Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Phishing**
- **Scam**
- **Jak się chronić**

Phishing i oszustwa w e-mailach

EDYTOR GOŚCINNY

Pieter Danhieux jest edytorem gościnnym tego wydania biuletynu OUCH! Pracuje dla BAE Systems Stratsec w Australii (www.stratsec.net) i jest instruktorem kursów SANS Institute dotyczących testów penetracyjnych.

WSTĘP

E-mail to jeden z podstawowych sposobów w jaki się komunikujemy. Nie tylko używamy go codziennie w pracy, ale dzięki niemu pozostajemy w kontakcie z przyjaciółmi i rodziną. Ponadto e-mail jest używany przez firmy do kontaktu z klientem w takich sprawach jak potwierdzenie zakupów online czy przesłanie informacji o zmianach na koncie bankowym. Ponieważ ludzie tak bardzo opierają swoją komunikację na poczcie elektronicznej, stała się ona jednym z podstawowych narzędzi do dokonywania ataków. W tym numerze biuletynu zostaną wyjaśnione niebezpieczeństwa związane z wiadomościami e-mail i kroki jakie można podjąć aby się ochronić.

PHISHING

Phishing to jeden z najpopularniejszych ataków opartych o wiadomości e-mail. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy Internetowi próbują Cię oszukać i spowodować abyś podjął działanie zgodnie z ich zamierzeniami. Phishing do niedawna był terminem określającym atak przygotowany, aby wykraść dane do logowania do banku. Jednakże termin ten ewoluował i teraz odnosi się niemal do każdego ataku dokonanego poprzez e-mail. Atak taki rozpoczyna się odebraniem wiadomości e-mail, która wydaje się być od osoby lub instytucji której ufamy, takiej jak bank czy ulubiony sklep internetowy. Treść takiej wiadomości zazwyczaj zachęca użytkownika do podjęcia jakiegoś działania, na przykład kliknięcia w link, otwarcia załącznika albo wysłania odpowiedzi na wiadomość. Cyberprzestępcy przebiegle przygotowują treść takich e-maili i wysyłają je do tysięcy, a nawet milionów odbiorców na całym świecie. Doskonale wiedzą, że im więcej takich wiadomości roześlą, tym więcej osób będą mogli oszukać. Ataki typu phishing mają najczęściej następujące cele:

- **Wyłudzanie informacji:** Celem atakującego jest zmanipulowanie Cię tak, abyś kliknął na link, który zabierze Cię na stronę pytającą o login i hasło, Twój ulubiony kolor czy nazwisko panieńskie matki. Takie strony bliźniaczo przypominają na przykład znane strony banku, jednak są zaprojektowane tylko po to, żeby wykraść dane potrzebne do uzyskania dostępu do Twojego konta bankowego.
- **Przejęcie kontroli nad komputerem poprzez złośliwy link:** I tym razem celem cyberprzestępcy jest nakłonienie Cię do kliknięcia w link. Jednak w tym wypadku zamiast wyłudzenia informacji od

Phishing i oszustwa w e-mailach

Ciebie, celem jest zainfekowanie Twojego komputera. Jeśli klikniesz na taki link zostajesz przekierowany na stronę, która w tle przeprowadza atak na Twoją przeglądarkę internetową i kiedy atak ten się powiedzie, przestępca uzyskuje kontrolę na Twoim komputerem.

- **Przejęcie kontroli nad komputerem poprzez złośliwe załączniki:** Złośliwe wiadomości mogą zawierać zainfekowane załączniki, takie jak pliki PDF lub dokumenty Microsoft Office. Jeśli otworzysz taki załącznik, atakuje on Twój komputer i jeśli atak się powiedzie, przestępca uzyskuje nad nim kontrolę.

SCAM

Scam nie jest nowym zjawiskiem. Innymi słowy są to próby oszustwa i kradzieży. Klasycznym przykładem są wiadomości informujące o wygranej w loterii (mimo, że nigdy nie brałeś w niej udziału), albo że jakaś ważna osobistość potrzebuje przelać miliony dolarów do Twojego kraju i chciałaby Ci zapłacić za pomoc w tym transferze. Następnie zostajesz poinformowany, że musisz zapłacić opłatę manipulacyjną zanim otrzymasz pieniądze. Kiedy zapłacisz, już nigdy się nie odezwie.

JAK SIĘ CHRONIĆ

Zazwyczaj otwieranie wiadomości e-mail jest bezpieczne. W większości przypadków, aby atak się powiódł, to Ty musisz zrobić coś po przeczytaniu takiego e-maila (otworzyć załącznik, kliknąć w link lub odpowiedzieć na wiadomość). Kiedy po przeczytaniu wiadomości podejrzewasz, że jest to phishing albo scam, po prostu skasuj tę wiadomość. Poniżej znajduje się kilka wskazówek, jak rozpoznać, że otrzymana wiadomość to atak.

- Bądź podejrzliwy jeśli jakikolwiek e-mail wymaga natychmiastowego działania lub powoduje wrażenie pilności. To znany trick, aby zmusić ludzi do szybkiego działania.

Użyj zdrowego rozsądku. Jeśli treść wiadomości e-mail jest podejrzana lub zbyt obiecująca, najprawdopodobniej jest to atak.

- Bądź podejrzliwy w stosunku do e-maili adresowanych podobnie jak „Dear Customer” / ”Drogi Kliencie” lub w inny, bardzo ogólny sposób.
- Zwiększ czujność, jeśli w wiadomości znajdują się błędy w pisowni lub gramatyczne. Większość firm bardzo dokładnie formułuje swoje wiadomości, a przestępcy lubią korzystać z często niedokładnych, automatycznych translatorów.
- Jeśli link wydaje Ci się podejrzany, najedź na niego myszką (nie klikając). Wówczas ukaże się prawdziwy adres, pod który zaprowadziłby Cię ten odnośnik jeśli byś na niego kliknął. Link, który widzisz w wiadomości może być zupełnie inny niż miejsce, do którego rzeczywiście prowadzi.
- Nie klikaj na linki w wiadomościach. Zamiast tego najlepiej skopiuj link i wklej go bezpośrednio do paska swojej przeglądarki. Innym sposobem jest

Phishing i oszustwa w e-mailach

wpisanie nazwy strony do wyszukiwarki. Na przykład, jeśli otrzymałeś e-mail od firmy kurierskiej, że Twoja przesyłka jest gotowa do dostarczenia, nie klikaj na link. Zamiast tego odwiedź stronę firmy i wklej tam numer przesyłki skopiowany z wiadomości

- Bądź podejrzliwy jeśli wiadomość zawiera załącznik, szczególnie jeśli nie spodziewałeś się takiej wiadomości. Otwieraj tylko załączniki, których oczekiwałeś.
- To, że otrzymałeś wiadomość od znajomego, wcale nie znaczy, że on ją rzeczywiście wysłał. Jego komputer mógł zostać zainfekowany lub jego konto mogło zostać przejęte, a tę wiadomość wysyła złośliwe oprogramowanie do wszystkich z kontaktów z książki adresowej Twojego znajomego. Jeśli otrzymasz podejrzany e-mail od znanej i zaufanej osoby, skontaktuj się z nią w inny sposób i zapytaj czy rzeczywiście go wysłała.

Aby bezpiecznie korzystać z poczty elektronicznej, należy po prostu użyć zdrowego rozsądku. Jeśli coś wydaje się podejrzane lub zbyt obiecujące, to zapewne jest to atak. Dla bezpieczeństwa skasuj taką wiadomość.

ŹRÓDŁA

Niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL dla lepszej czytelności tekstu. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

Jak działa phishing:
http://preview.tinyurl.com/7xqf9bc

OnGuard Online – Jak uniknąć SCAMu (EN):
http://preview.tinyurl.com/6vfoljs

Anti-Phishing Working Group (EN):
http://www.apwg.org

Phishtank (EN):
http://www.phishtank.org

Definicje pojęć związanych z bezpieczeństwem (EN):
http://preview.tinyurl.com/6wkpae5

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

POLSKI PRZEKŁAD

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagownia 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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak and Paweł Jacewicz