Спектральный анализ трафика сети «Honeypot»

Хусни[1]

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

СПбГЕТУ, Профессора Попова, д. 5, Санкт-Петербург, 197376

[1]<bang.husni@gmail.com>

УДК 681.324

Хусни. **Спектральный анализ трафика сети «Honeypot»** // Труды СПИИРАН. Вып. 4 . — СПб.: Наука, 2008.

Аннотация. *Появление аномалий, таких как сбои и атаки, стали обычным явлением в современных компьютерных сетях. Выявление, диагностика и анализ аномалий составляют важнейшую часть повседневных сетевых операций. В этой статье мы предлагаем дизайн с использованием спектрального анализа для изучения сетевого трафика атак, захваченного honeypot. Как образец нападения использовалась Yahoo Messenger бот-атака. Мы использовали пакет входного трафика в заданных временных рамках и в виде временных рядов и спектральных форм.* — Библ. 4 назв.

UDC 681.324

Husni. **Spektral Analysis of Honeypot Network Traffic** // SPIIRAS Proceedings. Issue 4. — SPb.: Nauka, 2008.

Abstract. *Traffic anomalies such as failures and attacks are commonplace in today's computer networks. Identifying, diagnosing and treating anomalies in a timely fashion are a fundamental part of day to day network operations. In this paper we propose the design of using spectral analysis to study network traffic attack captured by honeypot. As sample attack we used yahoo messenger bots. We use the amount of packet traffic arrival in certain time frame and represent it into time series and spectral form.* — Bibl. 4 items.

1. Введение

Honeypot (хонипот) - информационный ресурс системы, ценность которого заключается в выявлении неправомочного или незаконного использовании ресурса [1]. Более ценным свойством Honeynet является снижение ложных срабатываний и ложных негативов, с которыми сталкиваются многие организации. Ложные срабатывания при отсутствии атак будут неправильной реакцией. Ложный негатив есть неспособность выявления действительно вредоносных атак или несанкционированной активности [2].

Наиболее опасны бот-атак (зомби-армия), представляющие собой использование ряда чужих Интернет-компьютеров, владельцы которых не знают, что их ресурс эксплуатируется. Их назначение связано с передачей спама, вирусов и др. на другие компьютеры в сети Интернет. Любой такой компьютер называется зомби или компьютер «Робот», который выполняет операции по заданию атакующего.

Мы разработали простую архитектуру (рис. 1) захвата botnet IRC нападения путем использования Windows honeypot с Yahoo messenger 9 и Wireshark. При этом происходит захват всего трафика данных от сети до нападения, во время него и после.

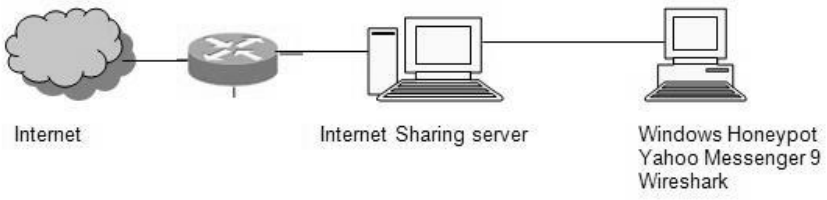

Рис. 1. Архитектура.

Мы применили бесплатный пакет Wireshark-снифер для поиска и устранения сбоев сети, анализа, программного обеспечения и протоколов. На рис.2 показан пример сбора данных с помощью Wireshark для случая атаки на протокол TCP.

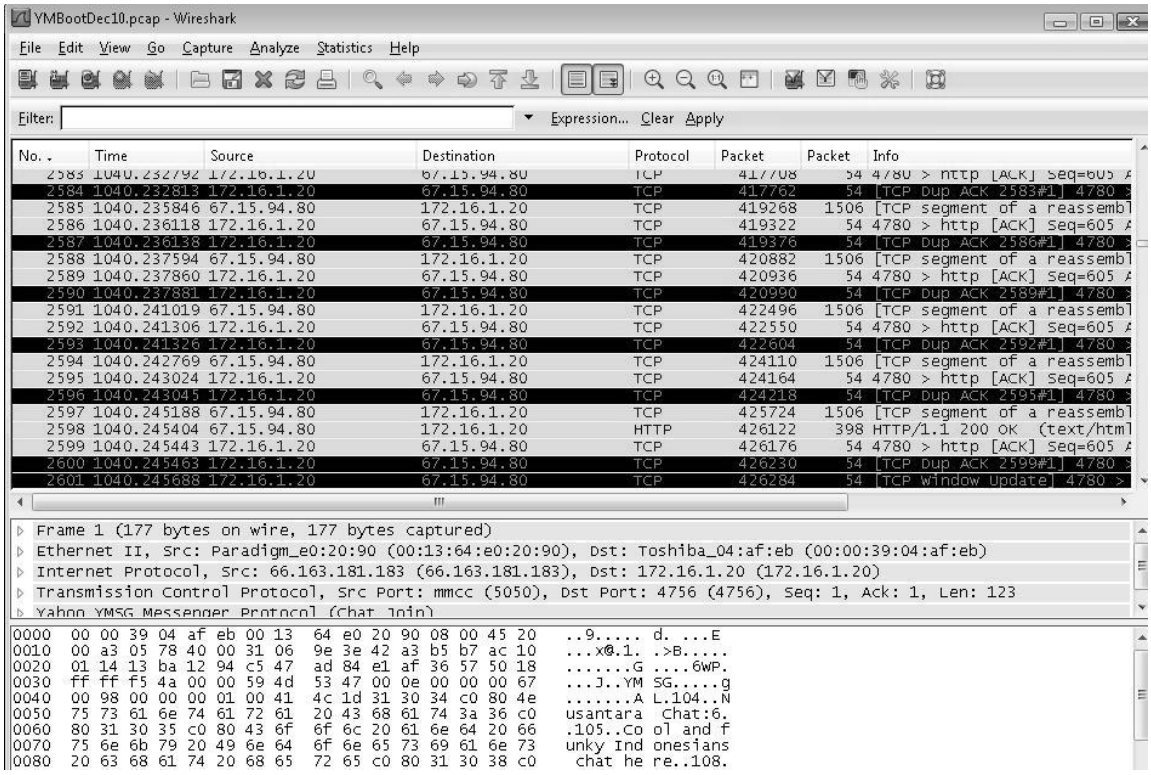

Рис.2 .Пример атаки (получены с помощью Wireshark).

2. Анализ трафика сети на основе спектрального метода

Спектральный анализ позволяет на основе временного ряда получить частотные характеристики, спектральную плотность и др. характеристики. Общие свойства сети пакетной передачи трафика интенсивно исследовались в течение многих лет, для чего применялись различные методы анализа. Большинство исследований опирались на типовые пакеты и сквозную регистрацию. Наше рассмотрение ограничивалось сетевым трафиком при наличие атаки и сравнением с чистым трафиком(без атаки).

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

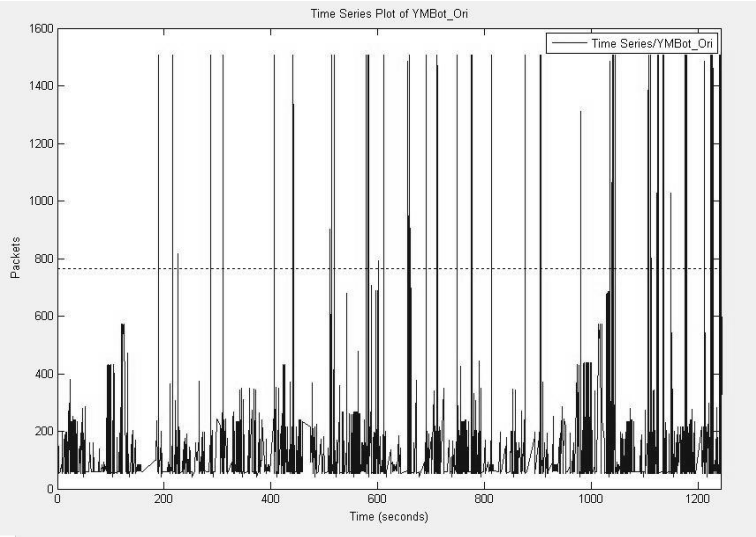

Рис. 3. Трафик с атаками.

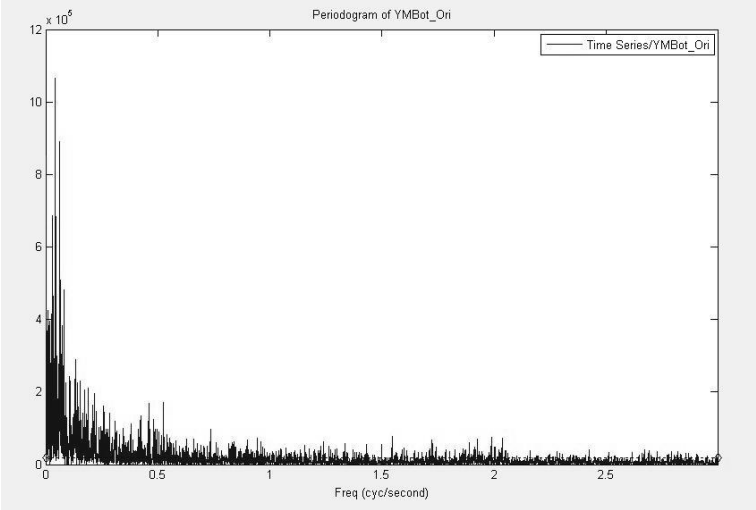

Рис. 4.Периодограмм пакета трафика с атаками.

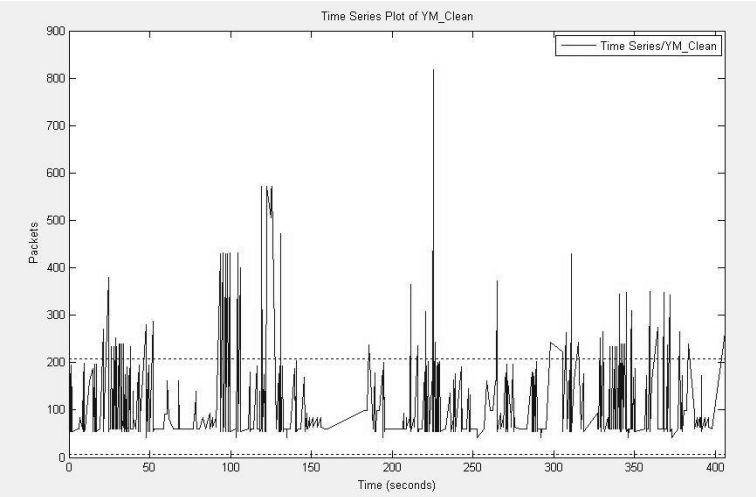

Рис. 5. Трафик без атак.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

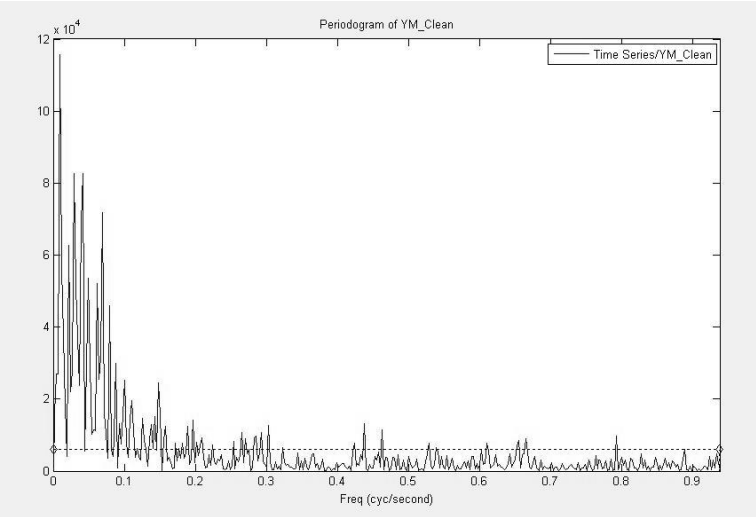

Рис. 6. Периодограмм пакета трафика без атак.

Мы приводим несколько примеров сетевого захваченного трафика. На рис.3, 4 показан трафик при нападении во время сетевых атак. Здесь мы сравнивали с образцом без атак на количестве пакетов более 1500. Рис. 5 и 6 показывают сетевой трафик без нападения во время экспериментов и его спектр. Мы видим, что спектральная плотность с атакой (рис.6) больше чем без атаки (рис.4). Трафик DDoS-атаки обладает высокой периодичностью в транспортном пакете с большим объемом, в то же время трафик без атак обладает меньшей периодичностью.

4. Заключение

Мы предлагаем средство для выявления атак в обычной сети - это анализ временных рядов и применение спектрального метода. Мы сравниваем спектр нормального трафика (без атак) и спектр трафика с нападением.
Градуировка величины спектральной плотности для конкретной сети позволит обнаружить порог атаки для быстрого её обнаружения.

Большинство организаций имеют механизмы для обнаружения атак, это система обнаружения вторжений, брандмауэр-журналы, системные журналы и т.д. Цель этих инструментов выявление подозрительной или несанкционированной деятельности. Однако остаются нерешенными две основные проблемы: обнаружение ложных атак и объемный трафик. Развитие предлагаемого метода путем детального анализа трафика позволит снизить появление ложных негативов.

Литература

1. *The Honeynet Project*. Know your enemy: Learning about security threats // Addison-Wesley, 2004.
2. *The Honeynet Project*. Know your enemy: Statistics // <http://old.honeynet.org/papers/stats/>, 2001.
3. *Wei Ren, Hai Jin.,* Honeynet based distributed adaptive network forensics and active real time investigation // ACM Symposium on Applied Computing, 2005.
4. *Searchsecurity.com,* botnet [Элэктронный ресурс] / Definition // <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1030284,00.html> (по состоянию на 04.02.2009).