OUCH! Wrzesień 2024

Biuletyn Bezpieczeństwa Komputerowego

Ataki z wykorzystaniem odwzorowanego głosu

Niespodziewana rozmowa telefoniczna: Historia oszustwa

Małgorzata, emerytowana nauczycielka spędzała spokojne poranki w swoim domu na przedmieściach. Pewnego dnia, gdy piła poranną kawę, odebrała telefon od wnuka Jakuba, który studiował w innym mieście. Poinformował swoją babcię, że miał wypadek samochodowy i pilnie potrzebuje pieniędzy, aby zapłacić za szkody i uniknąć kłopotów prawnych. W jego głosie słychać było panikę. Jeżeli nie dostanie pieniędzy od razu, może trafić do więzienia. Głos po drugiej stronie należał niewątpliwie do Jakuba – serce Małgorzaty zabiło mocniej. Bez zbędnych pytań poszła do swojego banku i przelała pieniądze na konto podane przez wnuka. Dopiero później tego samego dnia Małgorzata zadzwoniła do matki Jakuba. Chciała się dowiedzieć, jak radzi sobie wnuk. Wtedy dowiedziała się, że została oszukana. Rozmowa była podstępem: przestępca wykorzystał technologię klonowania głosu przy pomocy sztucznej inteligencji (AI), aby naśladować głos Jakuba, wywołując tym samym u Małgorzaty panikę.

Czym jest klonowanie głosu?

Klonowanie głosu ma miejsce wtedy, gdy ktoś używa sztucznej inteligencji do odtworzenia głosu danej osoby, uwzględniając jej intonacje i rytm mowy i tworzy niemal idealną replikę.

Atak polegający na klonowaniu głosu rozpoczyna się od zebrania przez cyberprzestępcę próbek dźwiękowych głosu ofiary. Próbki te można pobrać z różnych źródeł, takich jak filmy na YouTube lub TikToku. Sztuczna inteligencja generuje nowy dźwięk, który brzmi jak głos ofiary podszycia. Wygenerowany głos można wykorzystać na różne sposoby, od połączeń telefonicznych po wiadomości głosowe, co czyni go niebezpiecznym narzędziem.

Tworząc ataki polegające na klonowaniu głosu, cyberprzestępcy często najpierw przeprowadzają rekonesans. Większość potrzebnych informacji jest publicznie dostępna w mediach społecznościowych. Uwzględniają zarówno głos osoby, pod którą zamierzają się podszyć, jak i ofiarę, która będzie manipulowana wygenerowanymi wiadomościami. Cyberprzestępcy nie tylko dowiadują się, kogo znają i komu ufają ich ofiary, ale także jakie czynniki mogą okazać się najbardziej skuteczne. Wykonując te połączenia telefoniczne, cyberprzestępcy często używają spoofingu, więc gdy ofiara spojrzy na swój telefon, wydaje się, że połączenie telefoniczne pochodzi ze znanego numeru. ID dzwoniącego można łatwo sfałszować i trzeba mieć na uwadze, że informacja o dzwoniącym pojawiająca się na ekranie telefonu nie zawsze jest prawdziwa.

Chroń siebie

Pierwszym krokiem do zapewnienia sobie ochrony jest świadomość, że klonowanie głosu jest teraz możliwe i staje się coraz bardziej powszechne dla przestępców. Kluczowe kroki, które powinieneś podjąć w celu ochrony swoich danych:

- **Prywatność**:Bądź świadomy i ograniczaj informacje, które udostępniasz innym, oraz ograniczaj widoczność swoich nagrań w mediach społecznościowych.

- **Wskazówki**:Nie ignoruj sygnałów sugerujących, że coś jest nie tak. Ilekroć ktoś dzwoni do Ciebie z niezwykle pilną potrzebą lub wywiera presję, abyś natychmiast zareagował, najprawdopodobniej jest to oszustwo. Im większe poczucie pilności, tym większe prawdopodobieństwo, że ktoś będzie próbował skłonić Cię do popełnienia błędu. Innym typowym sygnałem jest sytuacja, kiedy coś wydaje się zbyt piękne, aby mogło być prawdziwe. Powinien również zastanowić telefon, który wydaje się po prostu dziwny.

- **Weryfikacja**: Jeśli nie masz pewności, czy połączenie telefoniczne jest prawdziwe, rozłącz się i oddzwoń do danej osoby na zaufany numer telefonu. Na przykład, jeśli zadzwoni do ciebie członek kadry kierowniczej wyższego szczebla lub współpracownik w Twojej firmie, oddzwoń pod numer, który jest używany przez daną osobę. Jeśli otrzymasz dziwny telefon od członka rodziny, spróbuj oddzwonić lub zadzwoń do innego członka rodziny, który dobrze go zna.

- **Kod**: Utwórz tajne hasło, które znasz tylko Ty i Twoja rodzina. W ten sposób, jeśli odbierzesz telefon, który wzbudzi podejrzenia, możesz sprawdzić za pomocą hasła, czy dana osoba jest zaufana, czy jedynie próbuje się podszyć pod kogoś, kogo znasz.

Redaktor gościnny

Maria Singh jest menedżerem w EnterpriseKC i zapalonym członkiem WiCyS z ponad 14-letnim doświadczeniem w zakresie technologii i cyberbezpieczeństwa. Posiada certyfikat SANS GIAC GSEC i ma tytuł magistra cyberbezpieczeństwa na Uniwersytecie Purdue. Jako była prezes Women in Security Kansas City i zdobywczyni nagrody OCA Corporate Achievement, Maria inspiruje kobiety w STEM i cyberbezpieczeństwie. Jej wystąpienia i przywództwo torują drogę przyszłym pokoleniom do rozwoju w tych dziedzinach.

Źródła

Trzy najczęstsze sposoby ataków: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Zatrzymaj oszustwa związane z połączeniami telefonicznymi: https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Działania na emocjach - o tym jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz