Biuletyn Bezpieczeństwa Komputerowego

Jak przestępcy kradną nasze dane

Cyfrowy koszmar: Kradzież danych Elizy

Eliza, utalentowany grafik komputerowy większość czasu spędza w Internecie. Zarządza bankowością, robi zakupy i utrzymuje kontakt ze znajomymi za pośrednictwem różnych stron i aplikacji. Pewnego dnia zauważyła na swoim koncie płatności w sklepach, których nigdy nie odwiedzała. W mediach społecznościowych na jej kontach zaczęły się pojawiać posty promujące dziwne produkty i usługi. Z kolei znajomi mówili jej o dziwnych e-mailach, które dostali z jej adresu.

Eliza zdała sobie sprawę, że straciła kontrolę nad swoim cyfrowym życiem. Ujawniono jej osobiste zdjęcia i prywatne rozmowy. Klienci zaczęli kwestionować jej wiarygodność, a jej reputacja bardzo ucierpiała. Po konsultacji z ekspertami ds. cyberbezpieczeństwa Eliza odkryła, że jej hasła zostały wykradzione. Przestępcy uzyskali dostęp do jej kont i wykradli wszelkie informacje, jakie udało im się znaleźć. Pytanie: jak to się stało?

Podstępne taktyki cyberprzestępców: pięć najbardziej powszechnych metod

Atakujący stosują różne techniki pozyskiwania haseł swoich ofiar. Oto pięć typowych sposobów, których mogli użyć w przejęciu haseł Elizy:

1. **Ataki socjotechniczne**

   Socjotechnika polega na tym, że napastnicy podszywają się pod osobę lub coś, co znasz lub komu ufasz, i nakłaniają Cię do zrobienia czegoś, czego nie powinieneś robić. Wysyłają e-maile lub wiadomości SMS, które wydają się prawdziwe, często wywołując silne poczucie pilności, strachu lub ciekawości.

   Jak to się stało: Eliza otrzymała e-mail, który wyglądał, jakby pochodził z jej banku. Wiadomość informowała o podejrzanej aktywności na koncie. W celu zweryfikowania tożsamości miała przejść do strony dostępnej pod wskazanym linkiem. Link prowadził do fałszywej strony internetowej, która zapisywała jej dane logowania, gdy je wpisywała w formularzu.

2. **Złośliwe oprogramowanie**

   Złośliwe oprogramowanie ma na celu infekowanie komputerów. Po zainfekowaniu urządzenia, cyberprzestępcy mogą mieć możliwość wykonania wielu niepożądanych czynności. Keylogger (czasami nazywany *information stealer*) to rodzaj złośliwego oprogramowania, które rejestruje każde naciśnięcie klawisza na urządzeniu, w tym login, hasła i inne wrażliwe dane.

   Jak to się stało: Eliza pobrała do swoich prac pakiet czcionek. W rzeczywistości był to keylogger, który zainstalowała na swoim komputerze. Przez dłuższy czas oprogramowanie zapisywało jej dane logowania do różnych kont i przesyłało je atakującym.

3. **Ataki brute force**

   W przypadku ataków brute force cyberprzestępcy korzystają z zautomatyzowanych narzędzi i próbują poznać hasło używając wiele kombinacji haseł. Słabe hasła są szczególnie podatne na tę metodę.

   Jak to się stało: Eliza od wielu lat używała prostych haseł takich jak "Eliza2020". Napastnicy korzystali z oprogramowania, które wykorzystywało popularne hasła i z łatwością poznawali hasła używane przez Elizę.

4. **Wyciek danych**

   Kiedy strona internetowa zostanie przejęta, może to mieć wpływ na konta wszystkich osób mających powiązanie ze stroną. Jeśli ktoś używa tego samego hasła do wielu kont i zostanie ono ujawnione, wówczas hasła tego można użyć również do uzyskania dostępu do innych kont ofiary.

   Jak to się stało: Na popularnej platformie, z której korzystała Eliza, doszło do wycieku danych. Ponieważ używała tego samego hasła do wielu kont, napastnicy uzyskali do nich dostęp.

5. **Kupno danych od innych przestępców**

   Cyberprzestępcy mogą po prostu kupić dane w Internecie, często w darknecie. Niektórzy przestępcy specjalizują się w kradzieży haseł ofiar przy użyciu dowolnej z metod, które omówiliśmy do tej pory. Następnie sprzedają skradzione hasła innym cyberprzestępcom.

   Jak to się stało: Przestępcy kupił na forum dane logowania ponad 100 000 przejętych kont. Dane jednego z kont Elizy znajdowało się na tej liście.

Trzy kroki, które możesz zrobić

Na szczęście wykonując trzy proste kroki, możesz znacząco poprawić bezpieczeństwo w sieci.

1. Używaj długiego, unikalnego hasła dla każdego ze swoich kont. Zalecamy hasła w formie zdań.
2. Użyj menedżera haseł, aby bezpiecznie przechowywać i zarządzać wszystkimi hasłami.
3. W miarę możliwości włączaj uwierzytelnianie wieloskładnikowe (MFA).

Redaktor gościnny

Lekshmi Nair jest starszym specjalistą ds. cyberbezpieczeństwa z 22-letnim doświadczeniem w zakresie bezpieczeństwa informacji i strategii cyberbezpieczeństwa. Obecnie jest dyrektorem ds. doradztwa w zakresie bezpieczeństwa aplikacji w BlackDuck Software. Jest założycielką i prezesem WiCyS India.

Źródła

Ataki polegające na klonowaniu głosu: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Ataki za pomocą wiadomości tekstowych: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/
Trzy sposoby ataków cyberprzestępców: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Siła haseł: https://www.sans.org/newsletters/ouch/power-passphrase/
Siła menedżerów haseł: https://www.sans.org/newsletters/ouch/power-password-managers/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz