**Прихований канал (covert channel)** — це комунікаційний канал, що пересилає інформацію методом, який спочатку був для цього не призначений. Також це техніка ухилення або атаки, яка використовується для передачі інформації в таємному, несанкціонованому або незаконному порядку. Найчастіше прихований канал є паразитом по відношенню до основного каналу: він зменшує пропускну здатність. Сторонні спостерігачі зазвичай не можуть виявити, що крім основного каналу передачі даних є ще додатковий, тільки відправник і одержувач знають це. Наприклад, в стеганографії приховані повідомлення кодувалися всередині графічних зображень або інших даних таким чином, що змін на око не було помітно, однак одержувач повідомлення міг розкодувати зашифроване повідомлення.

Прихований канал може бути використаний для отримання інформації з організації або імплантації інформації в організацію. Інтернет-таємний канал - це цифровий еквівалент портфеля з секретним відділенням, який шпигун може використовувати, щоб просунути конфіденційні документи повз охоронців в захищений об'єкт або з нього. Так само, як шпигун може використовувати той самий секретний відсік, щоб приховати зброю від охоронців при вході в захищений об’єкт, зловмисник може використовувати приховані Інтернет-канали, щоб приховати кіберзброю, наприклад, завантаження шкідливого програмного забезпечення із зовнішнього сервера на хост в приватній мережі організації.

Основи прихованих Інтернет-каналів

Інтернет-таємні канали можуть використовувати звичайні протоколи Інтернету нетрадиційними способами. Кінцеві точки каналу - заражений комп’ютер та комп’ютер управління та керування зловмисником - повинні використовувати програмне забезпечення для ухилення або атаки, яке розпізнає та обробляє ці нетрадиційні методи. Або користувач, або зловмисник може встановити це програмне забезпечення за допомогою інструменту віддаленого адміністрування (remote administration tool, RAT). Інтернет-приховані канали відрізняються від зашифрованих тунелів. Вони можуть передавати інформацію чистим текстом, але їх не спостерігають. Хоча вони не вимагають методів або ключів шифрування, деякі приховані канали використовують шифрування або інші засоби для затухання даних.  
Давайте розглянемо дві техніки. Перший прийом передбачає передачу інформації таємно, по одному символу за раз, в поле ідентифікації (ID) заголовка Інтернет-протоколу (IP). Популярні реалізації цієї техніки помножать значення ASCII кожного символу на 256, щоб створити 16-бітові значення для цього поля ID. Для передачі абревіатури "ICANN" відправник відправив 5 IP-пакетів із полем ID, кодованим таким чином:

|  |  |  |
| --- | --- | --- |
| Пакет | ASCII десяткове значення | IP ID поле (помножене на 256) |
| 1 | 71 (“I”) | 18176 |
| 2 | 67 (“C”) | 17152 |
| 3 | 65 (“A”) | 16640 |
| 4 | 78 (“N”) | 19968 |
| 5 | 78 (“N”) | 19968 |

Потім приймаючий комп’ютер декодує поле ідентифікатора IP, поділивши значення на 256. Ці значення не є підозрілими, і оскільки IP допускає повторювані пакети, цей трафік, швидше за все, ухиляється від виявлення. Це повільно, але крадькома.

Другий прийом передбачає створення прихованого каналу, який використовує корисне навантаження протоколу - інформацію, яку протокол передає між комп’ютерами. Цей прийом додає дані до запитів ECHO та повідомлень відповідей Протоколу керуючих Інтернетом (ICMP). ECHO зазвичай використовується для послуги під назвою ping. Оскільки мережеві адміністратори зазвичай використовують ping, щоб перевірити, чи доступний віддалений хост, трафік ICMP ECHO зможе обійти брандмауери - заходи безпеки.

Загрози прихованих каналів переважно присутні в системах із спільними ресурсами як об'єкти файлової системи, віртуальна пам'ять, мережеві стеки та канали, кеші процесора, пристрої введення тощо.

У порівнянні з іншими прихованими канальними носіями, кеш-пам'ять процесора є більш привабливою для використання, оскільки його висока робоча швидкість може забезпечити високу пропускну здатність каналу, а розміщення на низькому рівні в ієрархії системи може обійти безліч механізмів ізоляції високого рівня. Таким чином, приховані кешовані канали залучили серйозну увагу в останніх дослідженнях.

На основі результати своїх вимірювань, дослідники дійшли висновку, що шкода розповсюдження даних із прихованих каналів кешу цілком обмежена через низьку досяжну ємність каналу.

У відповідь на відкриття кешованого каналу атак, запропоновано ряд архітектурних рішень для обмеження каналів кешування, включаючи RPcache, PLcache та Newcache. RPcache та Newcache використовують рандомізацію для запобігання передачі даних шляхом встановлення схеми кодування на основі місцезнаходження. Однак PLcache базується на примусовій ізоляції ресурсів шляхом розділення кешу. Одним недоліком апаратних рішень є їх висока вартість адаптації та затримка. З метою запропонувати захист, який можна негайно розгорнути, HomeAlone пропонує попередньо виявити спільне проживання недружніх віртуальних машин. Використовуючи знання про існуючі

методи прихованого кешування кешу, HomeAlone виявляє наявність зловмисної ВМ, діючи як прихований приймач каналу та спостереження за часом кешування аномалії, спричинені діяльністю іншого приймача. Промисловість застосувала більш прагматичний підхід для пом'якшення прихованих канальних загроз. Аmazon EC2 cloud надає функціональну послугу, яка називається виділеними екземплярами, яка забезпечує віртуальні машини, що належать кожному орендарю. Ця послуга ефективно усуває різні приховані канали, індуковані апаратним забезпеченням спільної платформи, включаючи прихований канал кешування. Однак для того, щоб насолоджуватися цією послугою, є у хмарних користувачів заплатити значну цінову премію.

.

Cписок літератури:

* [Прихований канал[ред. | ред. код]](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D1%85%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B9_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB)
* https://www.icann.org/news/blog/what-is-an-internet-covert-channel
* https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final97.pdf