УДК 521.384

М.А. Павленко, Д.В. Прибильнов, О.В. Сісков, В.О. Капранов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

КЛАСИФІКАЦІЯ ПРОГРАМНИХ ЗАСОБІВ АНОНІМНОГО ВИКОРИСТАННЯ РЕСУРСІВ ГЛОБАЛЬНОЇ МЕРЕЖІ

В даній статті розглянуті питання пов'язані з заходами комп'ютерної безпеки при використанні ресурсів глобальної мережі Інтернет, а саме проаналізовані можливості програмного забезпечення, яке дозволяє анонімне використання даної мережі. Розкриті питання щодо використання проксі серверів і наведені приклади програмного забезпечення.

Ключові слова: *проксі, анонімний доступ, конфіденційність, комп'ютерна безпека, порт.*

Вступ

Постановка проблеми. XXI століття вносить корективи у рівень розвитку сучасної людини та ступінь інформатизації суспільства. Великого розповсюдження набуває автоматизація процесів життєдіяльності людини. Користувачі, які мають персональні комп'ютери, намагаються використати їх з найбільшою ефективністю, що вимагає пошуку і аналізу великої кількості інформації. Зазвичай, користувачі використовують ресурси глобальної мережі «Інтернет», яка є найбільшим носієм інформації. Але з-поміж багатьох переваг, якими володіє ця мережа:

– доступність;

– зручність;

– інформативність;

– можливість використання порад інших користувачів;

– миттєвість обміну повідомленнями тощо.

Існують також небезпеки, пов'язані з приватністю або конфіденційністю роботи і зберігання даних. Наприклад:

– можливість зараження комп'ютерними вірусами;

– можливість несанкціонованого використання персонального комп'ютера (ПК);

– можливість вилучення ключових файлів електронних підписів;

можливість вилучення файлів паролів з подальшим їх дешифруванням тощо.

Отже, головним питанням стає захищеність ПК користувача під час роботи у глобальній мережі. Яким чином можливо використовувати ресурси «Інтернет» і водночас бути певним, що ПК буде захищеним. Один із шляхів вирішення даного питання є використання програм анонімного доступу до мережі. Також розглядаються певні особливості анонімного використання ресурсів «Інтернет».

Метою даної статті є приведення класифікації програмних засобів анонімного використання ресурсів глобальної мережі, а також відображення одного із способів захисту ПК від несанкціонованого доступу під час роботи з ресурсами «Інтернет».

Основна частина

Непрямий доступ до будь-яких ресурсів завжди вимагає додаткових зусиль на пошук основної особи, яка зробила запит. Даний принцип лежить в основі анонімного використання ресурсів глобальної мережі. Спеціально для ретранслювання запитів або анонімного доступу до ресурсів, що запитуються, були створені проксі-сервера.

Проксі-сервер (від англ. *proxy* — «представник, уповноважений») — служба в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до проксі-серверу й запитує який-небудь ресурс (наприклад, файл), розташований на іншому сервері.

Потім проксі-сервер або підключається до зазначеного сервера й одержує ресурс у нього, або повертає ресурс із власного кеша (у випадках, якщо проксі має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінена проксі-сервером у певних цілях. Також проксі-сервер дозволяє захищати клієнтський комп'ютер від потужних мережних атак [4].

Найчастіше проксі-сервери застосовуються для наступних цілей:

– забезпечення доступу з комп'ютерів локальної мережі в Інтернет;

– кешування даних: якщо часто відбуваються звертання до одних і тих самим зовнішніх ресурсів, то можна тримати їхню копію на проксі-сервері й видавати по запиту, знижуючи тим самим навантаження на канал у зовнішню мережу й прискорюючи одержання клієнтом запитаної інформації;

– стискання даних: проксі-сервер завантажує інформацію з Інтернету й передає інформацію кінцевому користувачеві в стислому виді. Такі проксі-сервери використаються в основному з метою економії зовнішнього трафіка;

– захист локальної мережі від зовнішнього доступу. Необхідно настроїти проксі-сервер так, щоб локальні комп'ютери зверталися до зовнішніх ресурсів тільки через проксі-сервер, тоді зовнішні комп'ютери не зможуть звертатися до локального взагалі (вони «бачать» тільки проксі-сервер);

– обмеження доступу з локальної мережі до зовнішньої: наприклад, заборона доступу до певних веб-сайтів, обмеження використання «Інтернету» якимсь локальним користувачам, установлення квоти на трафік або смугу пропущення, фільтрування реклами й вірусів.

анонімізація доступу до різних ресурсів. Проксі-сервер може приховувати відомості про джерело запиту або користувача. У такому випадку цільовий сервер бачить лише інформацію про проксі-сервер, наприклад, IP-адреса, але не має можливості визначити справжнє джерело запиту. Існують, також, проксі-сервери, які передають цільовому серверу помилкову інформацію про дійсного користувача[4].

Багато проксі-серверів використаються для декількох цілей одночасно. Деякі проксі-сервери обмежують роботу декількома портами: 80 (Браузер), 443 (Шифроване з'єднання (HTTPS)), 20,21 (FTP).

На відміну від шлюзу проксі-сервер найчастіше не пропускає ICMP-трафік (неможливо перевірити доступність машини командами ping і tracert), що в свою чергу надає можливість залишатися для зовнішньої мережі неіснуючими[1].

Проксі-сервер, до якого може одержати доступ будь-який користувач мережі Інтернет, називається відкритим. Списки відкритих проксі серверів можна зібрати використовуючи спеціальне програмне забезпечення, наприклад, ProxyLancher, ProxyFinder, ProxyChecker. Данні програми не лише збирають проксі-листи але і мають вбудовані функції фільтрації та відсіювання, виходячи з певних критеріїв, заданих користувачем у настройках.

Необхідно звернути увагу на можливості проксі-серверів надавати користувачу здатності залишатися анонімним під час роботи з глобальною мережею. Тобто, користувач на пряму не звертається до глобальної мережі, що робить неможливим видалений доступ до ПК. Ця властивість відкритих проксі-серверів використовується анонімайзерами. Спеціально розробленим програмним забезпеченням, яке дозволяє працювати з проксі-серверами.

Користувач самостійно може, знаючи адресу проксі-сервера, прописати її в настройках програми, наприклад: ваб-браузера чи ICQ. Але постає проблема зручності. Кожен раз змінювати настройки програмного забезпечення, яке пов'язане з Інтернет є досить довгою справою. До цього слід додати, що не кожна програма вміє працювати з проксі-серверами.

Розглянемо схему роботи веб-браузера через проксі [4] (рис. 1)

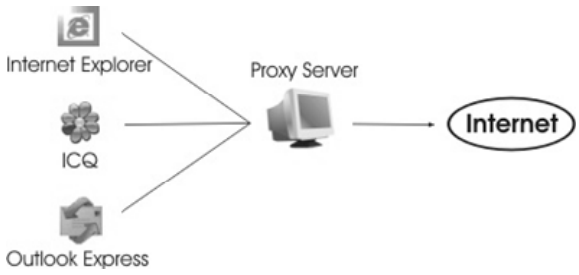

Рис. 1. Схема роботи програмного забезпечення через проксі-сервер

Необхідно створити уніфіковану програму, яка дозволить змінювати настройки роботи з проксі-серверами будь-якого програмного забезпечення. Класом таких програм виступають анонімайзери. Схема їх роботи представлена на наступному рисунку.

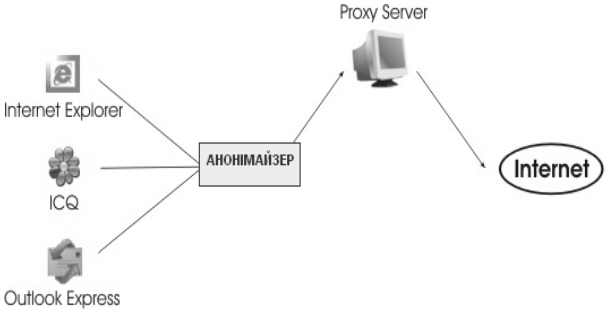

Рис. 2 Схема роботи програмного забезпечення через анонімайзер

Класифікація та характеристики програм анонімного доступу до мережі.

Ознаки класифікації. Програми анонімного доступу до мережі Інтернет поділяються за наступними ознаками:

– за способом реалізації: локально реалізовані; реалізовані на спеціальному сервері.

– за видами проксі-серверів, які використовуються: SOCKS4; SOCKS5; HTTP; HTTPS; універсальні, мають можливість використовувати всі типи проксі-серверів.

– за можливістю не пропускання ICMP-трафіку: з командами ping і tracert; без команд ping і tracert.

– за доступністю широкому колу користувачів: безкоштовні; комерційні.

Серед програмного забезпечення дуже розповсюдженими є наступні анонімайзери: SocksCap, HideIP, AnGuestPro, Steganos Internet Anonym Pro.

Використання локально реалізованого програмного забезпечення, яке дозволяє бути анонімним при використанні ресурсів Інтернет, має всі переваги використання проксі серверів, але і наслідує всі недоліки. Зокрема: повільну роботу; недостатню надійність передачі інформації; збої в роботі.

Але, якщо проксі сервер знаходиться на одній ділянці мережі з користувачем або служить для підключення локальної мережі до Інтернет, то уповільнення в роботі непомітні. Крім того, слід пам'ятати, що використання

анонімайзерів не забезпечить повної анонімності. Звісно, можна обрати список проксі-серверів, які будуть анонімними і перевіреними з використанням спеціальних ресурсів, для роботи анонімайзера, але не дивлячись на всю конфіденційність кожен сервер завжди веде свій власний лог. Також існують так звані Free web anonymizer, CGI proxy, web proxy. Вони дозволяють анонімно продивлятися Інтернет сторінки. Прикладами таких анонімайзерів є:

– http://proxyguy.com/

– http://gamesproxy.com/

– http://proxyz.be/ тощо.

Сервер даного типу являє собою (з погляду користувача) web-сторінку, дуже схожу на сторінки пошукових систем. Тільки замість пошукових фраз необхідно в поле уведення набрати URL того сайту, на який необхідно перейти. Натиснувши кнопку "Submit" або "Go" йде перехід на сторінку, URL якої вказано у CGI proxy.

Головним недоліком анонімайзерів даного типу є те, що з їхньою допомогою можна подивитися не всі сайти. Справа в тому, що для того, щоб всі посилання працювали правильно, анонімайзер повинен скачати собі web сторінку з потрібного сайту, вибрати відтіля всі посилання й виправити їх таким чином, щоб ці посилання також вели на анонімайзер. Багато web сайтів використають різні сучасні технології (JavaScript, Flash, Active тощо), які анонімайзери не в змозі "переробити під себе". Тому багато сайтів (особливо це стосується сайтів, що вимагають авторизації, або активно використають JavaScript / Flash) не будуть коректно відображатися або працювати через анонімайзер.

Крім того, до числа недоліків використання CGI proxy можна віднести наявність додаткової реклами (додає сам cgi proxy – за рахунок реклами вони існують), обмежену підтримку HTTPS і FTP (вони не завжди підтримується) і іноді, можливо, CGI proxy не дозволяють переглядати картинки. Деякі CGI proxy можна встановити в якості proxy у браузері, але цей рідкісний виняток і тут фактично використаються 2 різних проксі: cgi proxy (анонимайзер) і HTTP proxy [2].

Отже були розглянуті основні засоби, що дозволяють анонімно використовувати ресурси Інтернет, але яким саме чином це захищає ПК від несанкціонованого доступу. Відповідь полягає у, власне, призначенні проксі-серверів, а також програмного забезпечення, яке дозволяє з ними працювати. Проксі-сервер ретранслює запит користувача, тим самим не показує його присутність, а якщо користувач не присутній у мережі, то неможливо отримати доступ до його конфіденційної інформації.

Висновки

Актуальність розглянутої проблеми полягає у необхідності захисту інформації будь-яких користувачів мережі Інтернет, адже суттєвого розповсюдження набула Інтернет торгівля, офіційна переписка засобами електронної пошти чи обмін миттєвими повідомленнями, тобто для збереження конфіденційних даних, список яких був приведений вище необхідно використовувати анонімайзери тобто проксі-сервери і відповідно спеціальне програмне забезпечення, яке дозволить їх зручну зміну чи налаштування параметрів.

Список літератури

1. Курило А. О парадигме информационной безопасности. [Електрон. ресурс]. – Режим доступа к ресурсу: http://www.morepc.ru/informatisation/ cio200 310086.html.

2. Щеглов А.Ю. «Защита конфиденциальной информации и персональных данных в современных условиях.». [Електрон. ресурс]. – Режим доступа к ресурсу: http://www.morepc.ru/informatisation/ cio200310096. html.

3. Дж. Феллинг «Основы сетевых портов. Часть 2». [Електрон. ресурс]. – Режим доступа к ресурсу: http://www.morepc.ru/net/net160120062.html.

4. «Расширенный FAQ по работе с прокси» [Електрон. ресурс]. – Режим доступа к ресурсу: http://www. spszone.com/articles/proxy_faq_ru.htm.

Надійшла до редколегії 10.02.2009

Рецензент: д-р тнхн. наук, доцент О.В. Лемешко, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

КЛАССИФИКАЦИс ПРОГРАММНОГО ОБЕСПЕЧЕНИс АНОНИМНОГО ИСПОЛЬЗОВАНИс РЕСУРСОВ ГЛОБАЛЬНОЙ СЕТИ

М.А. Павленко, Д.В. Прибыльнов, О.В. Сисков, В.О. Капранов

В данной статье рассмотрены вопросы, связанные с компьютерной безопасностью при использовании ресурсов глобальной сети Интернет, а именно проанализированы возможности программных продуктов, которые позволяют анонимно использовать ресурсы глобальной сети. Раскрыты вопросы использования прокси серверов и приведены примеры программного обеспечения.

Ключевые слова: *прокси, анонимный доступ, конфиденциальность, компьютерная безопасность.*

CLASSIFICATION OF SOFTWARE TOOLS FOR ANONYMOUS USE OF GLOBAL NETWORK RESOURCES

M.A. Pavlenko, D.V. Prybylnov, O.V. Siskov, V.O. Kapranov

Present article covers the questions related to computer security precautions while using global network (Internet) resources, videlicet: capabilities of software, which allows to use present network anonymously, are analyzed. Questions of proxy servers use are examined and examples of software are presented.

Keywords: *proxy, anonymous access, confidentiality, computer security, port.*