Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Wstęp**
- **Czym jest phishing?**
- **Jak się chronić?**

Email i ataki phishingowe

REDAKTOR GOŚCINNY

Redaktorem gościnnym tego wydania biuletynu OUCH! jest Pieter Danhieux. Na stałe pracuje w BAE Systems Detica w Australii w Australii (www.baesystemsdetica.com.au). Jest także instruktorem kursów dla Instytutu SANS dotyczących testów penetracyjnych.

WSTĘP

Poczta elektroniczna, potocznie zwana emailem, jest jedną z podstawowych form komunikacji w sieci Internet. Używamy jej wszędzie, zarówno do komunikacji z przyjaciółmi i rodziną, jak i codziennie w pracy. Email stał się także jednym ze sposobów w jaki usługi internetowe komunikują się ze swoimi użytkownikami, np. potwierdzając realizację zakupów w sklepach online lub dostarczając wyciągi z kont bankowych. Jego popularność przyczyniła się do tego, że stał się jedną z podstawowych metod ataku stosowanych przez cyberprzestępców. W tym wydaniu omawiamy najpopularniejsze ataki wykorzystujące pocztę elektroniczną oraz przedstawiamy kroki, które pomogą się przed nimi zabezpieczyć.

- **Zbieranie informacji:** Cyberprzestępca stara się treścią wiadomości email nakłonić odbiorcę, aby kliknął w zamieszczony w niej link, który kieruje przeglądarkę internetową na stronę WWW proszącą o podanie danych takich jak: login i hasło, numer karty kredytowej, itp. Owa strona internetowa może do złudzenia przypominać stronę Twojego banku, popularnego sklepu internetowego lub serwisu pocztowego. Jest to zamierzone i ma pomóc przestępcy zyskać Twoje zaufanie i nakłonić Cię do wyjawienia poufnych informacji.
- **Infekcja komputera z użyciem złośliwych linków:** Ponownie treść wiadomości email zachęca do odwiedzenia pewnej strony internetowej. Jednakże tym razem przestępca nie stara się wyłudzić Twoich danych, ale zainfekować komputer. Po kliknięciu na link i odwiedzeniu strony WWW, w tle uruchamiane jest złośliwe oprogramowanie, które stara się zainfekować Twój system operacyjny i przekazać kontrolę nad nim przestępcy.
- **Infekcja komputera z użyciem złośliwych załączników:** Zdarza się, że otrzymana wiadomość phishingowa zawiera złośliwy załącznik, np. plik PDF lub dokument z pakietu MS Office. Jeżeli zdarzy Ci się otworzyć taki załącznik, może zostać uruchomiony złośliwy kod, który jest w nim zawarty. Jeśli atak się powiedzie, Twój komputer najprawdopodobniej zostanie zainfekowany.
- **Oszustwa:** Są to próby wyłudzeń. Sztandarowymi przykładami są tu powiadomienia o wygranej na loterii, fundacje proszące o wsparcie finansowe

Email i ataki phishingowe

w związku z niedawną klęską żywiołową lub ważne osobistości, które potrzebują pomocy w transferze milionów euro w zamian oferując część przelewanych pieniędzy. Nie daj się oszukać! Mają one wyłącznie na celu wyłudzenie Twoich oszczędności.

JAK SIĘ CHRONIĆ?

W większości przypadków otwarcie wiadomości email nie wiąże się z jakimkolwiek ryzykiem. Jedynie podjęcie akcji opisanej w treści wiadomości (np. otwarcie załącznika, kliknięcie w link lub przesłanie danych) może uruchomić ciąg zdarzeń, które spowodują, że atak się powiedzie. Jeżeli otrzymany email cechuje się jedną z poniżej wymienionych właściwości, może to oznaczać, że jest to próba ataku:

- Jeśli w treści wiadomości pojawiają się stwierdzenia o potrzebie podjęcia natychmiastowego działania należy być bardzo ostrożnym. Takie próby pospieszania użytkownika są bardzo powszechną metodą mającą na celu spowodowanie, że popełnimy jakiś błąd.
- Zwróć uwagę na formę powitania w treści emaila. Ogólne stwierdzenia typu "Szanowny Panie/Pani" nie powinny pojawiać się w wiadomościach od instytucji takich jak np. bank, które przecież znają Twoje dane. Email powinien być kierowany imiennie.
- Zwróć uwagę na błędy ortograficzne lub gramatyczne. Szanujące się przedsiębiorstwa nie dopuszczają do wysyłania wiadomości z błędami. Jeżeli email jest napisany niedbale i odnosisz wrażenie, że osoba, która go pisała mogła posłużyć się automatycznym tłumaczem, to jest to najprawdopodobniej próba ataku.
- Przesuń kursor myszki na link, ale nie klikaj w niego! Jeżeli Twój klient pocztowy ma taką funkcjonalność to powinien wyświetlić prawdziwy adres, na który dany link kieruje. Jeśli wyświetlany w treści emaila link różni się od tego, który pokazał klient pocztowy po najechaniu na niego myszką, może to oznaczać próbę ataku.
- Nie klikaj w linki. Skopiuj podany adres URL i wklej do paska adresowego przeglądarki. Zabezpieczysz się w ten sposób przed sfałszowanymi adresami URL, które wyglądając niewinnie kierują użytkownika na złośliwą stronę WWW.
- Bądź bardzo podejrzliwy wobec załączników, zwłaszcza jeśli się takowych nie spodziewałeś. Otwieraj tylko takie, na które czekałeś i pochodzą o zaufanych osób.

Zdrowy rozsądek to najlepsza metoda obrony. Jeśli treść wiadomości obiecuje nam "gruszki na wierzbie" jest to najprawdopodobniej próba wyłudzenia danych lub pieniędzy. Miej się na baczności!

Email i ataki phishingowe

- Nawet jeśli otrzymałeś email od znajomego, to wcale nie oznacza, że to właśnie on ten email wysłał. Jego komputer mógł być zainfekowany wirusem lub jego konto pocztowe mogło paść łupem cyberprzestępcy, a prawdziwym nadawcą wiadomości jest złośliwe oprogramowanie. Jeżeli otrzymałeś podejrzany i niespodziewany email od znajomego, zadzwoń do niego i upewnij się, że to naprawdę on go wysłał. Jeśli wiadomość zawierała rzekomy nowy numer telefonu pod którym możesz się skontaktować z nadawcą, nie używaj go. Zadzwoń na numer, który znasz i zweryfikowałeś wcześniej.

Jeśli po przeczytaniu wiadomości uznasz, że jest to próba ataku, zgłoś incydent poprzez formularz na stronie "Zgłoś incydent" (link poniżej), załącz podejrzany email oraz opisz zdarzenie - wystarczy kilka prostych zdań. Pomożesz w ten sposób Zespołowi Reagowania na Incydenty Naruszające Bezpieczeństwo Teleinformatyczne (CERT) ustrzec innych użytkowników sieci przed zagrożeniem. Pamiętaj, aby później usunąć taką wiadomość ze swojej skrzynki odbiorczej.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. 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.

Zgłoś incydent do CERT Polska -
http://preview.tinyurl.com/zglos-incydent

OnGuard Online (j. ang.) -
http://www.onguardonline.gov/phishing

Jak rozpoznać atak phishingowy (j. ang.):
http://preview.tinyurl.com/3c2axs8

OpenDNS Phishing Protect (j. ang.):
http://www.opendns.com/phishing-protection

Pojęcia z dziedziny bezpieczeństwa (j. ang.):
http://preview.tinyurl.com/6wkpae5

Porada dnia od SANS (j. ang.):
http://preview.tinyurl.com/6s2wrkp

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 reagowania 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
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski