OUCH! Kwiecień 2023

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Scareware: Historia

Ostrzeżenie! Twój komputer jest zainfekowany oprogramowaniem ransomware Black Basta. Zadzwoń natychmiast pod ten numer telefonu, aby naprawić to naprawić! *Czy gdybyś zobaczył to ostrzeżenie na swoim komputerze, zadzwoniłbyś pod podany numer telefonu?*

Atak

Po trzydziestu latach ciężkiej pracy Bożena zaoszczędziła wystarczająco dużo pieniędzy, aby przejść na emeryturę. Chcąc przejrzeć swoje konta, wpisała w przeglądarce nazwę swojego banku. Nie zdawała sobie sprawy, że popełniła pomyłkę w nazwie, przez to trafiła na inną stronę internetową, która wyświetlała przerażający baner, informujący o zainfekowaniu komputera. Komunikat zawierał również kontakt do pomocy technicznej. Wyskakujące ostrzeżenie wyglądało bardzo autentycznie. Zawierało szczegółowe informacje o złośliwym oprogramowaniu, które zainfekowało jej komputer, oficjalne logo firmy i numer telefonu, pod który mogła zadzwonić.

Bożena natychmiast zadzwoniła pod numer, który odebrała rzekoma pomoc techniczna. Przedstawiciel wyjaśnił, że jej komputer rzeczywiście został zainfekowany i że potrzebują do niego dostępu, aby go naprawić. Musiała wejść na stronę internetową, pobrać oprogramowanie, a następnie je zainstalować. Zrobiła wszystko zgodnie z instrukcją, a przedstawiciel pomocy technicznej poinformował ją, że mają dostęp do jej komputera i zaczęli lokalizować problem.

Wkrótce potwierdzili jej najgorsze obawy, nie tylko jej komputer został zainfekowany, ale okazało się, że włamano się na jej konto bankowe. Na szczęście firma zajmująca się pomocą techniczną miała bezpośredni kontakt z jej bankiem i szybko przekierowano ją do kolejnej osoby zajmującego się oszustwami. Operator zajmujący się oszustwami potwierdził, że jej konto rzeczywiście zostało przejęte i było wykorzystywane do przesyłania pieniędzy pochodzących z oszustw. Kazał jej natychmiast przelać wszystkie swoje pieniądze na inne konto bankowe, aby je chronić. Bożena wykonała polecenie. Następnie poinformował ją, że jej konto emerytalne również zostało przejęte. Na szczęście mieli również szybki kontakt z rządową agencją zajmującą się podatkami. Bożena została połączona z kolejnym operatorem, który wyjaśnił, że aby zabezpieczyć swoje konto emerytalne, musi przenieść wszystkie oszczędności na inne konto, zanim przestępcy uzyskają do nich dostęp. Zrobiła to. To była długa i bardzo nerwowa noc, ale Bożena była zadowolona, że nie tylko naprawiła swój komputer, ale także ochroniła pieniądze, przenosząc je na nowe, zabezpieczone konta. Wyczerpana poszła spać.

Następnego ranka zalogowała się na swoje nowe konto bankowe, aby uzyskać dostęp do swoich niedawno przeniesionych oszczędności, ale wszystkie pieniądze zniknęły. W panice zadzwoniła pod numer pomocy technicznej, z którym kontaktowała się poprzedniego dnia. Usłyszała tylko komunikat "abonent jest nieosiągalny". Wkrótce zdała sobie sprawę, że oszczędności całego jej życia przepadły. Po prostu oddała je przestępcom.

Jak tego uniknąć

Cyberprzestępcy nauczyli się, że najłatwiejszym sposobem na skuteczny atak jest po prostu pytanie. Scareware jest sposobem, w jaki przestępcy oszukują ludzi. Chcą, abyś myślał, że twój komputer jest zainfekowany, kiedy tak naprawdę nie jest. Następnie nakłaniają do podjęcia pochopnych działań, aby móc wykorzystać sytuację. Ta historia jest oparta na prawdziwych wydarzeniach, które przydarzyły się prawdziwym ludziom. Komputer Bożeny nigdy nie został zainfekowany, jednak przypadkowo odwiedziła niewłaściwą stronę internetową. Firma zajmująca się wsparciem technicznym nie była prawdziwą firmą, ale grupą cyberprzestępców. Zarówno agent bankowy jak i inni przedstawiciele byli po prostu różnymi członkami tej samej grupy zajmującej się wyłudzeniami. Gdy uda im się zacząć rozmowę przez telefon, spróbują wszystkiego, co możliwe, aby zdobyć pieniądze. Jak możesz się ochronić?

- Bycie nieufnym jest najlepszą obroną. Za każdym razem, gdy ktoś próbuje skłonić cię do podjęcia pochopnych działania, może to być próba ataku. Im większe poczucie pilności, tym większe prawdopodobieństwo ataku.
- Żadna legalna organizacja nie poprosi Cię o podanie hasła. Żaden bank nie poprosi Cię o przelew pieniędzy z konta.
- Nigdy nie używaj danych kontaktowych podanych w alercie lub wyskakującym okienku. Jeśli chcesz sprawdzić zasadność ostrzeżenia, zawsze korzystaj ze znanych Ci metod kontaktu, takich jak numery telefonów na wyciągu bankowym lub kartach kredytowych.

Jeśli uważasz, że padłeś ofiarą oszustwa finansowego, natychmiast zgłoś to organom ścigania i swojemu bankowi. Im szybciej to zgłosisz, tym większe prawdopodobieństwo odzyskania pieniędzy.

Źródła

Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Przeglądarki internetowe: https://www.sans.org/newsletters/ouch/browsers/
Działania na emocjach - o tym jak cyberprzestępcy oszukują:
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Ataki phishingowe: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz