SANS SECURITY AWARENESS

Oszustwa bazujące na wiadomościach tekstowych

Wstęp

Jednym z najczęściej stosowanych sposobów w jaki cyberprzestępcy próbują oszukiwać swoje ofiary jest phishing za pośrednictwem wiadomości e-mail lub przy pomocy rozmów telefonicznych. Atakujący w dalszym ciągu poszukują nowych, kreatywnych sposobów oszukiwania ludzi. Warto wiedzieć, że ataki wykorzystujące wiadomości tekstowe oraz aplikacje takie jak iMessage/Facetime, WhatsApp, Slack lub Skype to żadna nowość. Poniżej zaprezentujemy kilka prostych wskazówek, które pomogą Ci zachować bezpieczeństwo oraz podpowiedzą w jaki sposób się ustrzec przed najpopularniejszymi atakami.

Czym są ataki wykorzystujące wiadomości tekstowe?

Ataki za pośrednictwem wiadomości tekstowych to wszelkie ataki, w których przestępcy do oszustw używają wiadomości tekstowych SMS lub komunikatorów tekstowych. Atakujący próbują wymóc na swojej ofierze otworzenie podejrzanego adresu internetowego lub przekonanie jej o zadzwonienie pod wskazany numer telefonu celem podania danych osobowych podszywając się chociażby pod bank. Tak jak w przypadku tradycyjnych ataków typu phishing, atakujący często wykorzystują emocje do podjęcia decyzji. To co sprawia, że ataki bazujące na wiadomościach tekstowych są niebezpieczniejsze od tych propagowanych wiadomościami e-mail, jest to że wydają się być bardziej osobiste a to sprawia, że bardziej im ufamy. Dodatkowo w ich przypadku w internecie jest mniej wskazówek oraz informacji opisujących czy wybrana wiadomość jest atakiem czy też nie. Dlatego ważne jest aby w momencie otrzymania wiadomości, która wydaje się być dziwna lub podejrzana zacząć od zadania sobie pytań: czy ta wiadomość jest prawdziwa, czy ma sens, dlaczego ją otrzymałem? Oto kilka najczęstszych wskazówek świadczących o tym, że możesz mieć do czynienia z atakiem.

Wiadomość, która bazuje na pilności, wymaga natychmiastowego działania.

Żądanie podania danych osobowych, hasła oraz innych wrażliwych informacji, do których ta osoba nie powinna mieć dostępu.

Czy wiadomość ma sens, czy może być prawdziwa? Jeśli nie brałeś udziału w loterii, to jasną sprawą jest to, że nie mogłeś jej wygrać, prawda?

Wiadomość pochodząca od współpracownika lub przyjaciela, lecz jej styl lub dobór słów nie pasuje do niego. Jeśli coś podejrzewamy zadzwońmy do tej osoby aby potwierdzić czy ktoś się pod nią nie podszywa. Jego konto mogło zostać skompromitowane i w tej sposób ktoś się za niego podaje lecz nim nie jest.

Jeśli otrzymasz wiadomość, która wywołuje u Ciebie silne emocje odczekaj moment, nie rób nic pod wpływem impulsu, przemyśl to na spokojnie.

Możemy spotkać się z atakami, które łączą w sobie oba rodzaje ataków: e-mail oraz wiadomości. Dobrym przykładem są oszustwa związane z kartami podarunkowymi. Atakujący wysyła wiadomość e-mail podając się za przyjaciela lub współpracownika z prośba o podanie numeru telefonu. Będąc w posiadaniu numeru, atakujący mogą wysyłać wiadomości SMS namawiające na zakup karty podarunkowej. Po zakupie karty, atakujący namawiają Cię pod różnymi powodami, abyś wysłał im zdjęcie kodu karty podarunkowej. Innym dobrym przykładem oszustwa jest otrzymanie wiadomości z treścią "Czy to Ty jesteś na tych zdjęciach? Sprawdź to, nie uwierzysz". Taka wiadomość budzi ciekawość. Jeśli znasz osobę która rzekomo wysłała tę wiadomość i masz podejrzenia co do jej wiarygodności, najlepszym rozwiązaniem będzie skontaktowanie się z osobą, która ją wysłała

Bądź podejrzliwym w stosunku do wszelkich wiadomości, szczególnie tych które wymagają od Ciebie natychmiastowego działania. Jeśli otrzymujesz wiadomość o problemie z kontem bankowym, z kartą kredytową, skontaktuj się bezpośrednio ze swoim bankiem lub firmą, która obsługuje Twoją kartę kredytową. Numer telefonu znajduje się na oficjalnej stronie internetowej banku lub na odwrocie karty kredytowej. Pamiętaj, że większość instytucji rządowych, podatkowych czy organy ścigania nie wysyłają SMSów.

Nasza czujność oraz logiczne myślenie jest najlepszą linią obrony przed wszelkimi atakami i oszustwami.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor gościnny

Jen Fox *zdobyła czarną odznakę podczas DEF CON 23 w kategorii Social Engineering. Zajmuje się zwiększaniem świadomości bezpieczeństwa komputerowego w firmie Dominos. Na Twitterze można znaleźć ją jako @j_fox.*

Źródła

Socjotechnika:	http://www.sans.org/u/XAQ
Powstrzymać phishing:	http://www.sans.org/u/XAV
Oszustwa telefoniczne oraz scam:	http://www.sans.org/u/XB0
Zgłaszanie oszustw:	https://www.consumer.ftc.gov/articles/0350-text-message-spam