na pewno czym jest phishing [10]. Strona www.retruster.com udostępniła raport dotyczący phishingu na rok 2019 według, którego 90% naruszeń danych stanowi wyłudzanie informacji a liczba prób phishingu wzrosła w ciągu ostatniego roku o ok. 65% [11]. Jak podaje Kaspersky Lab najczęstszym obiektem ataków phishingowych w pierwszym kwartale 2019 roku były banki, stanowiły ponad 25% wszystkich ataków. W czołówce znajdują się rónież globalne portale internetowe oraz systemy płatnicze [12]. Na rys. 1. przedstawiono pełny wynik badania.



Rysunek 1: Rozkład organizacji narażonych na ataki phishingowe według kategorii w 1. kwartale 2019 r .[12].

Portal www.webroot.com podaje, że co miesiąc powstaje ok. 1,5 mln stron phishingowych [13]. Przytoczone badania pozwalają stwierdzić, że atak phishing jest niezwykle popularną oraz niebezpieczną formą ataku internetowego**.**

1.2. Metodyka badawcza

Badaniu został poddany atak phishingowy. Dokonano analizy tego ataku. W tym celu wykorzystano wcześniej przygotowaną stronę phishingową. Aby dokonać dokładniejszej analizy ataku phishingowego wykonano go na grupie stu osób. Badane osoby podzielono na dwie grupy po 50 osób. Pierwszą grupę zaatakowano z prywatnego, zaufanego konta. Było to konto na portalu społecznościowym Facebook użytkownika znanego badanym. Użyto socjotechniki wysyłając wiadomość o treści: "Cześć, biorę udział w konkursie i potrzebuję twojej pomocy. Wystarczy, że klikniesz w www.facebook-konkursy.eeu.pl i oddasz głos na mój komentarz. Z góry dziękuję za pomoc." Drugą grupę zaatakowano z obcego adresu e-mail, nieznanego badanym. Użyto socjotechniki wysyłając wiadomość z adresu e-mail Konkursy.Facebook2019@gmail.com o treści: "Witaj, zostałeś wylosowany w naszym konkursie i masz szanse wygrać Iphone 10s. Wystarczy, że klikniesz w podany link i będziesz postępować według wskazówek. Nie czekaj klikaj w www.facebookkonkursy.eeu.pl i ciesz się nowym telefonem." Następnie badanych poinformowano o fakcie wykonania na nich ataku, poinstruowano jak się przed nim zabezpieczyć oraz zapewniono ich, że ich dane nie zostaną nigdzie udostępnione a atak przeprowadzono tylko dla celów naukowych. Potem poproszono badanych o wypełnienie ankiety na temat przeprowadzonego ataku phishingowego. W ankiecie wzięły udział 93 osoby ze 100 zaatakowanych, 50 respondentów zaatakowano z zaufanego konta, natomiast 43 z obcego adresu e-mail.

1.3. Stanowisko badawcze

Do przeprowadzenia badań użyto komputera typu laptop o następujących parametrach:

- dostęp do Internetu,
- procesor Intel Core I5 2,3 GHz,
- pamięć RAM 8GB,
- karta graficzna NVIDIA GeForce GTX 1050, 4096 MB DDR5,
- system operacyjny Windows 10

2. Eksperyment

Celem przeprowadzenia badań naukowych było przeanalizowanie podatności użytkowników na atak phishingowy. Badanie przeprowadzono na podstawie samodzielnie wykonanego ataku. W przedstawionym eksperymencie dokonano ataku na portal społecznościowy Facebook. Według danych StatCounter Facebook we wrześniu 2019 roku miał udział w światowym runku mediów społecznościowych na poziomie 72,94% co czyni go najpopularniejszym medium społecznościowym na świecie. W Polsce ten odsetek wynosił 75,79% [14]. Zważając na ten fakt wybrano go do przeprowadzenia ataku.

W początkowej fazie eksperymentu przygotowano oraz przetestowano stronę internetową podszywającą się pod portal społecznościowy Facebook (rys. 2.). Strona została umieszczona na darmowym serwerze.

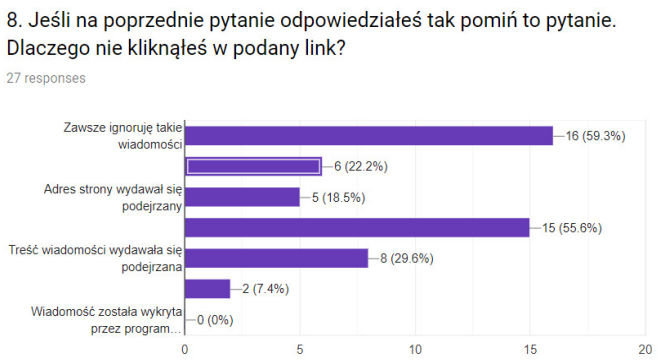
Rysunek 2: Strona phishingowa.

Po próbie logowania z utworzonej strony, dane logowania zostały wysyłane na serwer. Zapisywano je w pliku logi.txt. Na rysunku 3. pokazano wyniki testu logowania.

Rysunek 3:Plik logi.txt.

Po przeprowadzeniu testów wykonano atak na grupie 100 osób. Badanych podzielono na 2 grupy po 50 osób. Pierwszą grupę zaatakowano z prywatnego, zaufanego konta a drugą z obcego adresu e-mail. W wyniku przeprowadzonego ataku 8% badanych padło jego ofiarą. Następnie przeprowadzono ankietę wśród zaatakowanych osób. Respondentom zadano 12 pytań.

Według wyników ankiety 87,5% badanych spośród tych, którzy padli ofiarą ataku zostało zaatakowanych z prywatnego konta. Używając do ataku obcego adresu e-mail napastnik podszywał się pod organizatora konkursu. Badanie pokazało, że 59,3% respondentów ignoruje takie wiadomości a 22,2% badanych w ogóle ignoruje wiadomości od obcych (rys. 4.)



Rysunek 4: Wyniki ankiety na temat przeprowadzonego ataku phishingowego z obcego adresu e-mail.

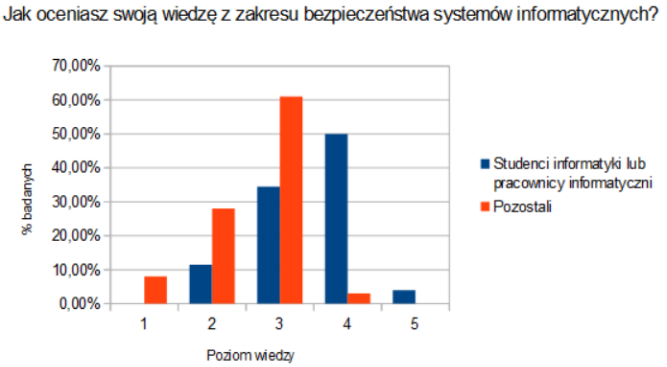
Pozwala to stwierdzić, że większe prawdopodobieństwo ataku phishingowego istnieje przy użyciu zaufanego konta. Używanie obcego adresu e-mail może być nieskuteczne ze względu na ignorowanie wiadomości przez odbiorców.

Spośród osób, które padły ofiarą ataku tylko 14% wiedziało czym jest phishing natomiast 86% osób nie widziało lub nie było pewne. Respondentów zapytano jak oceniają swoją wiedzę z zakresu bezpieczeństwa systemów informatycznych w skali od 1 do 5, gdzie 1 to brak wiedzy natomiast 5 to ekspert. Odpowiedzi osób, które padły ofiarą ataku pokazano na rysunku 5.

Rysunek 5: Poziom wiedzy osób, które padły ofiarą ataku.

Jak widać na rysunku 5. poziom wiedzy jest niski. Ponad 70% respondentów oceniło go jako poniżej przeciętnej. Żadna z badanych osób nie uważa, że poziom jej wiedzy na temat bezpieczeństwa systemów informatycznych jest wysoki. Wynik badania pozwala twierdzić, że brak wiedzy na temat phishingu oraz niski poziom ogólnej wiedzy z zakresu bezpieczeństwa systemów informatycznych ma wpływ na wyższą podatność użytkownika na atak phishingowy.

Respondentów zapytano czy studiują informatykę lub pracują na stanowisku informatycznym. Twierdząco odpowiedziało 28% z nich. Wśród osób, które padły ofiarą ataku nie znalazł się ani jeden student informatyki lub pracownik stanowiska informatycznego. 80,7% studentów informatyki i pracowników informatycznych deklaruje, że wie czym jest phishing. Wśród pozostałych natomiast taką wiedzę deklaruje jedynie 20,9%. Studenci informatyki i osoby pracujące na stanowiskach informatycznych znacznie lepiej oceniają swoją wiedzę z zakresu bezpieczeństwa systemów informatycznych w porównaniu do pozostałych. Zostało to zaprezentowane na rysunku 6.



Rysunek 6: Porównanie poziomu wiedzy studentów informatyki lub pracowników IT oraz pozostałych osób.

Wyniki uzyskane w kwestionariuszu pokazują, że ponad połowa studentów informatyki lub pracowników stanowisk informatycznych deklaruje swój poziom wiedzy powyżej przeciętnej, 4% nawet uważa się za eksperta w dziedzinie bezpieczeństwa a tylko 11,5% z nich ocenia swój poziom wiedzy poniżej średniej. Sytuacja wygląda inaczej wśród pozostałych badanych. Większość z nich czyli 61% uważa swoją wiedzę za przeciętną a tylko 3% z nich ocenia swoją wiedzę na 4 w skali do 5. Nikt z nich nie uważa się za eksperta w tej dziedzinie. 8% z pozostałych badanych deklaruje kompletny brak wiedzy z zakresu bezpieczeństwa systemów informatycznych. Przytoczone wyniki badania pozwalają

twierdzić, że studia informatyczne oraz praca na stanowiskach związanych z informatyką ma znaczący wpływ na poziom wiedzy na temat bezpieczeństwa systemów informatycznych. Osoby te cechują się większą wiedzą z tego zakresu co jak wcześniej udowodniono przekłada się na podatność użytkownika na atak phishingowy. Z przeprowadzonych badań wynika, że im wyższa jest wiedza użytkownika na temat phishingu oraz ogólnego bezpieczeństwa systemów informatycznych tym jego podatność na atak phishingowy jest niższa.

Badanych pytano czy po przeczytaniu wiadomości kliknęli w podany link. Wśród osób, które zadeklarowały wiedzę powyżej średniej (4 albo 5 w skali od 1 do 5) odsetek osób, które kliknęły w proponowany link był niższy od 1%. Na pytanie dlaczego nie kliknęli w podany link ankietowani odpowiadali, że adres strony wydawał się podejrzany- 76% oraz, że treść wiadomości wydawała się podejrzana- 24%. Wynik badania pokazuje, że osoby posiadające wysoką wiedzę na temat bezpieczeństwa systemów informatycznych zachowują większą czujność podczas korzystania z Internetu co przekłada się na ich mniejszą podatność na atak. Wynik tego badania potwierdza wcześniej wyciągnięte wnioski

3. Wnioski

Celem badania prezentowanego w niniejszym artykule była analiza podatności użytkowników na atak phishingowy. W wyniku przeprowadzonego na 100 osobach ataku 8% badanych padło jego ofiarą.

Korzystając z internetu jesteśmy narażenie na liczne ataki mające na celu kradzież naszych danych, loginów, haseł, wiadomości. Możemy stać się ofiarą jednego z nich na przykład ataku phishingowego. Osiągnięcie pełnego bezpieczeństwa systemu informacyjnego jest niemożliwe jednak korzystając z sieci Internet należy zachować szczególną uwagę. Nie należy logować się za pomocą linków wysyłanych przez nieznanych nadawców. Logując się do systemu należy zwracać szczególną uwagę czy link, z którego się logujemy jest poprawny(np. nie zawiera literówek, nie różni się od oryginalnego adresu strony). Atak phishingowy wykorzystuje podatność ofiary na socjotechnikę dla tego zalecane jest zwracać uwagę na treść oraz nadawcę otrzymywanych wiadomości. Większość badanych zwraca uwagę na adres linku, co może być powodem uniknięcia ataku phishingowego.

Większe prawdopodobieństwo powodzenia ataku phishingowego istnieje przy użyciu zaufanego konta niż w przypadku obcego adresu. Może mieć na to wpływ fakt, iż wiele osób ignoruje wiadomości otrzymane od nieznanych nadawców.

Badane osoby, które padły ofiarą ataku phishingowego nie widziały lub nie były pewne czym on jest oraz deklarowały niską wiedzę na temat bezpieczeństwa internetowego. Wiedzę większą niż przeciętna (powyżej 3 w skali 1-5) na temat biezpieczeństwa internetowego deklarowały jedynie osoby studiujące informatykę lub pracujące na stanowisku informatycznym.

Literatura

[1] https://www.wirtualnemedia.pl/artykul/22-miliardy-urzadzen-podlaczonych-do-internetu [28.10.2019]

[2] http://www.benchmark.pl/aktualnosci/ile-osob-ma-dostep-do-internetu-na-swiecie-juz-ponad-4-miliardy.html [28.10.2019]

[3] http://edu.pjwstk.edu.pl/wyklady/bdk/scb/main06.html [28.10.2019]

[4] https://devpark.pl/pl/najpopularniejsze-wedlug-owasp-rodzaje-atakow-sieciowych-i-jak-sie-przed-nimi-zabezpieczyc/ [28.10.2019]

[5] https://www.cert.pl/ [28.10.2019]

[6] https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/ [28.10.2019]

[7] https://www.secureworks.com/research/threat-group-4127-targets-google-accounts [28.10.2019]

[8] https://www.theregister.co.uk/2008/04/16/whaling_expedition_continues/ [28.10.2019]

[9] https://www.lifewire.com/what-is-whaling-2483605 [28.10.2019]

[10] https://www.prnews.pl [28.10.2019]

[11] https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html [28.10.2019]

[12] https://www.securelist.pl/analysis/7483,spam_i_phishing_w_2018_r.html [28.10.2019]

[13] https://www.webroot.com [28.10.2019]

[14] https://www.gs.statcounter.com/ [28.10.2019]