Phishing

Nikodem Kaczmarek, Patryk Garwol

10 grudnia 2023

Rysunek 1: Humorystyczne ukazanie Phishingu, Scott Adams, 2005

1 Wprowadzenie

2 Mechanizm działania phishingu

Phishing przypomina słowo fishing, w szczególności gdy skupimy się na wymowie. Nie jest to przypadek, ponieważ ataki tego rodzaju są w pewien sposób "łowieniem rybek"[6]:

→ wędkarz - przestępca

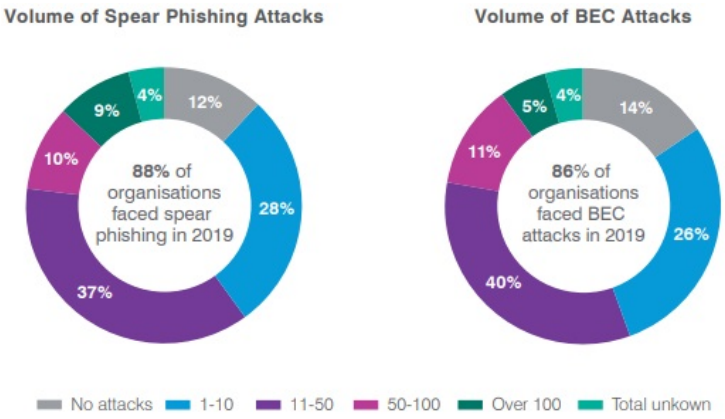
→ przynęta - wiadomość, szkodliwy link, fałszywa strona itp.

→ ryba - zasoby nieświadomej ofiary

Mowa tutaj zatem o inżynierii społecznej, czyli technice manipulacji, która wykorzystuje ludzkie błędy w celu uzyskania prywatnych informacji lub innych zasobów [7]. Zdarzają się również przypadki, w których przestępca jest na tyle złośliwy, że wykorzystując phishing instaluje na sprzęcie ofiary złośliwe oprogramowanie, które niekoniecznie służy do kradzieży danych. Oszustwa te wykorzystują najsłabsze ogniwo w świecie informatyki, czyli człowieka. Większość populacji, w szczególności osoby starsze - nie jest obeznana w kwestii informatyki [3], nie mówiąc już o cyberbezpieczeństwie. Łatwo jest wykorzystać ich niewiedzę, co w połączeniu z socjotechnikami daje atakującym dużo pola do popisu w kwestii doboru ich "przynęty".

Atak phishingowy może zostać przeprowadzony na nieokreślonych ofiarach. Atakujący wówczas liczą, że ktokolwiek "złapie się na haczyk". W dobie internetu bardzo łatwo jest wysyłać e-maile, lub nawet sms-y do niezliczonej liczby osób. Próg wejścia do zautomatyzowania takich procesów jest bardzo niski i ofiara nie potrzebuje lat nauki programowania, żeby do takiego ataku doprowadzić, ponieważ wystarczy zainstalować na komputerze IDE Pythona, a następnie poświęcić 5 sekund życia, aby znaleźć odpowiedni przewodnik, na przykład "How to Send Automated Email Messaged in Python"opublikowany w witrynie geeksforgeeks.org [4]. Czyni to ten proceder bardziej przerażającym, wiedząc jak proste jest to przedsięwzięcie. Zdecydowana osób nie nabierze się na e-mail przysłowiowego Księcia z Nigerii [12]. Jest jednak procent ludzi, które są podatne na ataki tego typu.

Groźniejszym rodzajem phishingu jest spear-phishing. Polega on na zaatakowaniu określonej osoby lub podmiotu, co rażąco wpływa na jego skuteczność. Ataki te są planowane dłuższy czas, aby dokładnie poznać słabe strony ofiary i tym sposobem zoptymalizować szanse powodzenia. Według raportu firmy Proofpoint z roku 2020, w roku 2019. 88% organizacji na świecie doświadczyło zagrożenia tego rodzaju. Spośród nich aż 55% stało się jego ofiarami [11].



Rysunek 2: Skala ataków phishingowych w 2019. roku wg. raportu Proofpoint

3 Wybrane narzędzia i techniki wykorzystywane przez oszustów

3.1 Inżynieria społeczna

Inżynieria społeczna została już przez nas wspomniana. Nazwa jest dość enigmatyczna, aczkolwiek sprowadza się do relatywnie prostej rzeczy - oszukanie człowieka. Kilka sposobów na osiągnięcie tego efektu to:

→ Pretexting - opiera się na budowaniu zaufania. Wymyślane są przeróżne scenariusze, których atakujący używają do nakłonienia ofiar, aby ujawniły informacje. Przestępca może użyć pretekstu, aby podszyć się pod personel IT i poprosić o dane logowania.

→ Podszywanie się pod kierownictwo - znane również jako CEO fraud, jest to połączenie spear-phishingu oraz pretextingu. Jak nazwa wskazuje, atakujący podszywa się pod przełożonego ofiary, przez co zdecydowanie łatwiej jest taką osobę nabrać .

→ Romansowe oszustwa - oszuści wykorzystują aplikacje (stricte randkowe) w celu znalezienia ofiary, aby następnie budować z nią romantyczną relację i w odpowiednim momencie zaatakować [1].

3.2 Spoofing

Spoofing odnosi się do fałszowania lub modyfikowania informacji w celu wprowadzenia w błąd lub oszukania odbiorcy co do prawdziwego źródła lub tożsamości nadawcy. Spoofing i phishing to de facto dwa różne sposoby ataku, jednakże często idą w parze. Warto tu nadmienić, że:

→ Atak spoofingowy **może** utworzyć grunt pod atak phishingowy

→ Atak phishingowy **nigdy** nie tworzy gruntu pod atak spoofingowy

Choć różnica między tymi atakami może być na pierwszy rzut oka niejasna, sedno motywacji wyżej wymienioncyh działań jest zgoła odmienne. Celem spoofingu jest podszywanie się pod czyjąś tożsamość, podczas gdy celem ataków phishingowych jest kradzież informacji [8]. Podszycie się może zostać osiągnięte na różne sposoby, m.in:

→ E-mail spoofing - atakujący tworzy adres e-mail, który przypomina ofiarze kogoś zaufanego, na przykład instytucję bankową lub kogoś z listy kontaktów.

→ Caller ID spoofing - spoofing telefoniczny - podobny do e-mail spoofingu, ale odnosi się do numeru telefonu, który wbrew intuicji - bardzo łatwo jest podrobić. "Dzieje się tak przez luki w używanych powszechnie protokołach VoiP, w których serwery mają gotowe rozwiązania do modyfikacji wyświetlanych nagłówków"[15].

→ DNS spoofing - "DNS (Domain Name System) to protokół, którego główna funkcja polega na tłumaczeniu łatwych do zapamiętania przez człowieka nazw domen na zrozumiałe dla komputerów dane liczbowe"[10]. Umiejętne zatrucie tego protokołu powoduje przekierowanie użytkownika do sfałszowanej strony.

3.3 Narzędzia automatyzujące

Narzędzia te zostały już przez nas wspomniane. Nie ma większego sensu rozwodzić się nad nimi, ponieważ ich nazwa tłumaczy działania w sposób wystarczający. Dostępność tego typu rozwiązań jest do tego stopnia, że podczas szukania rozwiązań do najzwyklejszych zagadnień języka programowania Python - natknęliśmy się na tutorial pokazujący jak wysyłać wiadomości przez aplikację WhatsApp, korzystając z krótkiego Pythonowego skryptu.

4 Cele ataków phishingowych

Cel ataków phishingowych nie różni się od innych rodzajów kradzieży, a więc mowa tu głównie o danych, pieniądzach - lub o obydwu [9]. Aby te cele osiągnąć, przestępcy skupiają się między innymi na zdobyciu:

→ Loginu i hasła do portali społecznościowych, banku, adresu e-mail itp. - tak wrażliwe dane otwierają przed atakującymi wiele możliwości, między innymi do autoryzacji na innych portalach, co znacznie zwiększa potencjalny łup.

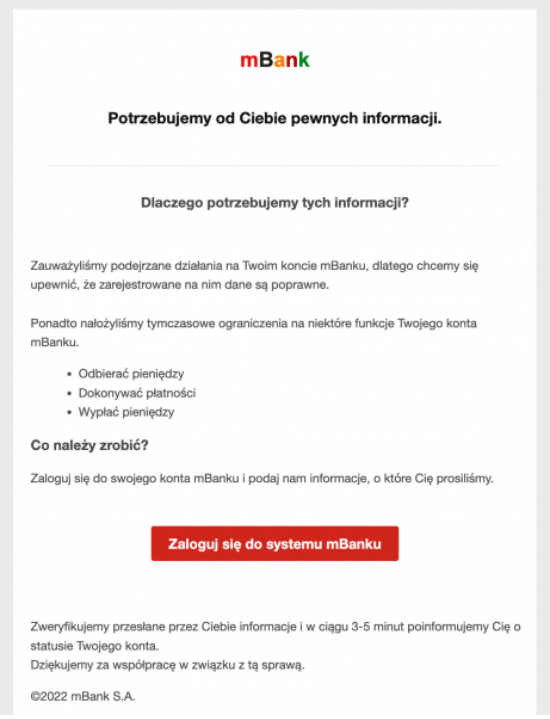
→ Danych finansowych - wiadomo - pieniądze są wtedy na wyciągnięcie ręki

→ Loginu i hasła do kont firmowych - dostęp do wewnętrznego systemu firm, często aby ukraść dane i zażądać za nie okup. Nie brakuje takich przypadków. O kilku napiszemy więcej w sekcji **Studium przypadku: Znane ataki phishingowe**.

5 Sposoby identyfikacji phishingu

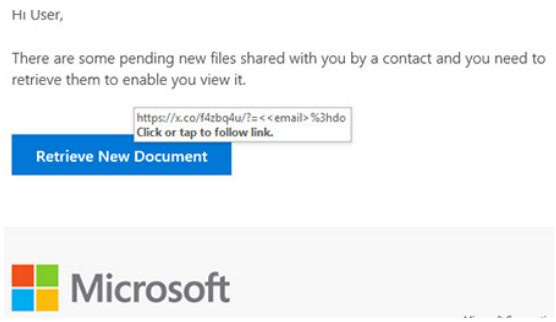
Phishing można zidentyfikować na wiele sposobów. Często ataki tego typu są przeprowadzone w sposób niedbały, co zdecydowanie ułatwia sprawę.

W przypadku maili konieczne jest sprawdzenie adresu. Nie jest to zawsze skuteczne, ponieważ system wysyłania poczty internetowej posiada wady i bardzo łatwo jest podszyć się pod kogoś, niezależnie od tego kim lub czym dana osoba albo instytucja jest [13]. Na szczęście niektóre serwisy (jak na przykład Gmail) radzą sobie z flagowaniem takich wiadomości. Innym aspektem, który warto wziąć pod uwagę również przy wiadomościach SMS jest pisownia. Poziom napisanej treści przez potencjalnego atakującego często odzwierciedla niską dbałość i pośpiech. Jeżeli wiadomość wygląda dobrze, należy się zastanowić - Czy wielki bank naprawdę potrzebuje moich dodatkowych danych? Jest to tak niezbędne do jego funkcjonowania?



Rysunek 3: Przykład ataku typu phishing, Niebezpiecznik.pl, 2022

W przypadku adresów URL ważną kwestią jest jego uważne sprawdzenie litera po literze, ponieważ różnice bywają ciężkie do dostrzeżenia. W pośpiechu może umknąć różnica pomiędzy małym L: "l", a wielkim i: "I". Wielkie "O"może przypominać "0"itd. Trudniejszymi przypadkami są ataki typu *IDN homograph attack*. Ich istota tkwi w tym, że alfabety posiadają litery, które są identyczne, jednakże ich kody *Unicode* się różnią. Dla przykładu alfabety: grecki, cyrylica, łaciński posiadają literę ⟨o⟩, która dla człowieka jest nierozróżnialna [14]. "Komputer"z rozróżnianiem liter nie ma najmniejszego problemu, stąd też da się go (a następnie ofiary) łatwo oszukać i zarejestrować domenę bliźniaczą do znanej, zaufanej przez potencjalną ofiarę. Bywa również, że między *hostem* a *subdomeną* brakuje kropki. Jest to znane jako *Doppelganger Domain* [5]. Należy uważać również na jaką stronę kieruje hiperłącze, ponieważ tekst hiperłącza niekoniecznie musi oznaczać, że jego atrybut *href* służący do wskazywania adresu docelowego - faktycznie wskazuje na pokazany adres.



Rysunek 4: Przykład fałszywego hiperłącza, digitalcheck.com, 2021

6 Rozpoznawanie phishingu przy pomocy nadzorowanego nauczania maszynowego

6.1 Zbiór danych

Za zbiór danych posłużył data set *Phishing Email Curated Datasets* [2]. Zawiera on 11 plików *csv*, które połączyliśmy w jeden.

6.2 Dobór parametrów

Przy rozpoznawaniu phishingu w wiadomościach e-mail kluczowe jest *body* wiadomości. Naturalnie znajduje się tam najwięcej treści, w tym *odnośniki* i *niebezpieczne słowa kluczowe*. W oparciu o podejmiemy się utworzenia klasyfikatora, który pod uwagę bierze 15 cech.

Niestety selekcja cech najbardziej liczących się jest trudna, a raczej - kosztowna. API, które prezentują wiele rozwiązań przydatnych do analizowanie m.

in domeny są płatne. Przy data secie liczącym 41 574 wiersze niemożliwym jest skorzystać z darmowych rozwiązań. Stąd też musieliśmy porzucić analizowanie takich cech jak:

→ wiarygodność certyfikatu SSL - w Pythonie istnieją moduły *ssl* i *socket*, które pomagają ustalić organizację wystawiającą certyfikat SSL. Problemem jest to, że w wielu przypadkach zwracany jest błąd requesta, także wynik nie byłby miarodajny. Trzeba by też było powoływać się na listę uznanych organizacji, która byłaby subiektywna.

→ liczba odwiedzin witryny

→ wiek domeny

W wyżej wspomnianych interfejsach programistycznych znajdują się także rozwiązania, które bezpośrednio zwracają informację, czy zadana domena znajduje się na czarnej liście, lub wykazuje skłonności do bycia zagrożeniem. Niestety wszystkojest za *paywallem*. Musieliśmy zatem analizować pobrane pliki *.csv* na podstawie charakterystyk odnośników URL i treści tematu, oraz *body* wiadomości e-mail. W ten sposób wyodrębniliśmy poniższe cechy:

→ ilość cyfr w nazwie nadawcy

→ ilość cyfr w domenie adresu nadawcy

→ długość domeny adresu nadawcy

→ ilość podejrzanych słów (na bazie subiektywnej listy) w temacie wiadomości

→ ilość podejrzanych słów w treści wiadomości

→ ilość odnośników URL w treści wiadomości

→ protokoły odnośników URL

→ informacja czy odnośnik zawiera IP

→ długości odnośników

→ informacja czy TLD zawiera tylko litery

→ poziom subdomeny

→ liczba wystąpień: "/", ".", "

→ informacja czy w odnośnikach znajdują się litery z alfabetu innego niż łaciński

6.3 Nauczanie

Po zmapowaniu wartości na liczbowe, podzieliliśmy zestaw na treningowy i testowy w proporcji 8:2. Sprawdziliśmy metodą *GridSearchCV* najlepsze parametry wybranych klasyfikatorów: *KNeighborsClassifier*, *LogisticRegression*, *DecisionTreeClassifier*, *RandomForestClassifier*, *SVM Classifier*. Najskuteczniejszy okazał się *RandomForestClassifier*, który osiągnął F1 na poziomie 0.89 i 0.93, odpowiednio dla klasy *safe* (oznaczającej bezpieczne e-maile) oraz *phishing*.

7 Skutki ataków phishingowych

8 Ochrona przed phishingiem

9 Studium przypadku: Znane ataki phishingowe

10 Przyszłość phishingu

11 Podsumowanie

Literatura

[1] abnormalsecurity.com. What is a social engineering attack? how they happen, why they work, and how to prevent them. *Abnormal Security Corp.*

[2] Anonymous. Phishing email curated datasets. *zenodo.org*, 2023.

[3] dsgi.wiley.com. The digital skills gap index (dsgi). *John Wiley and Sons, Inc*, 2021.

[4] gittysatyam. How to send automated email messages in python. *geeksforgeeks.org*, 2021.

[5] godaigroup.net. Doppelganger domains. *Godai Group*, 2011.

[6] gov.pl. Czym jest phishing i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz sms-y? *www.gov.pl*.

[7] kaspersky.co.uk. What is social engineering? *AO Kaspersky Lab.*

[8] Bart Lenaerts-Bergmans. Understanding the difference between spoofing vs phishing. *crowdstrike*, 2023.

[9] Jory MacKay. What data do cybercriminals steal? (how to protect yours). *IdentityGuard*, 2023.

[10] Netia.pl. Serwer dns – co to jest? do czego służy? *Netia*, 2020.

[11] proofpoint. 2020 state of the phish. an in-depth look at user awareness, vulerability and resilience. *proofpoint.com*, 2020.

[12] Maxwell Timothy. The nigerian prince scam has evolved: How to spot this phishing email. *makeuseof.com*, 2023.

[13] Dylan Tweney. How to fake an email from almost anyone in under 5 minutes. *Hackernoon.com*, 2017.

[14] Wikipedia.com. Idn homograph attack. *Wikipedia*, 2011.

[15] Tomasz Łużak. Spoofing – co to jest? jak się przed nim bronić? *Netia*, 2022.