УДК 004.056.53

Гермак В.С.
Кіровоградський національний технічний університет

Дослідження вразливостей та загроз в соціальних мережах

Завдяки соціальним мережам в суспільстві розпочалася епоха надмірної інформаційної відвертості, що в свою чергу породило на світ новітні методи соціальної інженерії, стеження і злому. Соціальні мережі сьогодні зачіпають практично кожен аспект нашого життя, і з кожним днем все більше людей викладають туди свою особисту інформацію. Більшість з нас викладають добровільно не лише свої дані, а й інформацію про своє оточення. Протягом останніх років сама концепція інформаційної безпеки значно розширилася, адже суспільство увійшло до ери надмірної інформаційної відвертості, прочинивши тим самим ящик Пандори, створивши мільйони нових погроз IT безпеці в мережі.

Основна проблема активних користувачів соціальних мереж в тому, що вони не замислюючись роблять своє особисте життя надбанням широкої публіки. При цьому, ніхто не може сказати напевно, хто дістане доступ до цієї інформації, а найголовніше, як саме він її використовуватиме. Які ж найголовніші загрози можуть підстерігати нас в соціальних мережах?

Сьогодні популярність соціальних мереж досягла неймовірних розмірів і це не залишилося непоміченим шахраями самих різних мастей. Окрім численного спаму в особистій пошті користувачів підстерігає і інша загроза – втрати облікового запису із-за злому. Зловмисник може зламати ваш обліковий запис з цікавості або в корисливих цілях. Якими ж методами злому зловмисники користуються найчастіше?

По перше далеко не завжди доводиться щось зламувати. Скільки б не з'являлося статей про те, як важливо підбирати надійний пароль, культура інтернет-безпеки в цілому залишається низькою. Користувачі інтернету вибирають одні і ті ж нехитрі кодові слова для різних сайтів, переходять по підозрілих посиланнях із спаму і принципово відмовляються від менеджерів паролів. Зазвичай зловмисники користуються наступними методами:

Фішинг. Користувача заманюють на сайт, який видає себе за справжній, і пропонують ввести пароль, який «витікає» до зловмисників. Фішинг нерідко організований вельми витончено. Введений пароль не тільки «витікає» до зловмисників, але і використовується для аутентифікації на справжньому сайті — наприклад, за допомогою JavaScript. Таким чином, з погляду користувача нічого страшного не відбувається: він вводить пароль і опиняється в своїй звичній стрічці друзів або в поштовій скриньці.

Шкідливе програмне забезпечення. Таке ПЗ розміщують на зламаних сайтах або засилають в недостатньо захищені системи. Шкідливе ПЗ потрапляє на комп'ютер користувача різними способами. Якщо зловмисники не займаються цільовою атакою на конкретну людину, а прагнуть заразити найбільше число комп'ютерів, то вони вважають за краще дістати доступ до популярних сайтів і упровадити в них шкідливий код. Найпривабливішими для зловмисників часто стають не самі сайти, а різні інструменти на них. Наприклад, це можуть бути рекламні мережі, бібліотеки JavaScript, різні API соціальних мереж і тому подібне. Зловмисники можуть навіть не зламувати такі сайти, а використовувати їх можливості по завантаженню призначеного для користувача контента: наприклад, рекламна мережа може дозволити завантажити flash-ролик. Тоді, якщо їм вдається обійти перевірку на безпеку, їх шкідливий контент буде

показаний в ході звичайної роботи сайту.

Соціальна інженерія. Іноді пароль вдається підглянути, а особливо довірливі користувачі можуть повідомити його зловмисникові самі: на цьому збудований цілий пласт системи інтернет-шахрайства.

Підбір пароля. Володіючи інформацією про користувача, яку легко знайти в соціальних мережах, можна спробувати вгадати пароль. Також можна автоматом перебрати величезну кількість варіантів, скориставшись асоціативною базою даних.

Вразливості сайтів - іноді зловмисники користуються помилками або недоробками на сайтах.

Як же і звідки можна дістати доступ до вашої системи зловмисникам? Як – запустивши в вашу систему різноманітне шкідливе ПЗ. Яким чином це шкідливе ПЗ може до вас потрапити – через зовнішні носії інформації; з інтернет сайтів, зокрема соціальних мереж (все, що просочується через браузер, використовуючи скрипти, уразливості браузера, уразливості системи); пошта; локальна мережа. Що ж саме загального у всіх джерел – це так звана точка входу, з якої починається будь-яке зараження шкідливим ПЗ. І це зовсім не інтернет, не зовнішні носії та інше, ні, першоджерело завжди користувач.

Практично не буває такого, щоб вірус завантажився сам по собі або пароль від аккаунта хтось непомітно вкрав, у 90% випадків користувач сам викачує сумнівний файл з пошти або переходить по посиланню з якимось рекламним текстом. Одними з ключових чинників подібних вчинків є невгамовна цікавість і необачність. Таким чином найефективніший спосіб, скажімо, злому аккаунтів - це соціальна інженерія, тобто метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкості людського чинника і вважається дуже руйнівним, бо достатньо, скажімо, просто досить хитро скласти лист і, використовуючи банальний людський чинник, отримати необхідні відомості, будь то пароль або щось ще. Адже, не дивлячись на те, що інформаційна безпека нескінченно удосконалюється, дані і об'єкти, що представляють інтерес для злому, захищають, перш за все, люди. Звичайні люди зі своїми страхами, забобонами, комплексами і слабкими місцями, на яких можна легко зіграти і виграти. Багато фахівців небезпідставно вважають, що в найближчому майбутньому соціальна інженерія почне представляти найбільшу загрозу, оскільки технічні засоби все більше і більше удосконалюються, а люди так і залишаються людьми.

Тому щоб уникнути зайвих проблем стримуйте свою цікавість, не переходьте по незнайомих посиланнях і не встановлюйте додатки створені невідомо ким.

Проте варто визнати, що не дивлячись на всі свої недоліки і підводні камені — соціальні мережі нікуди не подінуться, суспільство просто не зможе від них відмовитися. Необхідно всього-лише навчиться правильно і безпечно їх використовувати. Найголовніше, про що завжди варто пам'ятати — це контроль за тим, які дані ви довіряєте соціальній мережі. Адже все, що потрапляє в інтернет, залишається там назавжди.

Список використаних джерел

1. *Влияние через социальные сети / под общей ред. Е.Г. Алексеевой. – М.: Фонд «ФОКУС-МЕДИА», 2010.*
2. *Барсукова С.Ю. Вынужденное доверие сетевого мира / С.Ю. Барсукова // Полис: Политические исследования. – 2001. – № 2. – С. 52–60.*
3. *Гнидко К.О. Контроль потенциально опасного информационно-психологического воздействия на индиви-дуальное и групповое сознание потребителей мультиме-дийного контента / К.О. Гнидко, А.Г. Ломако // Труды СПИИРАН. – 2015. – Вып. 1(38). – С. 9-33.*