Перехват IP-сетей: реальная угроза

Суть атаки: аннонсирование злоумышленниками сети, содержащей ресурс жертвы, из сети злоумышленника.

Наиболее резонансный случай: YouTube и Пакистан.

Демонстрация атаки

- Тут будет демонстрация атаки на реальном сайте, 5 минут.

Области применения атаки

- Перехват трафика с сайтов, сбор паролей и банковских реквизитов, создание подложных сайтов, вывод сайтов из строя
- Перехват почты, VoIP-разговоров, запросов и ответов баз данных
- Подмена DNS серверов серверами злоумышленника
- Многое другое — все, на что хватит фантазии!

Борьба с такими атаками

Какие есть методы борьбы с аннонсированием Ваших сетей злоумышленниками?

Борьба с такими атаками

ЭФФЕКТИВНЫХ МЕТОДОВ БОРЬБЫ В НАСТОЯЩЕЕ ВРЕМЯ НЕ СУЩЕСТВУЕТ.

Снижение уровня опасности

- ВЛАДЕНИЕ И ПОЛНЫЙ КОНТРОЛЬ НАД КРИТИЧЕСКИМ АДРЕСНЫМ ПРОСТРАНСТВОМ (PI сеть и AS)
- Аннонсирование критической инфраструктуры сетями /24 и более короткими где это возможно (прямые пиринги, точки обмена трафиком)
- Использование средств мониторинга: myASN, свои удаленные скрипты мониторинга таблиц BGP

Снижение уровня опасности

- Использование SSL сертификатов (в то же время, можно проаннонсить и сеть центр сертификации заодно — не панацея)
- Сертификация IP-ресурсов — следующий шаг развития Интернет. Обратная сторона — тотальная цензура Сети и появление централизованных рычагов отключения от Интернет
- Не использовать Интернет где не нужно
- Применение правильных методов авторизации, например, одноразовых паролей

Расследование атак

- Неприятный сюрприз для злоумышленников: сервисы RIS, BGP Play.
- Не верить данным в RIPE DB!
- Отличия физического и логического коннективити: идем по кабелю, а не по аннонсам

Вопросы и ответы

Максим Тульев
ООО “НетАссист”
Киев, Украина
+380 44 2398999
www.netassist.ua
maxtul@netassist.ua