ДОСЛІДЖЕННЯ РУТКИТІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Гончар О.В.

Науковій керівник - доц. кафедри «Прикладна математика та інформаційні технології у бізнесі» , канд. техн. наук Савчук В.П.

Руткити зовсім не нове явище, оскільки їх появу пов'язують ще з UNIX-платформами.

Руткит – це програма, що приховує деякі елементи : файли, процеси, записи в реєстрі, адреси елементів пам'яті, мережеві підключення і ін., від інших програм або операційної системи.

Руткит сам по собі не представляє для системи ніякої шкоди – це технологія, яка може бути використана як в конструктивних, так і в деструктивних цілях. У системах UNIX руткити використовуються як гарантія безперервного доступу до видаленого комп'ютера, який заздалегідь був заражений з метою установки backdoor - коду, через який можна отримати доступ до комп’ютеру, захована змін, застосованих до конфігурації, захована логів, що залишилися після вторгнення в систему. Для систем Windows мета залишається аналогічною.

З іншого боку, є і потенційні переваги використання руткитів, які можуть цілком легітимно застосовуватися в наступних областях: моніторинг співробітників, захист інтелектуальних даних, захист програм від дії шкідливих код або помилок користувачів.

Як ми бачимо, навіть якщо руткит використовується в легітимних цілях, завжди є особливості, які вимагають ретельного аналізу.

Дипломна робота присвячена дослідженню функціонування руткитів методами теорії активних агентних систем та розробці відповідних програмних засобів.

1. Хоглунд Р., Батлер Дж. Руткити: внедрение в ядро Windows, 1-е издание М.: Издательский дом "Питер", 2007. 288 с.