OUCH! Czerwiec 2025

OUCH!

SANS SECURITY AWARENESS

Biuletyn Bezpieczeństwa Komputerowego

Obrona przed złośliwym oprogramowaniem

Niewinny e-mail z druzgocącymi konsekwencjami

Sara jest utalentowanym grafikiem, a jej źródło utrzymania uzależnione jest od jej laptopa. Pewnego popołudnia otrzymała e-mail od potencjalnego klienta. Temat otrzymanej wiadomości to: „Możliwość realizacji wartościowego projektu". Nazwisko nadawcy wydawało się znajome, być może przez polecenie przez stałego klienta. Chcąc poznać nowe możliwości pracy, Sarah otworzyła e-mail i znalazła w nim opis potencjalnego projektu oraz załącznik nazwany „ProjectBrief.pdf". Bez wahania kliknęła załącznik, licząc, że pozna szczegóły umowy.

Sara nie wiedziała, że to kliknięcie zapoczątkowało ciąg zdarzeń, które wkrótce miały zakłócić jej życie zawodowe i osobiste. Załącznikiem był sprytnie zamaskowany złośliwy program, który miał na celu zainfekowanie systemu. W kolejnych dniach Sarah zauważyła, że wydajność jej laptopa spadła, a aplikacje niespodziewanie się zawieszały. Zbagatelizowała te problemy, uznając je za typowe usterki techniczne, przypisując je intensywnemu użytkowaniu laptopa.

Jednak sytuacja wkrótce uległa zmianie. Kiedy Sara próbowała zalogować się do bankowości internetowej, aby sprawdzić stan swojego konta, okazało się, że nie ma dostępu do swojego konta bankowego. Wpadła w panikę, gdy zadzwoniła do swojego banku i dowiedziała się, że z jej konta wykonano przelewy na zagraniczne rachunki. Jej oszczędności, gromadzone przez lata ciężkiej pracy, zniknęły. Sara szybko zdała sobie sprawę, że padła ofiarą złośliwego oprogramowania, które zainfekowało jej laptop, wykradło dane logowania do bankowości, a potencjalnie także naraziło na szwank jej reputację zawodową.

Czym jest malware, czyli złośliwe oprogramowanie?

Malware to program komputerowy stworzony przez cyberprzestępców w celu infiltracji, uszkodzenia lub kontrolowania systemów lub urządzeń mobilnych bez zgody i wiedzy użytkownika. Termin ten jest połączeniem słów "*malicious*" i "*software.*" Prawdopodobnie słyszałeś o wirusach, robakach, trojanach, oprogramowaniu ransomware i oprogramowaniu szpiegującym. Są to rodzaje złośliwego oprogramowania.

Złośliwe oprogramowanie jest tak niebezpieczne, ponieważ, cyberprzestępca może przejąć całkowitą kontrolę nad urządzeniem, a właściciel urządzenia może się nawet o tym nie dowiedzieć. Atakujący może uzyskać informacje o wykonywanych działaniach, kontaktach, rozmowach, a także może uzyskać dostęp do danych logowania.

Złośliwe oprogramowanie może również niepostrzeżenie przechwycić wszystkie pliki, w tym zdjęcia, filmy i dokumenty. Może zainfekować niemal każdy system, smartfon, smartwatch, a nawet urządzenia w domu. Tak, nawet iPhone'y i komputery Mac mogą zostać zainfekowane, jeśli nie zostaną odpowiednio zabezpieczone.

Obrona przed malware: strategie ochrony

Na szczęście jest kilka prostych kroków, które możesz podjąć już teraz, aby zapobiec zainfekowaniu.

1. **Aktualizuj swój system**: Regularnie aktualizuj system operacyjny i aplikacje, aby mieć pewność, że zostały naprawione znane luki i zainstalowane najnowsze funkcje zabezpieczeń. Najprostszym sposobem, aby to zrobić, jest włączenie automatycznej aktualizacji.
2. **Zachowaj ostrożność w przypadku wiadomości e-mail**: Jednym z najczęstszych sposobów, w jaki cyberprzestępcy infekują Twoje urządzenia, jest nakłonienie Cię do otwarcia zainfekowanego załącznika, lub pobrania zainfekowanego oprogramowania. Uważaj na wiadomości, które wywierają presję, abyś natychmiast podjął działanie lub na te, które są zbyt dobre, aby mogły być prawdziwe.
3. **Silne, unikalne hasła**: Hasła są kluczem do bezpieczeństwa. Jeśli cyberprzestępca uzyska dostęp do haseł powiązanych z ważnymi kontami lub usługami, może przejąć nad nimi kontrolę. Zabezpiecz wszystkie swoje urządzenia unikalnym, silnym hasłem lub tzw. passphrase. Długość hasła ma znaczenie. W miarę możliwości włącz uwierzytelnianie wieloskładnikowe (MFA or 2FA).
4. **Pobieraj z zaufanego źródła**: Pobieraj oprogramowanie, multimedia i aplikacje wyłącznie z oficjalnych i renomowanych witryn. Częstą metodą infekowania urządzeń mobilnych przez cyberprzestępców jest nakłonienie użytkownika do pobrania nieautoryzowanych aplikacji mobilnych, których celem jest zainfekowanie złośliwym oprogramowaniem.
5. **Antywirus:** Jeśli to możliwe, zainstaluj zaufane oprogramowanie antywirusowe i w ustawieniach zaznacz, żeby było automatycznie aktualizowane. Nie wszystkie systemy i urządzenia mogą obsługiwać oprogramowanie antywirusowe, a program antywirusowy nie wykryje całego złośliwego oprogramowania, ale może pomóc.

Redaktor gościnny

Sherry Peng jest dyrektorem ds. prywatności w firmie Agora. Swoją karierę rozpoczęła w samorządzie lokalnym, a po uzyskaniu tytułu magistra w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa przeszła do sektora prywatnego. Sherry pracuje w sektorze bezpieczeństwa od prawie dziesięciu lat i jest prezeską WiCyS Colorado.

Źródła

Siła haseł: https://www.sans.org/newsletters/ouch/power-passphrase/
Siła menedżerów haseł: https://www.sans.org/newsletters/ouch/power-password-managers/
Siła aktualizacji: https://www.sans.org/newsletters/ouch/power-updating/
Jak przechytrzyć złośliwe aplikacje mobilne: https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps/

Polski przekład CERT Polska: Aleksandra Węgrzynowicz, Bartłomiej Wnuk