КІБЕРЗЛОЧИНИ В МЕРЕЖІ ШТЕРІШТ ЯК СПОСІБ ОТРИМАННЯ НЕЗАКОННОЇ ВИГОДИ

Никифорчук Дмитро Йосипович, доктор юридичних наук, професор, начальник кафедри оперативно-розШукової діяльності Національної академії внутрішніх справ
Лизогубенко Євген Віталійович, кандидат юридичних наук, викладач кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ

Із виникненням та популяризацією платних інтернет-сервісів (пошта, веб, хостинг) комп'ютерний андеграунд проявляє підвищений інтерес до отримання доступу в мережу за чужий рахунок, тобто за допомогою крадіжки логіна і пароля іншої людини (або декількох логінів і паролів із різних уражених комп'ютерів) шляхом застосування спеціально розроблених троянських програм.

На початку 1997 року в світі зафіксовано перші випадки створення і поширення троянських програм за допомогою яких вчиняються крадіжки паролів доступу до системи AOL (інтернет-провайдер America Online).

У 1998 році, з подальшим поширенням інтернет-послуг, аналогічні троянські програми з'являються і для інших інтернет-сервісів. Троянські програми даного типу, як і віруси, як правило, створюються особами, у яких немає коштів для оплати інтернет-послуг. По мірі здешевлення інтернет- сервісів зменшується і кількість троянських програм. Проте, досі такі «троянські» програми складають значну частину щоденних «надходжень» до лабораторій антивірусних компаній всього світу.

Злочинці також створюють троянські програми і інших типів, зокрема: програми, за допомогою, яких викрадають реєстраційні дані і ключові файли різних програмних продуктів, що використовують ресурси заражених комп'ютерів в інтересах свого «господаря» і, які крадуть персональну інформацію з мережевих ігор (ігрову віртуальну власність) з метою її несанкціонованого використання або перепродажу тощо.

Як свідчать результати досліджень найбільш небезпечна категорія авторів вірусів є хакери-одинаки або їх групи, які створюють такі шкідливі програми з корисливою метою. Наприклад, створення вірусів чи троянських програм для отримання коду доступу до банківських рахунків; або використовуючи ресурси зараженого комп'ютера несанкціоновано рекламують різні товари чи послуги тощо.

До основних видів кримінального бізнесу в мережі відносяться:

- розподілені мережеві атаки

У літературі окрім назви розподілені мережеві атаки використовуєтьсяя назва DDoS-атака (Distributed Denial of Service), тобто - розподілена відмова в обслуговуванні. Мережеві ресурси (наприклад, веб-сервера) мають обмежені можливості за кількістю запитів, одночасно обслуговуються. Дана кількість обмежена як потужностями сервера, так і шириною каналу, яким він підключений до Інтернету. Якщо кількість запитів перевищує допустиму, то робота з сервером значно сповільнюється або взагалі запити користувачів будуть «проігноровані».

В зв'язку з цим «хакери» ініціюють «сміттєві» запити на ресурси, які піддаються атаці. Кількість таких запитів значно перевищує можливості ресурсу-жертви. За допомогою «зомбі-мережі» організовується масована DDoS-атака на один або декілька інтернет-ресурсів, що призводить до відмови атакованих вузлів мережі. Тому звичайні користувачі не мають можливості отримати доступ до атакованого ресурсу. Як правило атака здійснюється на інтернет-магазини, інтернет-казино, букмекерські контори, інші компанії, бізнес яких безпосередньо залежить від працездатності своїх інтернет-сервісів. Найчастіше розподілені атаки відбуваються або з метою «знищити» бізнес конкурента, або з подальшою вимогою грошової винагороди за припинення атаки;

- створення мереж «зомбі-машин»

З метою функціонування подібних мереж створюються спеціалізовані троянські програми - «боти» (від «robot»), якими централізовано керує так званий «господар». Така троянська програма може управляватися до мільйонів комп'ютерів. Як наслідок, «господар зомбі-мережі» (або «бот- мережі») одержує доступ до ресурсів усіх заражених комп'ютерів і використовує їх у власних інтересах;

- дзвінки на платні телефонні номери або відправлення платних SMS-повідомлень

Особою (групою осіб) створюється і поширюється спеціальна програма, що здійснює несанкціоновані користувачем телефонні дзвінки або відправлення SMS-повідомлень із мобільних телефонів. Заздалегідь або паралельно із зазначеним ті ж особи реєструють компанію, від імені якої укладається договір із місцевим телефонним провайдером про надання платного телефонного сервісу. Провайдер не інформується, що дзвінки будуть здійснюватись без відома користувача. Надалі програма здійснює дзвінки або відправляє Sms а, телефонна компанія виставляє рахунки на номери, з яких надійшли дзвінки, і відраховує зловмисникові обумовлену в контракті суму.

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ НОРМАТИВНО-ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ АГЕНТУРНИХ ОПЕРАЦІЙ ЯК РІЗНОВИДУ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ ДІЙ, ПЕРЕДБАЧЕНИХ НОВИМ КПК УКРАЇНИ

Підюков Петро Павлович, доктор юридичних наук, професор, заслужений юрист України, завідувач наукової лабораторії з проблем психологічного забезпечення навчального процесу навчально-наукового інституту права та психології Національної академії внутрішніх справ
Конюшенко Яна Юріївна, кандидат юридичних наук, старший викладач кафедри кримінального процесу Національної академії внутрішніх справ

У наукових здобутках відомих учених С.Г. Гордієнка, В.В. Крутова, Д.Й. Никифорчука, М.А. Погорецького, І.В. Сервецького, Л.Д. Удалової, С.М. Стахівського, О.М. Юрченка та інших авторів протягом вже тривалого часу справедливо зверталась увага на те, що як у міжнародно-правовому просторі, так і в національному законодавстві Європейських країн (у тому числі України) застосовується різна термінологія щодо визначення поняття негласної діяльності працівника правоохоронного органу (чи іншого його представника), який здійснює негласне оперативно-розшукове провадження під прикриттям або як вигадана особа.

Так, за законодавством про оперативну-розшукову діяльність Азербайджану (п.16 ст. 10 Закону Азербайджанської республіки від 28.10.1999 р. «Про оперативно-розшукову діяльність») [1], Білорусі (п.13 ст. 11 Закону Республіки Білорусь від 09.07.1999 р. «Про оперативно-розшукову діяльність») [2, с.136], Грузії (п. к ст.7 Закону Грузії від 30.04.1999 р. «Про оперативну-розшукову діяльність») [2 с. 18Г], Молдови (п. р ст. 6 Закону Республіки Молдова від 12.04.1994 р. «Про оперативно-розшукову діяльність» [2, с. 3081, Російської Федерації (п. 12 ст. 6 Федерального Закону РФ від 12.08.1995 р. «Про оперативно-розшукову діяльність») [2, с. 338] та деяких інших країн зазначений різновид оперативно-розшукового заходу іменується «оперативним впровадженням», Казахстану (ч. 2 ст. 11 Закону Республіки Казахстан від 15.09.1994 р. «Про оперативно-розшукову діяльність» [2, с. 224] - «впровадженням співробітників у злочинне середовище».

Ще до прийняття нового КПК України законодавство України про ОРД (п.8 ч.1 ст. 8 ЗУ «Про оперативно-розшукову діяльність») [3] передбачало право оперативно-розшукових підрозділів здійснювати «проникнення в злочину групу негласного працівника оперативного підрозділу або особи, яка співробітничає з останнім, із збереженням в таємниці достовірних даних щодо її особистості, а також використовувати документи, які зашифровують особу чи відомчу належність працівників, приміщень і транспортних засобів оперативних підрозділів».

Як ученими, так і практиками вносилися численні пропозиції, по-перше, уніфікувати назву таких дій, здійснюваних по лінії оперативних підрозділів, по-друге - привести її у відповідність до міжнародно-правових норм та