УДК 004.45
Д.Р. Карабан; Р.О. Жаровський , к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В ІНТЕРНЕТІ

D.R. Karaban; R.O. Zharovskyi, Ph.D.

METHODS OF PROVIDING ANONYMITY IN THE INTERNET

Існує широкий спектр методів для забезпечення анонімності користувачів в Інтернеті. Проксі-сервери мають кілька видів із своїми особливостями, проте найчастіше для анонімізації використовуються SOCKS5. Зараз їх надійність вважається обмеженою, оскільки вони самі по собі не забезпечують шифрування трафіку і можуть легко піддаватися деанонімізації, навіть при використанні проксі-ланцюга. Цю проблему часто вирішують шляхом комбінування їх з VPN.

VPN-сервіси також використовуються для анонімізації, проте основною проблемою залишається питання довіри до постачальника послуг. Більшість VPN-провайдерів стверджують, що не ведуть логів, але це важко перевірити, і часто логування все ж здійснюється. Крім того, при раптовому відключенні VPN-підключення весь трафік може потрапити в Інтернет безпосередньо, розкриваючи реальний IP. Ця проблема розв'язується налаштуванням правил файрвола.

SSH-тунелі спочатку були створені для інших цілей, але зараз використовуються і для анонімізації. Їхня шифрувальна техніка схожа на VPN, але принципи роботи та швидкість можуть бути іншими. На відміну від VPN, вони не направляють за умовчанням весь трафік через тунель і можуть використовуватися як локальні проксі-сервери.

Dedicated-сервери використовуються як віддалені робочі станції або платформа для власного VPN-сервера. Їх використання часто включає в себе віртуалізацію, коли на одному фізичному хості розташовано кілька віртуальних серверів, що ускладнює відстеження конкретного сервера.

Анонімна мережа Tor, яка раніше вважалася однією з найбільш надійних, тепер має випадки деанонімізації користувачів. Трафік на виході може бути прослуховований, і вихідна IP-адреса, що належить Tor, може викликати підозри.

JonDonym або JAP (Java Anonymous Proxy) направляє трафік через ланцюг серверів, і користувач може вибирати використовувані "каскади". Він має безкоштовні та платні варіанти. Браузер JonDoFox, спочатку збиралися як змішаний Firefox з додатковими розширеннями, зараз модифікований Tor Browser.

I2P - це анонімна децентралізована мережа, яка працює поверх інтернету і не використовує IP-адресацію. Вона перевершує Tor у надійності шифрування передаваних даних, але не завжди підходить для анонімізації доступу до зовнішнього інтернету через нестабільне та повільне підключення.

Віртуальні машини допомагають вирішити додаткові завдання безпеки під час анонімної роботи, а їх використання у поєднанні з іншими засобами є досить ефективним. "Антидетект" використовують складання браузерів із вбудованими заміною різних ідентифікаторів, але їх використання зачасту є обмеженим і часто пов'язане з нелегальною діяльністю.

Інші методи анонімізації можуть бути менш популярними, менше перевіреними або не гарантувати надійну анонімність. До них відносяться програми та браузерні розширення, спрямовані на захист від відстеження браузера, і вони часто доповнюють систему анонімізації.