Д. В. Сергеев (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Источники данных для обнаружения бот-сетей.**

Все подсети, составляющие глобальную сеть Интернет, в широком понимании можно разделить на две категории: сети Интернет-провайдеров и частные сети организаций. Несмотря на тот факт, что инфраструктура, базовые принципы администрирования и обеспечения безопасности применимы к обеим категориям, однако цели Интернет-провайдеров и организаций различны. Сетевая безопасность Интернет-провайдеров в основном связана с обеспечением «живучести» сетевых сервисов и предупреждение сбоев, в то время как безопасность в частных сетях организаций во многом связана с защитой вычислительной инфраструктуры.

Одним из важных аспектов различия между провайдерами и организациями являются доступные для анализа данные. В сетях организаций можно получить доступ к журнальным записям DHCP и DNS-серверов, доступ к сетевым сессиям каждого хоста, журнальным записям почтовых серверов, правилам политики безопасности, журнальным записям антивирусов и т. д. В сетях Интернет-провайдеров можно получить доступ исключительно к сетевым потокам. Рассмотрим некоторые из важных типов данных [1, 2]:

- данные сетевых потоков;
- данные DNS-серверов;
- данные о расположении хоста;
- данные систем-приманок;
- данные уровня хоста.

Технологии обнаружения бот-сетей неразрывно связаны с перечисленными источниками данных. В зависимости от объема используемых источников зависит эффективность той или иной технологии.

СПИСОК ЛИТЕРАТУРЫ

1. *Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, Manish Karir* A Survey of Botnet Technology and Defenses. — In: Proceedings of Cybersecurity Applications & Technology Conference for Homeland Security, 2009, p. 299–304.
2. *Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, Andreas Terzis* A multifaceted approach to understanding the botnet phenomenon. — In: Proceedings of 6th ACM SIGCOM Internet Measurement Conference, 2006, p. 41–52