#### МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

## «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

## Обнаружение сетевого Р2Р-трафика

Курсовую работу выполнил студент 4 курса 431 группы специальности 10.05.01 «Компьютерная безопасность» факультета компьютерных наук и информационных технологий

Стаин Роман Игоревич

Научный руководитель доцент, к.ю.н.

Алексей Владимирович Гортинский

Р2Р-сети используются для обмена файлами и распространения контента, в том числе нелегального. Это может приводить к нарушению авторских прав и угрожать безопасности пользователей, так как в Р2Р-сетях часто распространяются вирусы и другие вредоносные программы. Пользователей таких сетей практически невозможно контролировать, поэтому необходимы способы обнаружения и идентификации Р2Р-трафика.

**Целью данной работы** является изучение и обнаружение общих и частных, позволяющих идентифицировать конкретные протоколы, признаков P2P-трафика.

#### Задачи исследования:

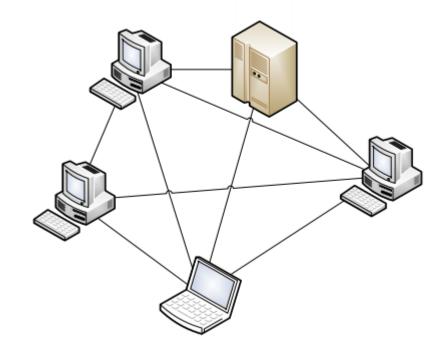
- Изучение архитектуры и общих принципов работы Р2Р-сети.
- Исследование общих признаков Р2Р-трафика.
- Исследование признаков некоторых Р2Р-протоколов.
- Рассмотрение протоколов и приложений, схожих по поведению с Р2Р.
- Разработка программы, способной перехватывать TCP/UDP-трафик и обнаруживать и идентифицировать P2P-трафик.

## Архитектура Р2Р-сети

**P2P** (**p**eer-**to**-**p**eer) — одноранговая, децентрализованная или пиринговая сеть. Это распределённая архитектура приложения, которая разделяет задачи между узлами (peer).







# Методы обнаружения Р2Р-трафика без анализа полезной нагрузки

- 1. Анализ портов
- 2. TCP/UDP-эвристика
- 3. IP/Port-эвристика
- 4. Пороговый метод идентификации BitTorrent

## Эвристические предположения

#### TCP/UDP-эвристика:

Если пара адресов использует одновременно TCP и UDP, то эти адреса считаются как P2P.

#### IP/Port-эвристика:

Факт, что при обращении к паре <dst\_ip, dst\_port> количество адресов источников практически совпадает с количеством портов источников, характеризует P2P-деятельность.

## Пороговый метод идентификации BitTorrent

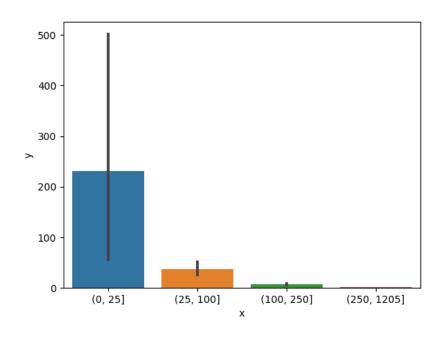
Каждые 30 секунд рассчитываются специальные метрики, которые сравниваются с пороговыми значениями, чтобы определить, является ли хост пиром BitTorrent.

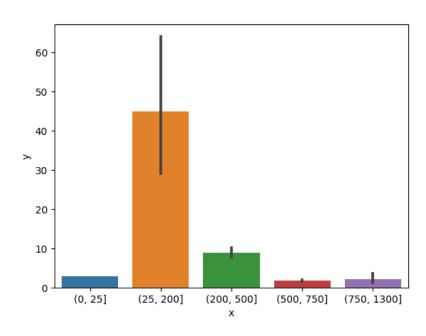
- 1. Число подключений к хосту C.
- 2. Коэффициент активной передачи  $R_{AT} = \frac{AT}{C}$ .
- 3. Двусторонние передачи данных ВіАТ.
- 4. Коэффициент изменений отношений  $R_{RC} = \frac{RC}{AT}$ .

### Исключения

Поведение некоторых легальных протоколов, например, SMTP, POP, DNS, NTP может быть схожим с поведением P2P-протоколов.

Также игры и вредоносные программы имеют уникальное поведение и номера портов, что усложняет обработку исключений.





## Идентификация Р2Р-трафика

Адреса могут быть отнесены к некоторому Р2Р-протоколу исходя из:

- 1. Номера порта.
- 2. Анализа полезной нагрузки.
- 3. Порогового метода идентификации BitTorrent.

## Анализ полезной нагрузки

#### Для идентификации BitTorrent:

- 1. Минимальная длина полезной нагрузки пакета 20 байт.
- 2. Байт со значением 19.
- 3. Следующая за ним строка «BitTorrent protocol».

#### Для идентификации Bitcoin:

- 1. Минимальная длина полезной нагрузки пакета 20 байт.
- 2. Порт источника или назначения равен 8333 или 8334.
- 3. Содержится команда или сообщение, характерное для Bitcoin.

## Описание программы

В данной работе был разработан сниффер или анализатор сетевого трафика, который перехватывает TCP/UDP-трафик и анализирует его на наличие P2P-деятельности.

При запуске программы предлагается выбор сетевого интерфейса, который будет прослушиваться:

| 🔳 Анализатор сетев                   | вого трафика 💮 🔾 🗴 |  |  |  |  |  |
|--------------------------------------|--------------------|--|--|--|--|--|
| Выберите интерфейс для прослушивания |                    |  |  |  |  |  |
| ІР-адрес                             | Интерфейс          |  |  |  |  |  |
| 127.0.0.1                            | lo                 |  |  |  |  |  |
| 10.0.2.15                            | eth0               |  |  |  |  |  |
| 192.168.1.71                         | eth1               |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |
|                                      |                    |  |  |  |  |  |

## Далее открывается основное окно программы:

| Анализатор сетевого трафика |                 |                |          |        |                |                     |                      |  |
|-----------------------------|-----------------|----------------|----------|--------|----------------|---------------------|----------------------|--|
| Время Источни               | к Назначение    | Порты          | Протокол | Длина  | Инфо           | Анализ портов       | IP/Port эвристика    |  |
| 13:07:25 192.168.1.13       | 2 20.135.20.1   | 50108 -> 443   | TCP      | 6 Б    |                | 15.235.40.193:6881  | 192.168.1.132:55069  |  |
| 13:07:25 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | 46.173.42.166:6881  | 192.168.1.132:6881   |  |
| 13:07:25 192.168.1.13       | 2 192.168.1.255 | 137 -> 137     | UDP      | 50 Б   |                | 81.28.188.57:6881   | 192.168.1.132:52050  |  |
| 13:07:25 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | 46.229.188.217:6883 |                      |  |
| 13:07:25 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | 89.109.199.212:6881 |                      |  |
| 13:07:25 192.168.1.13       | 5.165.50.102    | 55069 -> 41741 | UDP      | 20 Б   | P2P BitTorrent | 5.165.240.56:6881   |                      |  |
| 13:07:25 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 1452 Б |                | 5.136.193.67:6881   |                      |  |
| 13:07:25 192.168.1.13       | 2 20.135.20.1   | 50108 -> 443   | TCP      | 6Б     |                | 109.167.170.28:6881 |                      |  |
| 13:07:25 192.168.1.13       | 2 20.135.20.1   | 50108 -> 443   | TCP      | 6Б     |                | 88.86.76.18:6881    |                      |  |
| 13:07:26 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 2904 Б |                | 95.29.97.200:6881   |                      |  |
| 13:07:26 95.73.67.8         | 192.168.1.132   | 55316 -> 49433 | TCP      | 0 Б    |                | 95.190.58.55:6881   |                      |  |
| 13:07:26 192.168.1.13       | 95.73.67.8      | 49433 -> 55316 | TCP      | 6Б     |                | 176.215.151.39:6881 |                      |  |
| 13:07:26 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | TCP/UDP эвристика   | По полезной нагрузк  |  |
| 13:07:26 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | 31.163.71.193       | 31.134.181.131:24737 |  |
| 13:07:26 192.168.1.13       | 5.165.50.102    | 55069 -> 41741 | UDP      | 20 Б   | P2P BitTorrent | 192.168.1.132       | 192.168.1.132:64474  |  |
| 13:07:26 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     | 192.168.1.132:55069  |  |
| 13:07:26 5.165.50.102       | 192.168.1.132   | 41741 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     | 212.93.112.149:28457 |  |
| 13:07:26 192.168.1.13       | 2 20.135.20.1   | 50108 -> 443   | TCP      | 6Б     |                |                     | 93.23.157.130:59590  |  |
| 3:07:26 20.135.20.1         | 192.168.1.132   | 443 -> 50108   | TCP      | 1452 Б |                |                     | 192.168.1.132:64496  |  |
| 13:07:26 5.137.229.92       | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     | 81.198.235.120:21467 |  |
| 13:07:26 5.137.229.92       | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     |                      |  |
| 13:07:27 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 1452 Б |                |                     |                      |  |
| 13:07:27 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 1452 Б |                |                     |                      |  |
| 13:07:27 192.168.1.13       | 2 20.135.20.1   | 50108 -> 443   | TCP      | 6Б     |                |                     |                      |  |
| 13:07:27 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 2904 Б |                |                     |                      |  |
| 13:07:27 5.137.229.92       | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | По метрикам BT      | Пересечение методо   |  |
| 3:07:27 5.137.229.92        | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent | 192.168.1.132:55069 | 192.168.1.132:55069  |  |
| 3:07:27 5.137.229.92        | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     | 192.168.1.132:6881   |  |
| 3:07:27 192.168.1.13        | 5.137.229.92    | 55069 -> 62030 | UDP      | 20 Б   | P2P BitTorrent |                     | 252,255,2,252,5552   |  |
| 13:07:27 5.137.229.92       | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     |                      |  |
| 13:07:27 5.137.229.92       | 192.168.1.132   | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     |                      |  |
| 13:07:27 192.168.1.13       | 5.137.229.92    | 55069 -> 62030 | UDP      | 20 Б   | P2P BitTorrent |                     |                      |  |
| 13:07:27 5.137.229.92       |                 | 62030 -> 55069 | UDP      | 1427 Б | P2P BitTorrent |                     |                      |  |
| 13:07:28 192.168.1.13       |                 | 50108 -> 443   | TCP      | 6Б     |                |                     |                      |  |
| 13:07:28 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 7260 Б |                |                     |                      |  |
| 13:07:28 192.168.1.13       |                 | 50108 -> 443   | TCP      | 6Б     |                |                     |                      |  |
| 13:07:28 20.135.20.1        | 192.168.1.132   | 443 -> 50108   | TCP      | 2904 Б |                |                     |                      |  |
| 13:07:28 192.168.1.13       |                 | 50108 -> 443   | TCP      | 6Б     |                |                     |                      |  |
|                             |                 | Стоп           |          |        |                |                     |                      |  |

### Заключение

В данной работе были рассмотрены теоретические сведения о технологии Р2Р, в частности, характерное поведение Р2Р-трафика и признаки некоторых протоколов.

В практической части была реализована программа — сниффер или анализатор сетевого трафика на языке Python, которая позволяет перехватывать ТСР и UDP трафик и анализировать его на присутствие P2P-активности, а также определять некоторые протоколы и приложения. Были реализованы методы анализа портов, обнаружения TCP/UDP- и IP/Port-эвристики, анализ полезной нагрузки для BitTorrent и Bitcoin и пороговый метод сравнения характерных метрик BitTorrent.

#### Список использованных источников

- 1. P2P (Peer-to-Peer) [Электронный ресурс]. URL: https://web.archive.org/web/20171205204322/http://ru.bmstu.wiki/P2P\_(Peer-to-Peer) (Дата обращения 19.05.2023). Загл. с экр. Яз. рус.
- 2. P2P [Электронный ресурс]. URL: https://glebradchenko.susu.ru/courses/bachelor/odp/2013/SUSU\_Distr\_11\_P2P.pdf (Дата обращения 14.05.2023). Загл. с экр. Яз. рус.
- 3. Bhatia, M. Multi-level p2p traffic classification using heuristic and statisticalbased techniques: A hybrid approach / M. Bhatia, V. Sharma, P. Singh, M. Masud // Symmetry. 12 2020. Vol. 12. P. 2117.

- 4. Karagiannis, T. A longitudinal study of p2p traffic classification / T. Karagiannis,
- K. Papagiannaki, M. Faloutsos // Proc. of 14th IEEE International Symposium on Modeling, Analysis, and Simulation. 2005.
- 5. Karagiannis, T. BLINC: multilevel traffic classification in the dark / T. Karagiannis, K. Papagiannaki, M. Faloutsos. 2005. Pp. 229–240.
- 6. Karagiannis, T. Transport layer identification of P2P traffic / T. Karagiannis,
- A. Broido, M. Faloutsos, K. C. Claffy. 2004. Pp. 121–134.
- 7. Ngiwlay, W. Bittorrent peer identification based on behaviors of a choke algorithm / W. Ngiwlay, C. Intanagonwiwat, Y. Teng-amnuay // Association for Computing Machinery. 2008.

- 8. Бредихин, С. В.Диагностика p2p-АКТИВНОСТИ на основе анализа потоков netflow / С. В. Бредихин, Н. Г. Щербакова // Проблемы информатики. 2012. № 1. С. 40–51.
- 9. Desclaux, F. Vanilla skype part 1 / F. Desclaux, K. Kortchinsky // Proc of RECON2006. 2006.
- 10. BitTorrentSpecification TheoryOrg. [Электронный ресурс]. URL: https://wiki.theory.org/BitTorrentSpecification (Дата обращения 19.05.2023). Загл. с экр. Яз. англ.
- 11. Protocol documentation Bitcoin Wiki. [Электронный ресурс]. URL: https://en.bitcoin.it/wiki/Protocol\_documentation (Дата обращения 19.05.2023). Загл. с экр. Яз. англ.

## Спасибо за внимание!