Тенденції соціальної інженерії

Віталій Юрчук

ГО “Центр дослідження проблем регіонального і міжнародного співробітництва”, УКРАЇНА, м.Львів, вул. ген.Тарнавського, 1/40, E-mail: yuvian@ukr.net

Social engineering, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. Social engineering as an act of psychological manipulation had previously been associated with the social sciences, but its usage has caught on among computer professionals. Report includes description of the most common social engineering techniques and new trends, which are used by cybercriminals to deceive and swindle money from their victims.

Ключові слова – соціальна інженерія, персональна інформація, програмне забезпечення, техніки соціальної інженерії, соціальна мережа.

I. Вступ

У безпековому контексті "соціальна інженерія" розглядається як протизаконна діяльність, спрямована на отримання персональної інформації про людину без її свідомої згоди. Отримання особистих даних відбувається за допомогою маніпулювання свідомістю особистості, прихованого примушення її до виконання певних дій з метою розголошення нею необхідної зловмиснику інформації.

II.Основна частина

З розвитком інформаційно-комунікаційних технологій, та, зокрема, стрімким зростанням популярності соціальних мереж, як платформ для організації соціальних взаємовідносин, соціальна інженерія перейшла на принципово новий рівень розвитку.

Найбільш актуальним прикладом використання соціальної інженерії може бути створення невідомими особами у "Facebook" фальшивих сторінок Верховного головнокомандувача ОЗС НАТО в Європі адмірала Джеймса Ставрідіса. Створені сторінки використовувалися для введення в оману знайомих та родичів високопосадовця та виманювання конфіденційної інформації.

На відміну від хакерства, яке передбачає розробку програм несанкціонованого доступу до електронних ресурсів, техніки соціальної інженерії базуються на специфічних характеристиках процесу прийняття людиною рішення. Формулювання питань у повідомленнях або електронних листах відбувається таким чином, щоб стимулювати оприлюднення особою необхідної злочинцю інформації, яка полегшить доступ до її електронних фінансових ресурсів.

Аналіз статистики використовуваних технік соціальної інженерії вказує на продовження зловмисниками активного використання претекстингу, який передбачає розробку попереднього сценарію вивідування інформації.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Відпрацювання сценарію, як правило, передбачає володіння атакуючим мінімальної первинної інформації про особу (наприклад, дати народження, її фінансової активності протягом останнього часу тощо), використання якої при спілкуванні підвищує довіру людини. Найбільш широко претекстинг використовується у службах миттєвого обміну повідомленнями (наприклад, ICQ).

Протягом останніх років простежується позитивна динаміка використання фішингу, як однієї із різновидностей спаму. Особливістю фішингу є те, що електронний лист маскується під офіційний та надсилається від імені відомого бренду, банку, Інтернет-сервісу тощо. Лист містить посилання, перехід по якому здійснюється на фальшивий сайт, який імітує оформлення офіційної Інтернет-сторінки відповідної установи. Після переходу на сайт особі пропонується заповнити відповідні форми, тобто оприлюднити особисту інформацію (номера кредитних карток, паролі доступу до систем он-лайн платежів тощо). Протягом першого півріччя 2011 року масштаби використання фішингу у соціальних мережах зросли на 60,3%. Близько 78% всіх листів розсилалися від імені фінансових установ.

Починаючи з 2009 року зловмисниками активно використовується розповсюдження "непідконтрольного антивірусного програмного забезпечення" (Rogue Security Sofware). Це один із типів шкідливих програм, які класифікують себе антивірусними, проте, не є такими. Після закінчення процесу інсталяції на комп’ютер вони імітують його сканування та генерують фальшиві повідомлення про знайдені заражені об'єкти. Кінцевою метою імітації є виманювання грошей у жертви, якій пропонується купити ліцензійну версію програми. При "купівлі" програмного продукту жертва розкриває інформацію про свої електронні фінансові ресурси. Протягом першої половини 2011 р. спостерігалося зростання кількості "непідконтрольного антивірусного програмного забезпечення" сімейства "FakeRean" на 300%.

Висновок

Розвиток електронних платформ соціальних комунікацій призвів до стрімкого зростання використання зловмисниками технік соціальної інженерії для отримання персональної інформації про людину. Ефективна протидія проявам соцільної інженерії вимагає щонайменше навчання користувачів Інтернету базовим принципам безпеки роботи у мережі.

Література

1. Security Intelligence Report. Volume 11 // Microsoft – www.microsoft.com/sir/.
2. The Evolution of Malware and the Threat Landscape – a 10-Year review // Microsoft - www.microsoft.com/sir/.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua