Phishing

Nikodem Kaczmarek, Patryk Garwol

2 grudnia 2023

1 Wprowadzenie

[7]

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"[3]:

→ wędkarz - przestępca

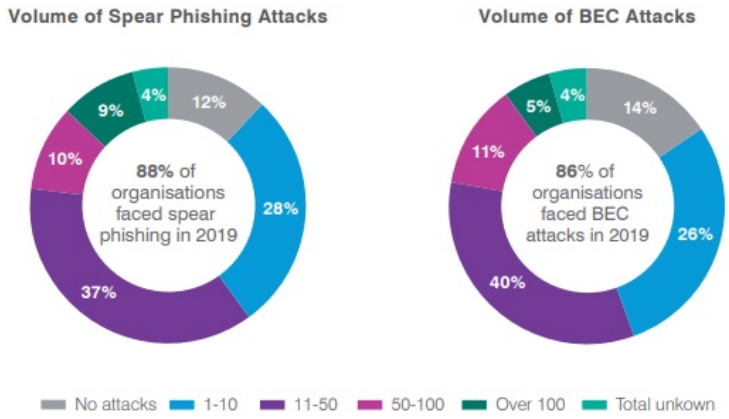
→ przynęta - wiadomość, szkodliwy link, fałszywa strona itp.

→ 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 [4]. 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 [1], 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 [2]. Czyni to ten proceder bardziej przerażającym, wiedząc jak proste jest to przedsięwzięcie. Zdecydowana osób nie nabierze się na e-mail przysłowiowego Księcia z Nigerii [6]. 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 [5].



Rysunek 1: Skala ataków phishingowych w 2019. roku wg. raportu Proofpoint

3 Narzędzia i techniki wykorzystywane przez oszustów

4 Cele ataków phishingowych

5 Sposoby identyfikacji phishingu

6 Skutki ataków phishingowych

7 Ochrona przed phishingiem

8 Studium przypadku: Znane ataki phishingowe

9 Przyszłość phishingu

10 Podsumowanie

Literatura

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

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

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

[4] kaspersky.co.uk. What is social engineering? *AO Kaspersky Lab*, -.

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

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

[7] Bob Violino. Phishing attacks are increasing and getting more sophisticated. here's how to avoid them. *cnbc.com*, 2023.