

Спектральный анализ трафика сети «Honeypot»

ХУСНИ¹

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

СПбГЭТУ, 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. — Библи. 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 неправомерного или незаконного использовании ресурса [1]. Более ценным свойством Honeypot 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-атаки (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.

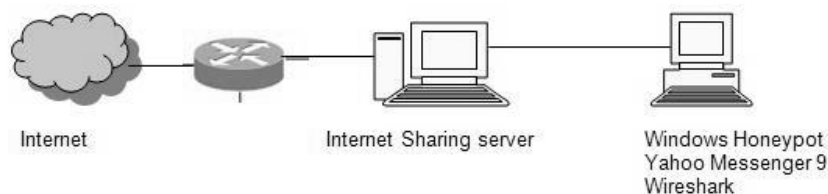


Рис. 1. Архитектура.

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.

The screenshot shows the Wireshark interface with a packet capture of a TCP attack. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Packet, and Info. The bottom pane shows the details of a selected packet (Frame 1) including Ethernet II, Internet Protocol, and Yahoo! Messenger Protocol.

No.	Time	Source	Destination	Protocol	Packet	Packet	Info
2585	1040.232792	172.16.1.20	67.15.94.80	TCP	417708	54	4780 > ntcp [ACK] seq=605 #1 4780 >
2584	1040.232813	172.16.1.20	67.15.94.80	TCP	417762	54	[TCP dup ACK 2583#1] 4780 >
2585	1040.235846	67.15.94.80	172.16.1.20	TCP	419268	1506	[TCP segment of a reassembl
2586	1040.236118	172.16.1.20	67.15.94.80	TCP	419322	54	4780 > http [ACK] seq=605 #1 4780 >
2587	1040.236138	172.16.1.20	67.15.94.80	TCP	419376	54	[TCP dup ACK 2586#1] 4780 >
2588	1040.237594	67.15.94.80	172.16.1.20	TCP	420882	1506	[TCP segment of a reassembl
2589	1040.237860	172.16.1.20	67.15.94.80	TCP	420936	54	4780 > http [ACK] seq=605 #1 4780 >
2590	1040.237881	172.16.1.20	67.15.94.80	TCP	420980	54	[TCP dup ACK 2589#1] 4780 >
2591	1040.241019	67.15.94.80	172.16.1.20	TCP	422496	1506	[TCP segment of a reassembl
2592	1040.241306	172.16.1.20	67.15.94.80	TCP	422550	54	4780 > http [ACK] seq=605 #1 4780 >
2593	1040.241326	172.16.1.20	67.15.94.80	TCP	422604	54	[TCP dup ACK 2592#1] 4780 >
2594	1040.242769	67.15.94.80	172.16.1.20	TCP	424110	1506	[TCP segment of a reassembl
2595	1040.243024	172.16.1.20	67.15.94.80	TCP	424164	54	4780 > http [ACK] seq=605 #1 4780 >
2596	1040.243045	172.16.1.20	67.15.94.80	TCP	424218	54	[TCP dup ACK 2595#1] 4780 >
2597	1040.245188	67.15.94.80	172.16.1.20	TCP	425724	1506	[TCP segment of a reassembl
2598	1040.245404	67.15.94.80	172.16.1.20	HTTP	426122	398	HTTP/1.1 200 OK (text/html)
2599	1040.245443	172.16.1.20	67.15.94.80	TCP	426176	54	4780 > http [ACK] seq=605 #1 4780 >
2600	1040.245463	172.16.1.20	67.15.94.80	TCP	426230	54	[TCP dup ACK 2599#1] 4780 >
2601	1040.245688	172.16.1.20	67.15.94.80	TCP	426284	54	[TCP window update] 4780 >

Frame 1 (177 bytes on wire, 177 bytes captured)
 Ethernet II, Src: Paradigm_e0:20:90 (00:13:64:e0:20:90), Dst: Toshiba_04:af:eb (00:00:39:04:af:eb)
 Internet Protocol, Src: 66.163.181.183 (66.163.181.183), Dst: 172.16.1.20 (172.16.1.20)
 Transmission Control Protocol, Src Port: mmcc (5050), Dst Port: 4756 (4756), Seq: 1, Ack: 1, Len: 123
 Yahoo! Messenger Protocol (chat inin)

```

0000 00 00 39 04 af eb 00 13 64 e0 20 90 08 00 45 20  ..9....d....E
0010 00 a3 05 78 40 00 31 06 9e 3e 42 a3 b5 b7 ac 10  ...x@.1. >B....
0020 01 14 13 ba 12 94 c5 47 ad 84 e1 af 36 57 50 18  ....G...6WP.
0030 ff ff f5 4a 00 00 59 4d 53 47 00 0e 00 00 00 67  ...J.YM SG....g
0040 00 98 00 00 00 01 00 41 4c 1d 31 30 34 c0 80 4e  ....A.L.104..N
0050 75 73 61 6e 74 61 72 61 20 43 68 61 74 3a 36 c0  usantara Chat:6.
0060 80 31 30 35 c0 80 43 6f 6f 6c 20 61 6e 64 20 66  .105..co ol and f
0070 75 6e 6b 79 20 49 6e 64 6f 6e 65 73 69 61 6e 73  unky Ind onesians
0080 20 63 68 61 74 20 68 65 72 65 c0 80 31 30 38 c0  chat he re..108.

```

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).

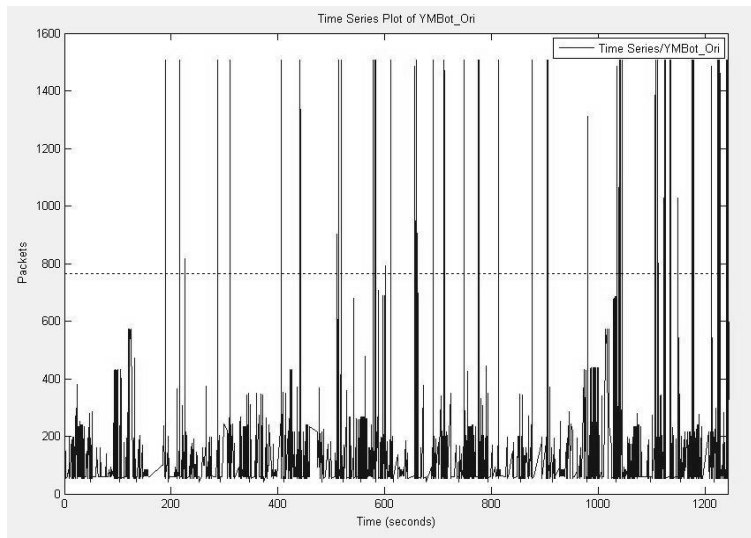


Рис. 3. Трафик с атаками.

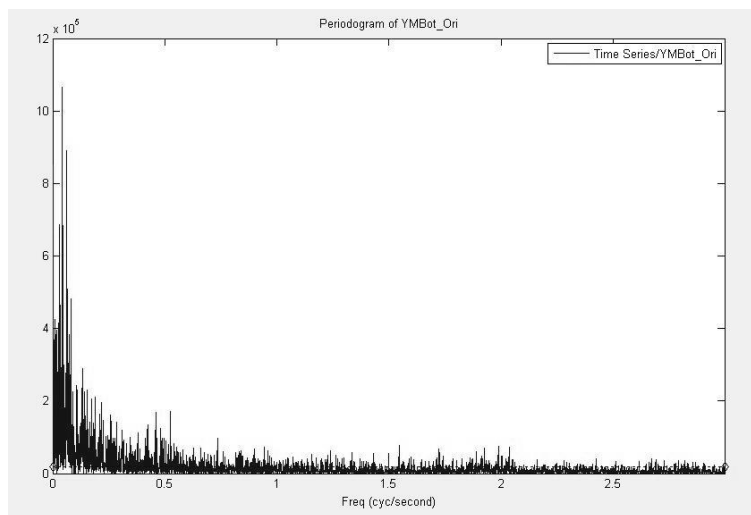


Рис. 4. Периодограмм пакета трафика с атаками.

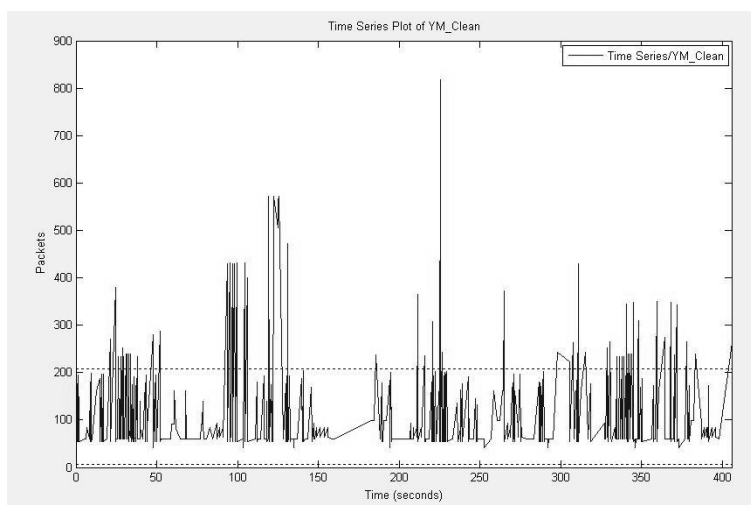


Рис. 5. Трафик без атак.

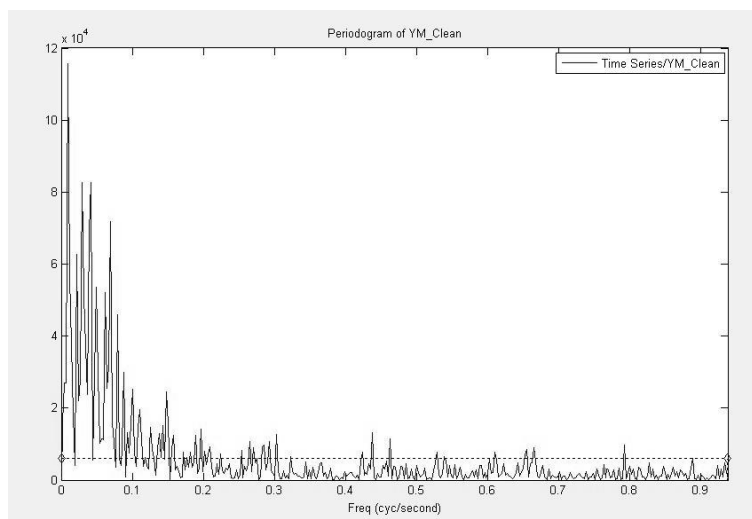


Рис. 6. Периодограмм пакета трафика без атак.

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 [Электронный ресурс] / Definition // <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1030284,00.html> (по состоянию на 04.02.2009).