Метод ловушек в обеспечении безопасности данных

Д.А. Шкирдов[1], Е.С. Сагатов[1], А.М. Сухов[1]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086

Аннотация. В работе представлены результаты анализа данных с географически распределенной сети ловушек. Такие сервера ловушки были развернуты в Самаре, Ростове на Дону, Крыму и США почти два года назад. Собранные данные позволяют построить модель сетевого вторжения. Эта модель включает в себя черные списки атакующих адресов для различных интернет сервисов, всевозможную статистику, в том числе обращения к портам и интернет-услугам.

1. Введение

С начала публичной эксплуатации глобальной сети она подверглась нападениям злоумышленников. Первоначальная цель злоумышленников заключалась в нанесении ущерба другим пользователям глобальной сети, в настоящее время действия злоумышленников все чаще направлены на то, чтобы нарушить техническую инфраструктуру сети в целом. Для достижения этих целей злоумышленники объединялись в группы и координировали свои действия, совершенствуя методы нападения. К деструктивным действиям частных лиц в последние десятилетия активно подключаются специальные службы многих государств, способные влиять на методы вторжений еще на этапе создания сетевого сервиса. То есть, осуществлять эффективный контроль над вторжениями достаточно тяжело, так новые методы взлома появляются и совершенствуются постоянно.

Для того, чтобы держать под контролем процесс появления новых технологий сетевых вторжений необходимо построить соответствующую модель [1]. Модель сетевых вторжений должна содержать ранжированный список типов атак для сетевых сервисов, а также базу данных IP адресов, с которых осуществляются вторжения. Ранжированный список – это список в котором типы атак расположены в порядке убывания частоты их применения. Сначала необходимо идентифицировать тип атаки, а потом найти сколько раз повторяется этот тип [2]. В настоящей статье речь пойдет о создании такой модели и необходимой для этого инфраструктуре.

Встает вопрос – как проводить подобные эксперименты. Работающий сайт с реальными сервисами плохо подходит на эту роль, так как выделить на нем атакующие запросы достаточно сложно. Поэтому для проведения подобных экспериментов идеально подходят сервера ловушки [3]. Это сервера с инсталлированными интернет сервисами, которые отвечают на запросы и записывают все обращения, тем не менее информационное наполнение их не производиться и принимаются меры, чтобы от этих серверов в сеть не попадала никакая информация. Эти сервера размещены на реальных IP адресах, но их сервисы не анонсируют в поисковых системах и сопутствующих базах данных [4]. Таким образом, обратиться к информационным сервисам ловушки можно только при сканировании адресного пространства и специальном обращении к портам. Подобные запросы, повторенные неоднократно, можно считать ключевым признаком, характеризующим вторжения.

Анализ данных с таких серверов ловушек позволяет извлечь сведения, необходимые для построения модели вторжения [5]. Для того, что данные были репрезентативны, необходима инсталляция целой сети серверов, которые покрывают территорию региона, для которого составляется модель. Кроме того, желательно инсталлировать один-два сервера в удаленных регионах, чтобы иметь возможность сделать сравнения и найти региональные особенности.

Конструкция сервера-ловушки определяется набором сервисов, наиболее уязвимых к сетевым вторжениям.

После своего построения сведения о модели вторжения [6] помогут модернизировать защитную инфраструктуру. Во-первых, будут выделены наиболее уязвимые сетевые сервисы на основании данных о числе запросов к ним и числе атакующих адресов. Во-вторых, станут известными механизмы и частота использования тех или иных уязвимостей программного обеспечения, что используют злоумышленники. В-третьих, сформируются базы данных атакующих адресов, которые упростят поиск злоумышленников и средств управления сетями, предназначенными для проведения сетевых атак (так называемых ботнетов). В-четвертых, станет возможным проведение активных мероприятий по разведке ботнетов с искусственным заражением сервера ловушки и отслеживанием дальнейших действий злоумышленников [7].

И, наконец, данные о модели вторжений позволят сформулировать актуальные правила для проведения аудита по сетевой безопасности. Причем эти правила будут обновляться по мере обновления модели. На основании правил для аудита должно быть разработано соответствующее программное обеспечение, которое могло бы работать в локальных сетях и проводить предварительное тестирование наиболее важных сетевых ресурсов.

2. Устройство узла и измерительная инфраструктура

При создании измерительной инфраструктуры необходимо решить две основных проблемы. Первая из них, касается конструкции измерительного узла [8], то есть набора информационных сервисов, инсталлированных на сервере ловушке, а также способе сбора информации о сетевой активности. Вторая проблема заключается в выборе мест для размещения серверов ловушек, а также способов управления полученной сетью [9].

В качестве операционной системы для сервера ловушки выбрана GNU Debian/Linux, так как это свободно распространяемая OS с доступными исходными кодами всего применяемого программного обеспечения [10]. Так как любое сетевое обращение к серверу осуществляется по коммуникационному порту, то контроль над портами является первостепенной задачей. Для осуществления этого контроля применяется ряд программных средств, к ним относятся wireshark, который записывает на внешнем порту весь траффик, утилита iptables, которая управляет межсетевым экраном, а также пакет sFlow предназначенный для учета траффика по технологии NetFlow.

Следующий сервис, который должен быть проанализирован в обязательном порядке, это веб сервис. В составе сервера ловушки были инсталлированы серверы Apache, Nginx. Однако современные реализации HTTP протокола обычно включают базу данных MySQL для хранения контента, а также систему управления траффиком. Поэтому в дополнение к стандартному веб серверу была установлена стандартная база данных.

Для тестирования безопасного удаленного управления по сети был инсталлирован пакет OpenSSH. Общий доступ к сетевым ресурсам осуществлялся с помощью протокола SMB, реализованного с помощью программного пакета Samba. Для получения электронной почты по протоколам POP3 и IMAP были установлены пакеты Dovecot и Exim.

Тестируемые протоколы включают также протокол передачи файлов FTP на основе vsftpd, SIP интернет-телефонию с пакетом Asterisk, прокси сервер с возможностью резервирования Squid, а также сервис доменных имен на базе программного пакета bind9.

Таким образом, была определена конструкция измерительного узла. Но для проведения измерений одного узла недостаточно, для проверки данных необходимо развернуть целую сеть таких узлов. Места их расположения зависят от сообщества, для которого необходимо построить модель сетевой атаки. Так как мы пытаемся построить такую модель для европейской части России, то и сервера ловушки разместим в Самаре, Ростове на Дону и Крыму. Выбор места размещения определялся простотой их развертывания. Для того, чтобы провести дополнительную оценку полученных данных мы инсталлировали подобный сервер на одном из хостингов в США.

Указанная инфраструктура, состоящая из четырех серверов ловушек, была полностью запущена в эксплуатацию в середине марта 2017 года. Информация с тех пор собиралась и накапливалась без перерыва, и мы проанализировали данные за год. Результаты нашего анализа представлены в следующем разделе.

3. Общая статистика по портам

Для обработки первичных данных из log файлов со статистикой были написаны специальные скрипты, которые работали с регулярными выражениями и извлекали необходимые нам данные.
Для начала представим разбиение траффика по портам, которое было получено путем анализа данных NetFlow за месяц. Данные о наиболее загруженных портах в зависимости от типа протоколов сведены в следующую Таблицу.

Таблица 1. Данные о числе запросов по портам.

№ пп	TCP		UDP		ICMP	
	номер порта	число потоков	номер порта	число потоков	тип запроса	число потоков
1	22	284452	5060	280161	8.0	23829
2	80	84934	137	45550	3.3	11989
3	23	43213	111	4509	3.10	1797
4	75	32984	523	2397	3.2	1121
5	3306	32738	0	2262	11.0	787
6	8291	32473	53413	1400		
7	139	13504	1900	1065		
8	21	11277	123	643		
9	8080	10798	53	596		
10	111	10676	11211	406		

Следует отметить, что в Таблице 1 приведены данные только для первых 10ти портов для каждого типа протокола. В графе число потоков показано число завершившихся потоков, которые передавали данные по заданному порту. Поток можно рассматривать как одно соединение между устройствами с фиксированными IP адресами и портами. Так как 10-ти первых строк недостаточно для понимания полной картины доступа по портам, то дополнительно нами представлен ранжированный график допуска по портам.

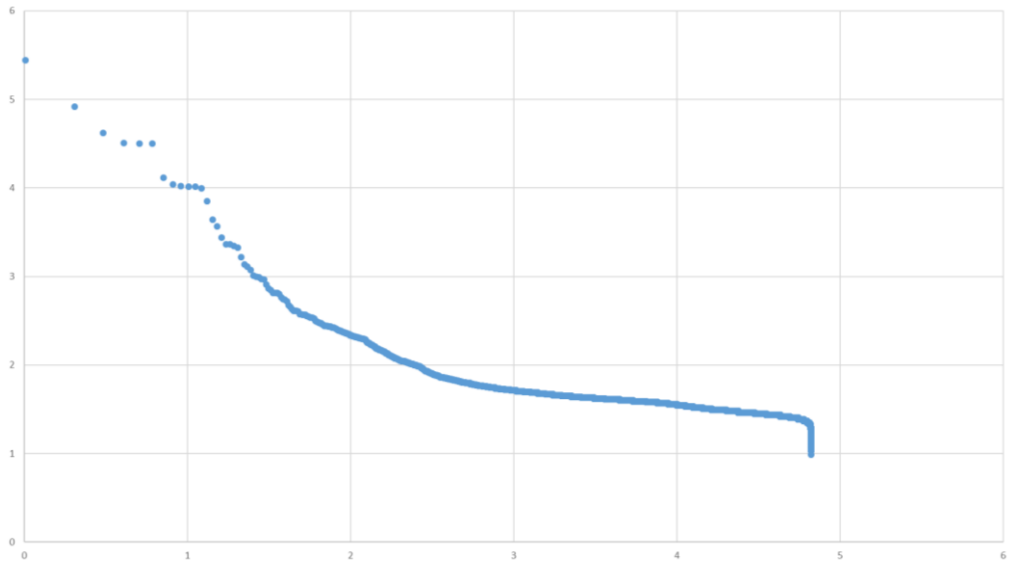

Рисунок 1. Ранжированный список запросов по протоколу TCP.

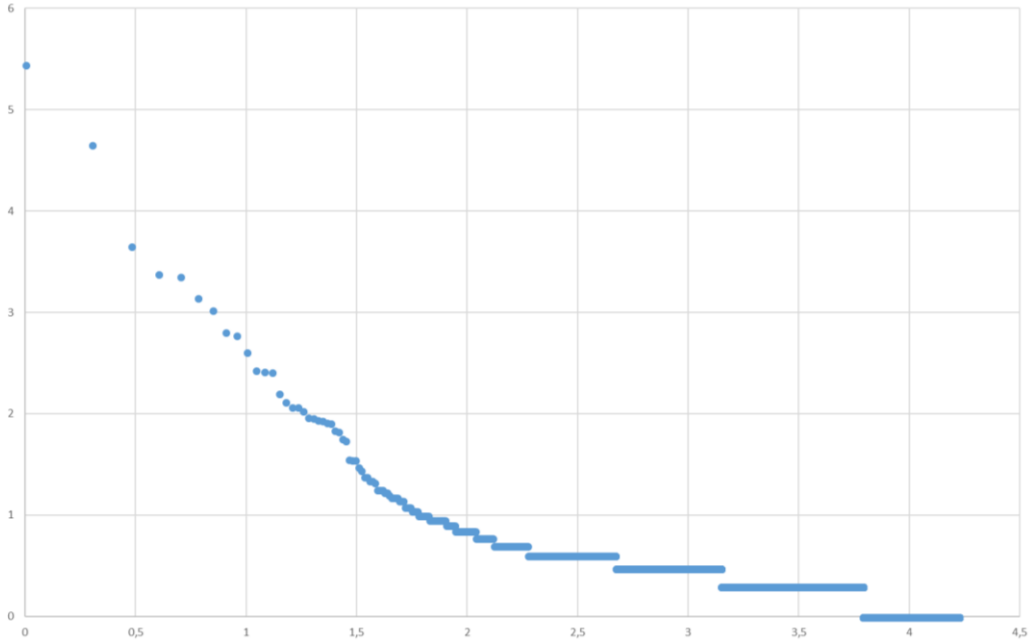

Рисунок 2. Ранжированный список запросов по протоколу UDP.

Следует отметить, что запросы осуществлялись ко всем без исключения портам TCP, причем количество запросов к самому непопулярному порту превысило 10 за один месяц. Однако по UDP были обращения только к 16743 портам и 74.5% портов не были использованы.
Собранная статистика позволяет ранжировать популярность нападений для различных типов интернет сервисов, о которых говорилось в разделе 3. В Таблице 2 выделены первая десятка наиболее популярных для взлома сервисов.

Таблица 2. Список популярности сервисов.

№ пп	Тип сервиса	Порты
1	SSH	22
2	SIP	5060
3	HTTP	80
4	Samba	137, 139
5	Telnet	23
6	MySQL	3306
7	Winbox	8291
8	FTP	21
9	Альтернативный HTTP	8080, 8088, 8888, 8081, etc
10	rpcbind	111

Здесь Winbox это приложение для управления MikroTik RouterOS, а rpcbind - служба вызовов удаленных процедур.

4. Правила обработки статистики на примере сервиса ssh

В этом разделе статьи будут представлены основные данные полученные после обработки статистики с серверов ловушек. Подчеркнем еще раз, что данные этого раздела основываются на лог файлах инсталлированных сервисов. Лог файлы в свою очередь содержат только отклик сервиса на внешние запросы. В этом разделе мы делаем попытку классифицировать угрозы на основании этих откликов. Полное содержание запроса в большинстве случаев остаются для нас неизвестным.
В начале раздела покажем, как обрабатываются данные на примере ssh сервера. Это сервис удаленного управления операционной системой, каждая сессия которого защищена с помощью шифрования, включая передачу пароля для идентификации пользователя. Данные собирались в

течение 2017-2018 годов, общий срок превысил один год. Информация о размере собранных данных размещена в Таблице 3.

Таблица 3. Размеры собранных данных.

Крым	Самара	Ростов-на-Дону	США
1,20 ГБ	1,15 ГБ	0,46 ГБ	2,53 ГБ

Так как данные о сервере ловушке не анонсировались никоим образом (ни через DNS, ни регистрацией в поисковой системе, ни в IP телефонии и т.д.), то все обращения к указанному IP адресу можно считать подозрительными. Тем более подозрительными выглядят обращения к ssh серверу, инсталлированному в составе ловушки.

Атакующие запросы можно разделить на две категории. К первой из них следует отнести запросы по подбору логина и пароля для входа. Если пароль простейший, то существует шанс путем небольшого перебора получить доступ к управлению системой. Вторая категория атакующих запросов пытается использовать выявленные уязвимости программного обеспечения, реализующего серверную часть ssh протокола. Следует отметить, что такие запросы достаточно сложно выявить с помощью анализа log файлов, так как этот содержит только отклики системы.

Анализ запросов, не содержащих попыток подбора набора «логин + пароль», показал, что встречаются четыре основных типа

1. Bad protocol version identification …
2. reverse mapping checking getaddrinfo for …
3. Address x.y.z.d maps to localhost, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
4. Did not receive identification string from x.y.z.d

Ни один из этих типов запросов не пытается использовать уязвимости протокола ssh. Запросы первого типа пытаются прислать не строку идентификации SSH, а другой код. Запросы типа 2 и 3 связаны с ошибочными разрешением доменного имени. Запросы типа 4 констатируют, что идентификатор пользователя не получен.

Таблица 4 содержит данные о количестве уникальных адресов, которые посылали запросы к серверу ловушке. Таблица 5 содержит данные об общем количестве запросов.

Таблица 4. Количество IP адресов, участвующих в запросах к ssh серверу.

	США	Крым	Ростов на Дону	Самара
Всего	15909	15970	15527	16486

Таблица 5. Количество запросов к ssh серверу.

	США	Крым	Ростов на Дону	Самара
Всего	21875655	1E+07	3221026	9002497

Сравнение данных Таблиц 4 и 5 показывает, что IP адреса шлют запросы неравномерно. Среди них есть и случайные устройства, которые посылают запросы по ошибке, их следует удалить из итогового черного списка. Для того, чтобы понять, насколько неравномерно осуществляют запросы различные устройства, построим ранговое распределение. Для этого, при помощи специально написанных скриптов установим, сколько раз посылались запросы с того или иного IP адреса n_i в период сбора статистики. Затем расположим эти адреса в порядке убывания числа запросов и пронумерует эти адреса согласно получившейся очереди. Зависимость числа запросов от места в упорядоченном списке i и есть ранговое распределение. Обычно его изображают на графике с логарифмическими осями $\lg(n_i)$ и $\lg(i)$. Полученный график можно найти на рис. 3.

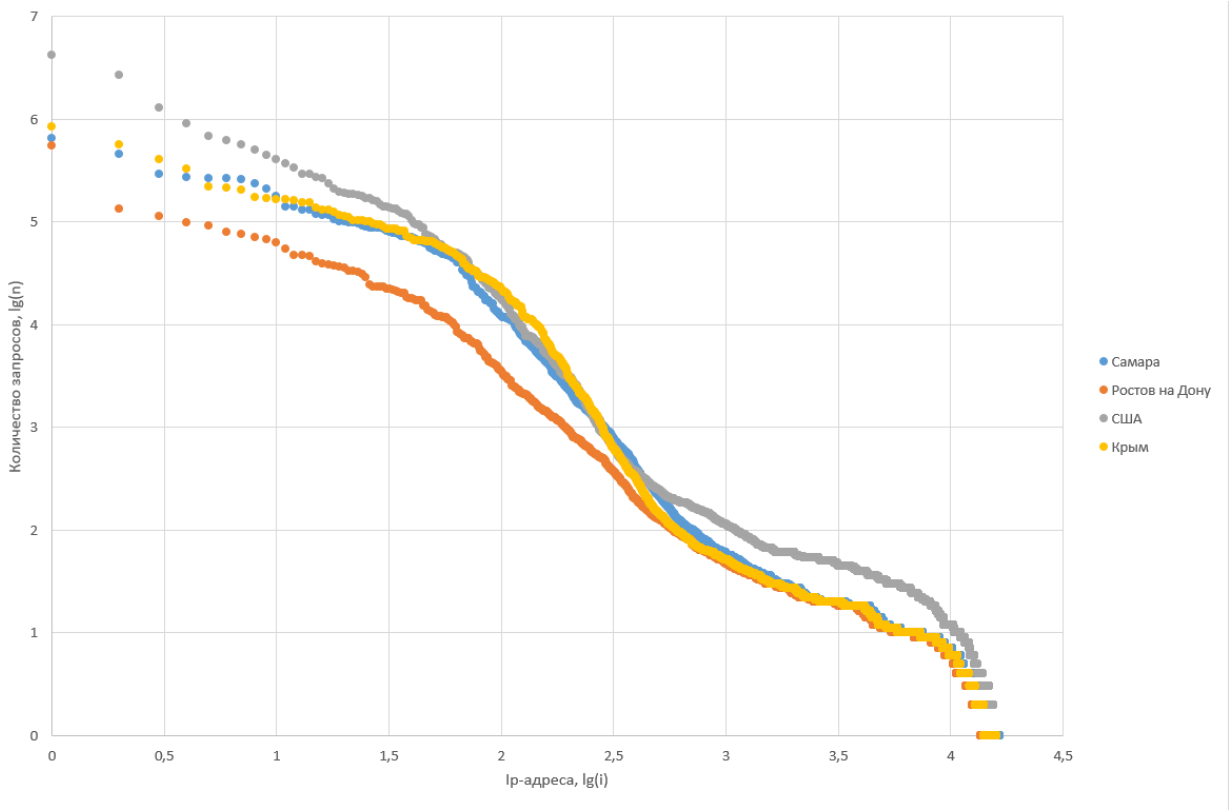

Рисунок 3. Ранговое распределение для числа запросов к ssh.

Самые активные IP адреса умудрились послать порядка миллиона запросов к ssh серверу. В то же время значительная часть адресов обращалась лиши однажды.
Следующая часть анализа посвящена совпадению атакующих узлов для географически распределенной сети серверов ловушек.

Таблица 6. Количество совпавших IP для двух узлов.

	США	Крым	Ростов на Дону	Самара
США	15909	15%	15%	14%
Крым	4201	15970	17%	16%
Ростов на Дону	4099	4560	15527	16%
Самара	4051	4414	4373	16486

В Таблице 6 приведены данные о количестве совпавших IP адресов, посылающих запросы к ssh, для каждой пары серверов-ловушек. По диагонали стоит общее число уникальных адресов, посылавших запросы к данной ловушке. Ниже диагонали в ячейке указано число совпадающих IP адресов для двух серверов ловушек, выше диагонали приведен соответствующий процент.
В Таблице 7 приведены данные о количестве адресов, с которых запросы посылались к трем и четырем ловушкам.

Таблица 7. Количество совпавших IP адресов для трех и более ловушек.

Крым, Самара, Ростов на Дону	3079
Крым, США, Ростов на Дону	2874
Самара, США, Ростов на Дону	2717
Крым, Самара, США	2793
Крым, Самара, США, Ростов на Дону	2235

Однако, график с рисунка 3 показывает, что количество запросов с единичного IP адреса может сильно разниться. Нам необходимо понять, как распределено это количество, и сколько запросов совпадает для двух, трех и четырех ловушек. В Таблице 8 показано попарное совпадение запросов для серверов ловушек.
Сравнение данных Таблиц 8 и 9 показывает, что совпадающие запросы исходят от IP адресов из верхней части рангового распределения. То есть подбор пароля осуществляют одни и те же атакующие сервера. В то время как адреса из нижней части (хвоста) рангового распределения скорее всего обращались только к одному серверу ловушке, да и то по случайности.

Таблица 8. Количество совпавших запросов.

	США	Крым	Ростов на Дону	Самара
США	21875655	40%	38%	46%
Крым	13021228	10352958	61%	56%
Ростов на Дону	9485649	8277703	3221026	57%
Самара	14235002	10856564	6978442	9002497

Таблица 9 содержит данные о количестве совпадающих запросов для 3 и 4 серверов ловушек. Наибольшая корреляция между атакующими запросами наблюдается на российских ловушках.

Таблица 9. Совпадение запросов для 3 и 4 серверов-ловушек

	Количество запросов	Соотношение от общего числа запросов
Крым, Самара, Ростов на Дону	11854523	53%
Крым, США, Ростов на Дону	13383641	38%
Самара, США, Ростов на Дону	12295278	36%
Крым, Самара, США	15314147	37%
Крым, Самара, США, Ростов на Дону	15832904	36%

В заключение хотелось бы обсудить вопрос о критериях включения адрес в черный список атакующих адресов и на основании этих критериев составить сам черный список.
В основу критериев положено два основных свойства – повторяемость атакующих действий и их географическая распространенность. То есть с IP адреса, внесенного в черный список, атаки должны производиться не менее трех раз, а целью этих атак должно стать не мене двух серверов ловушек. В результате обработки данных в черный список вошло 7475 адресов.
Диаграмма с рисунка 4 содержит распределение IP адресов из черного списка по странам.

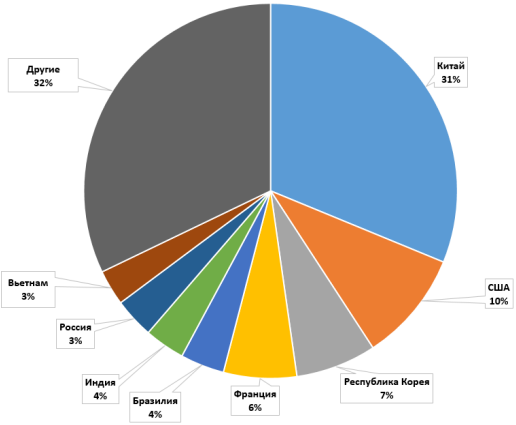

Рисунок 4. Распределение IP адресов по странам.

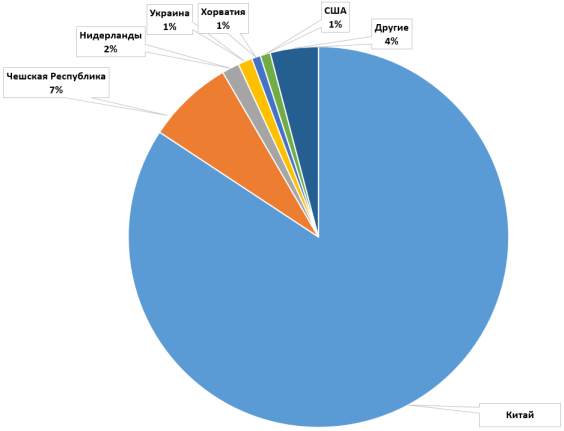

Рисунок 5. Распределение атакующих запросов по странам.

Диаграмма с рисунка 5 содержит распределение атакующих запросов по странам.

5. Общая статистика для интернет-сервисов

После того, как будут обработаны log файлы для все десяти интернет сервисов, хотелось бы увидеть сравнительные таблицы для основных типов переменных, характеризующих атаки. Первая из этих таблиц должна содержать данные о количестве адресов в черном списке для каждого сервиса, инсталлированного в составе ловушки.

Таблица 10. Количество адресов в черном списке.

№ пп	Тип сервиса	Число адресов в черном списке
1	iptables	76 278
2	samba	66 262
3	web	7 870
4	ssh	7 475
5	sip телефония	1 914
6	mysql	1 039
7	dns	657
8	mail	387
9	ftp	360
10	squid	279

Естественно, что самый большой список атакующих адресов получен при помощи межсетевого экрана. Он засекает обращение по любым портам и типам протоколов, следовательно, размер его черного списка является наиболее полным. Он содержит атакующие адреса всех сетевых протоколов. Удивительным является тот факт, что на втором месте по количеству атакующих адресов расположен сервис samba, который позволяет обращаться к дискам и принтерам из различных операционных систем.

Кроме числа адресов в черном списке необходимо понять, с какой частотой ведутся атаки, производиться ли один атакующий запрос раз в день или несколько раз в минуту. Для этого необходимо проанализировать число запросов к тому или иному серверу. В Таблице 11 собраны данные по числу запросов ко всем сервисам. Так как данные собирались с четырех серверов ловушек, то количество запросов к сервису также было разным. В третий столбец Таблицы 11 заносилось наибольшее число запросов из всех мест сбора статистики, а также указывалось месторасположение сервера. В Таблицу 11 добавлен дополнительный столбец, который показывает интенсивность входящего потока запросов.

Таблица 11. Анализ интенсивности запросов.

№ пп	Тип сервиса	Количество запросов к сервису	Интенсивность запросов
1	sip телефония	490 766 969 (Самара)	15,6 запроса в секунду
2	iptables	45 934 880 (США)	1,5 запроса в секунду
3	ssh	21 875 665 (США)	0,7 запроса в секунду
4	samba	14 540 573 (США)	0,5 запроса в секунду
5	DNS	617 221 (США)	1,2 запроса в минуту
6	web	471 381 (Самара)	0,9 запроса в минуту

7	mysql	134 677 (Самара)	15 запросов в час
8	mail	41319 (Самара)	4,7 запроса в час
9	squid	9 271 (Крым)	1 запрос в час
10	ftp	1217 (Ростов)	3,3 запроса в сутки

Следует отметить, что число запросов к одному и тому же сервису изменялось незначительно для различных географических мест. Исключение составляет сервисы ftp и samba, к серверу ловушке, размещенному в США за год вообще не было зафиксировано попыток доступа к ftp, в то время как к мультиоперационному сервису samba число обращений было на три порядка выше, чем к ловушкам в России. Следует обратить внимание и на частоту попыток позвонить, используя sip телефонию, а также общую частоту сканирования различного рода интернет сервисов.

Еще одним полезным типом информации о структуре вторжений является анализ стран с IP адресов которых происходят атакующие запросы. Такая информация собрана в Таблицах 12 и 13. В этих Таблицах для каждого из интернет сервисов приведены первые три страны из рейтинга вторжений. Таблица 13 построена на основе данных по IP адресам, а Таблица 13 содержит данные по количеству запросов. В каждой ячейке, где указана страна, приведены также данные о процентном вкладе ее в общую структуру атакующих запросов.

Таблица 12. Страны-лидеры по количеству атакующих адресов.

№ пп	Тип сервиса	Страны, с IP адресов которых, производятся атаки		
1	iptables	Китай (14%)	США (14%)	Индия (7%)
2	samba	Россия (14%)	Вьетнам (12%)	Индонезия (12%)
3	web	США (13%)	Китай (8%)	Индия (6%)
4	ssh	Китай (31%)	США (10%)	Республика Корея (7%)
5	sip телефония	Франция (24%)	США (22%)	Германия (16%)
6	mysql	Китай (82%)	США (9%)	Бразилия (1%)
7	dns	США (26%)	Китай (19%)	Россия (8%)
8	mail	США (41%)	Франция (11%)	Россия (10%)
9	ftp	США (30%)	Франция (15%)	Россия (11%)
10	squid	Россия (18%)	Китай (17%)	США (16%)

Таблица 13. Страны лидеры по количеству атакующих запросов.

№ пп	Тип сервиса	Страны, с IP адресов которых, производятся атаки		
1	sip телефония	Франция (41%)	Нидерланды (24%)	Германия (9%)
2	iptables	Франция (40%)	Германия (24%)	Россия (14%)
3	ssh	Китай (83%)	Чехия (7%)	Нидерланды (2%)
4	samba	Россия (13%)	Вьетнам (11%)	Индия (8%)
5	DNS	Китай (90%)	Нидерланды (2%)	США (2%)

6	web	Украина (24%)	США (20%)	Франция (18%)
7	mysql	Китай (82%)	США (9%)	Гонконг (2%)
8	mail	США (41%)	Франция (11%)	Россия (10%)
9	squid	Франция (38%)	Россия (12%)	Литва (11%)
10	ftp	Литва (77%)	Франция (10%)	США (8%)

Данные этих Таблиц убедительно свидетельствуют о том, из какой страны осуществляется подавляющее большинство атак. К первой тройке таких стран можно отнести Францию, Китай и США.

Также данные Таблиц 10, 11, 12, 13 позволяют выделить основные типы вторжений. Наибольшую угрозу представляет подбор пароля (простой пароль это до 90% всех инцидентов, связанных со взломами)

Недостатки программного обеспечения — это вторая по популярности угроза. Анализ данных показывает, что наибольшее количество дыр можно найти в сервисе samba, но критические уязвимости могут встречаться и у web серверов, баз данных и почтовых серверов.

6. Выводы

В настоящей работе мы представили ряд результатов, которые были получены при помощи метода приманок. Под приманкой мы понимаем сервер на котором инсталлированы 10 наиболее популярных интернет сервисов, причем этот сервер установлен анонимно, без извещений и регистрации, но на реальном IP адресе. Поэтому, повторяющиеся обращения к серверу ловушке можно считать подозрительными.

Анализ лог файлов сети ловушек, сервера которой разбросаны по миру, позволяют составить модель сетевого вторжения. Такая модель состоит из ряда элементов. В данной работе представлена статистика обращений по портам и протоколам, проанализирована популярность установленных интернет сервисов.

Приведен подробный анализ данных собранный при атаках на веб-сервис. Проведен географический анализ данных с привязкой к географически распределенным серверам ловушкам. Обсуждены правила занесения IP адреса в черный список и представлен список таких адресов. Выделены основные типы атакующих запросов, а также составлен их ранжированный список. Объем полученных данных достаточно большой, в настоящей статье приведена только небольшая часть результатов. Мы предполагаем в ближайшее время представить новую статистику, полученную при обработке полученных данных.

7. Литература

[1] Lee, W. A data mining framework for building intrusion detection models. In Security and Privacy / W. Lee, S. J. Stolfo, K.W. Mok // Proceedings of the IEEE Symposium. – 1999. – P. 120-132.

[2] Stoll, C. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage // Pocket Books. – New York,1990.

[3] Wang, R. Identifying Internet background radiation traffic based on traffic source distribution / R. Wang, Z. Liu, M. Tao, L. Zhang //Journal of High Speed Networks. – 2015. – Vol. 21(2). – P. 107-120.

[4] Spitzner, L. The honeynet project: Trapping the hackers // IEEE Security & Privacy. – 2003. – Vol. 99(2). – P. 15-23.

[5] Kabiri, P. Research on intrusion detection and response: A survey / P. Kabiri, A.A. Ghorbani // Network Security. – 2005 – Vol. 1(2). – P. 84-102.

[6] Bhuyan, M.H. Towards Generating Real-life Datasets for Network Intrusion Detection / M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita // Network Security. – 2015. – Vol. 17(6). – P. 683-701.

[7] Wang, R. Identifying Internet background radiation traffic based on traffic source distribution / R. Wang, Z. Liu, M. Tao, L. Zhang // Journal of High Speed Networks. – 2015. – Vol. 21(2). – P. 107-120.
[8] Carrasco, A. A Proposal for a New Way of Classifying Network Security Metrics: Study of the Information Collected through a Honeypot / A. Carrasco, J. Ropero, P.R. de Clavijo, J. Benjumea, A. Luque // IEEE International Conference on Software Quality, Reliability and Security Companion. – 2018. – P. 633-634.
[9] Singh D. Collaborative ids framework for cloud // International Journal of Network Security. – 2016. – Vol. 18(4). – P. 699-709.
[10] Bhingarkar, A.S. A survey: Securing cloud infrastructure against edos attack / A.S. Bhingarkar, B.D. Shah // The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2015. – P. 16.

Honeypot method in data security

D.A. Shkirdov [1], **E.S. Sagatov**[1], **A.M. Sukhov**[1]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086

Abstract. The paper presents the results of data analysis from a geographically distributed honeypots network. Such honeypots servers were deployed in Samara, Rostov-on-Don, Crimea and the USA almost two years ago. The collected data allows to build a network intrusion model. This model includes blacklists of attacking addresses for various Internet services, all sorts of statistics, including calls to ports and Internet services.