KASPERSKY lab

DDOS-АТАКИ В ТРЕТЬЕМ КВАРТАЛЕ 2015 ГОДА

Содержание

События квартала

Мы выбрали события третьего квартала, которые, на наш взгляд, иллюстрируют основные направления развития в сфере DDoS-атак и инструментов для их осуществления:

- DDoS-атаки на финансовые организации с целью вымогательства;
- новые техники, позволяющие увеличить мощность атак за счет манипуляций с веб-страницами;
- активное развитие Linux-ботнетов для DDoS-атак.

Атаки на финансовые организации

В третьем квартале 2015 года увеличилась активность известной хакерской группы DD4BC, которая атаковала ряд крупных банковских организаций в различных странах мира, в том числе в России. Данная преступная группа известна с сентября 2014 года и осуществляет DDoS-атаки на банки, медиа-группы и игровые компании. Злоумышленники используют атаки, направленные на отказ в обслуживании, как средство вымогательства. У владельца атакуемого ресурса требуют выкуп от 25 до 200 биткойнов (6500 – 52500 USD), в случае неуплаты – угрожают вывести в офлайн его серверы. Ранее жертвами атак группы стали, в частности, организации из Австралии, Новой Зеландии и Швейцарии, предупреждение получили крупные финансовые организации Гонконга. О незаконных действиях известили Банк Китая и Банк Восточной Азии. В третьем квартале группой DD4BC были атакованы и некоторые российские финансовые организации, они также получили от злоумышленников сообщения с требованием заплатить за прекращение атаки определенную сумму в криптовалюте.

Необычный сценарий атаки

Компания CloudFlare сообщила об обнаружении необычного сценария DDoS-атаки. Сайт одного из клиентов CloudFlare находился под атакой, суммарная мощность которой составляла 275 000 HTTP-запросов в секунду. Примечательным является тот факт, что злоумышленники задействовали вредоносный JavaScript, внедренный в рекламу. Iframe с вредоносной рекламой, содержащей JavaScript, запускался в браузерах многочисленных пользователей, и в результате рабочая станция пользователя начинала отправлять XHR-запросы жертве. Эксперты полагают, что подобную вредоносную рекламу могут отображать и некоторые легитимные приложения.

Активность XOR-DDoS бота

Специалисты компании Akamai Technologies зафиксировали рост мощностей DDoS-ботнета, состоящего из Linux-компьютеров, жертвами которого преимущественно стали азиатские сайты образовательных учреждений и игровых сообществ. Особенностью бота является использование XOR-шифрования как в самой вредоносной программе, так и для коммуникаций C&C-серверами. При этом для своего распространения бот использует брутфорс паролей от учетной записи root в Linux-системах.

Как известно, операционная система Linux чаще всего используется в качестве серверной ОС, а это значит, что у сервера также имеются канальные и вычислительные ресурсы, которые злоумышленники в дальнейшем могут использовать для осуществления DDoS-атак. Данный

ботнет уже успешно реализует DDoS-атаки мощностью 109-179 ГБ/с при помощи сценариев типа «SYN flood» и «DNS flood».

По данным «Лаборатории Касперского», ботнеты из Linux-серверов, зараженные ботом XOR-DDoS, активно атаковали ресурсы, расположенные в Китае.

Доступный DDoS

С одной стороны, программное обеспечение, которое используется для осуществления DDoS-атак, усложняется, с другой — инструменты для проведения DDoS-атак становятся доступнее и проще. Как следствие, организация и осуществление DDoS-атаки не требует особых технических познаний атакующих. Более-менее грамотный злоумышленник легко может организовать атаки с усилением, достигающие значительной мощности.

Данный факт подтверждается атаками на образовательный портал республики Татарстан, которые осуществляли студенты, пытаясь таким образом блокировать коммуникации преподавателей и родителей. Атакующие в течение года раз за разом упорно и безрезультатно атаковали портал, находящийся под защитой Kaspersky DDoS Prevention, чем и привлекли внимание экспертов «Лаборатории Касперского».

Доступность и простота использования инструментов для проведения DDoS-атак приводит к тому, что ширится диапазон атакуемых целей. Традиционно считается, что DDoS-атакам подвергаются преимущественно финансовые организации, государственные учреждения, коммерческие компании и СМИ. Но практика показала, что мишенью DDoS-атаки может стать любой ресурс, вызвавший недовольство нескольких аморальных интернет-пользователей, — даже образовательный портал.

Статистика DDoS-атак с использованием ботнетов

Методология

Система DDoS Intelligence является частью решения Kaspersky DDoS Prevention, предназначена для перехвата и анализа команд, поступающих ботам с серверов управления и контроля, и не требует при этом ни заражения каких-либо пользовательских устройств, ни реального исполнения команд злоумышленников.

За отдельную (одну) DDoS-атаку в данном отчете принимается та, во время которой перерыв между периодами активности ботнета не превышает 24 часов. Так, например, в случае, если один и тот же ресурс был атакован одним и тем же ботнетом с перерывом в 24 часа и более, это рассматривается как две атаки. Также за отдельные атаки засчитываются запросы на один ресурс, но произведенные ботами из разных ботнетов.

Географическое расположение жертв DDoS-атак и серверов, с которых отправлялись команды, определяется по их IP-адресам. Количество уникальных мишеней DDoS-атак в данном отчете считается по числу уникальных IP адресов в квартальной статистике.

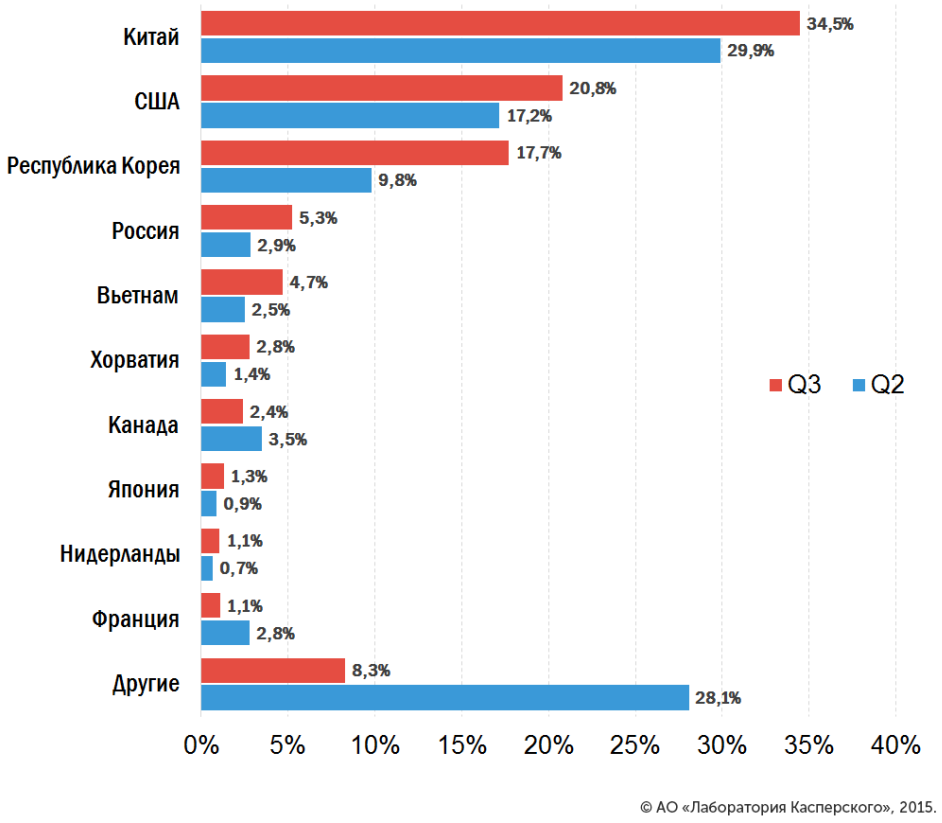
Важно отметить, что статистика DDoS Intelligence ограничена только теми ботнетами, которые были обнаружены и проанализированы «Лабораторией Касперского». Следует также понимать, что ботнеты – это лишь один из инструментов осуществления DDoS-атак, и представленные в данном отчете данные не охватывают все без исключения DDoS-атаки, произошедшие за указанный период.

Итоги квартала

- В третьем квартале 2015 года DDoS-атакам подвергались цели, расположенные в 79 странах мира.
- 91,6% атакованных ресурсов были расположенные в 10 странах мира.
- Китай, США и Республика Корея остаются лидерами как по количеству зафиксированных атак, так и количеству жертв, страдающих от DDoS-атак.
- Наиболее продолжительная DDoS-атака в третьем квартале 2015 года продолжалась 320 часов (13,3 дней).
- Самыми популярными методами атаки по-прежнему остаются SYN-DDoS, TCP-DDoS и HTTP-DDoS.
- Linux-боты активно используются киберпреступниками, доля DDoS-атак с ботнетов на основе ОС Linux в третьем квартале составила 45,6%.

География атак

В третьем квартале 2015 года мишенями DDoS-атак стали ресурсы, расположенные в 79 странах мира. 91,6% атакованных ресурсов были расположены в 10 странах.

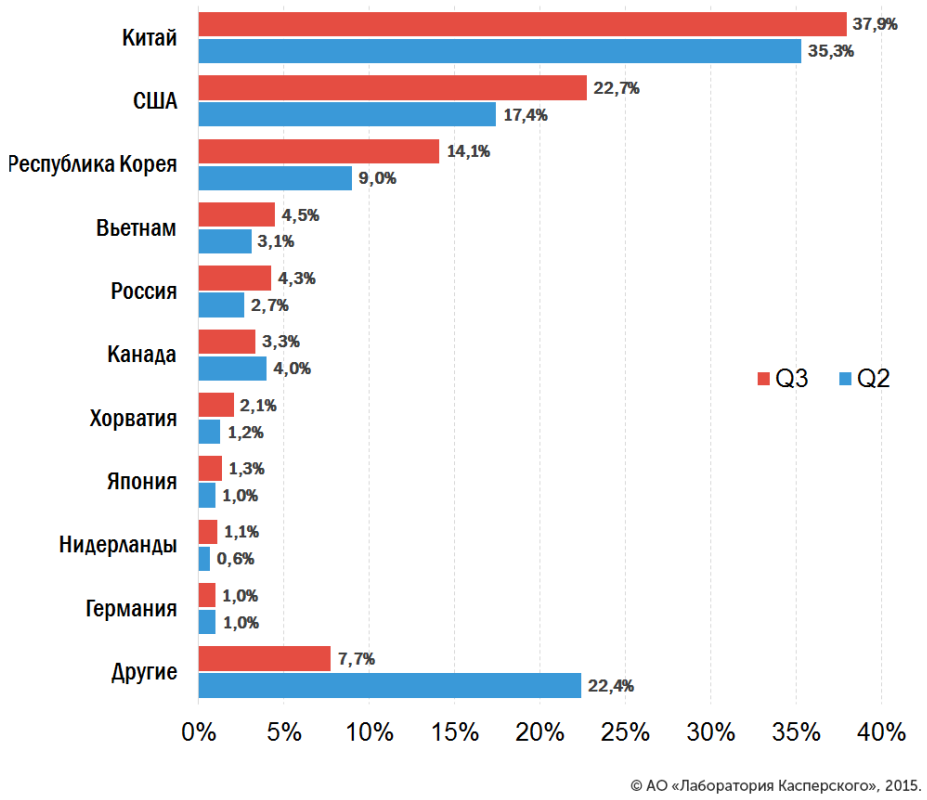


Распределение уникальных мишеней DDoS-атак по странам, Q2 и Q3 2015

В рейтинге стран по количеству атакованных уникальных ресурсов по-прежнему лидирует Китай, где в третьем квартале были расположены 34,5% мишеней DDoS-атак — это на 4,6 п.п. больше, чем в предыдущем квартале. Второе место удерживают США с 20,8%. На третьем месте осталась Южная Корея с 17,7%. Отметим, что показатель этой страны увеличился наиболее значительно — на 7,9 п.п.

Вернулись в первую десятку Нидерланды (1,1%). Новичок рейтинга — Япония, на которую пришлось 1,3% всех атакованных ресурсов. Германия (1,0%) и Гонконг (0,9%) вышли из ТОР 10.

Данные о количестве отмеченных атак показывают, что 92,3% атак (это на 14,7 п.п. больше, чем во втором квартале) пришлось на 10 стран:



Распределение DDoS-атак по странам, Q2 и Q3 2015

В третьем квартале тройка лидеров не изменилась и в этом рейтинге – Китай (37,9%), США (22,7%) и Южная Корея (14,1%). По числу атак Нидерланды (1,1%) и Япония (1,3%) также вытеснили из ТОР 10 Францию (0,9%) и Гонконг (0,9%). Больше всего за квартал увеличилась доля атак на США — на 5,4 п.п.

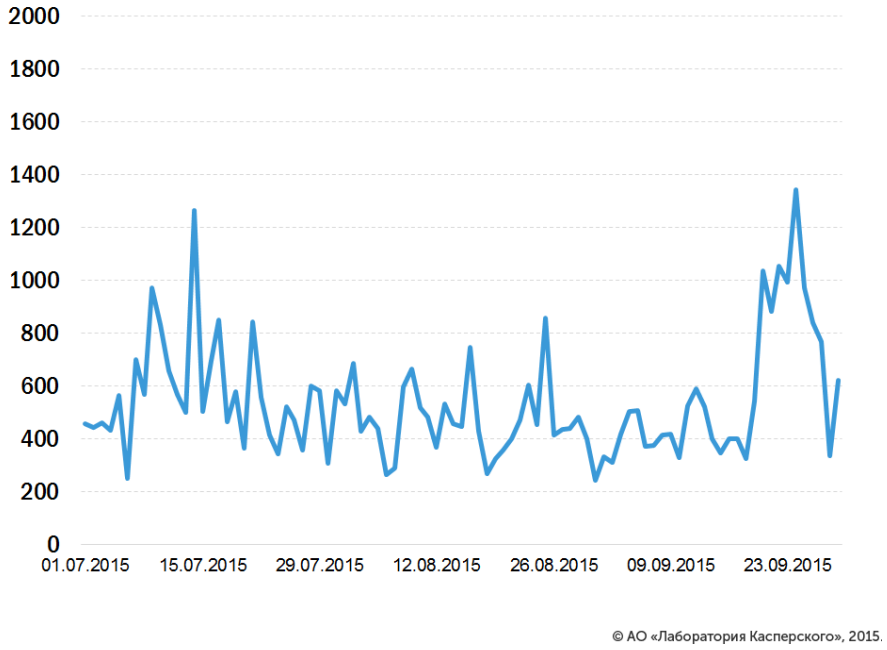
Показатели первой тройки стран в обоих рейтингах — как по числу атак, так и по числу целей — увеличились больше, чем у других стран из ТОР 10. Бессменное лидерство Китая и США в

рейтингах по числу атак и по количеству мишеней обусловлено дешевизной веб-хостинга в этих странах, вследствие чего большинство целевых веб-ресурсов располагаются именно там.

Лидером по количеству атак стал IP-адрес, предположительно принадлежащий дата-центру в Гонконге – в течение квартала его атаковали 22 раза.

Динамика числа DDoS-атак

В третьем квартале 2015 года DDoS-активность была распределена неравномерно, с двумя пиками: первый пришелся на середину июля, второй на конец сентября. Самым спокойным оказался период с начала августа до середины сентября.

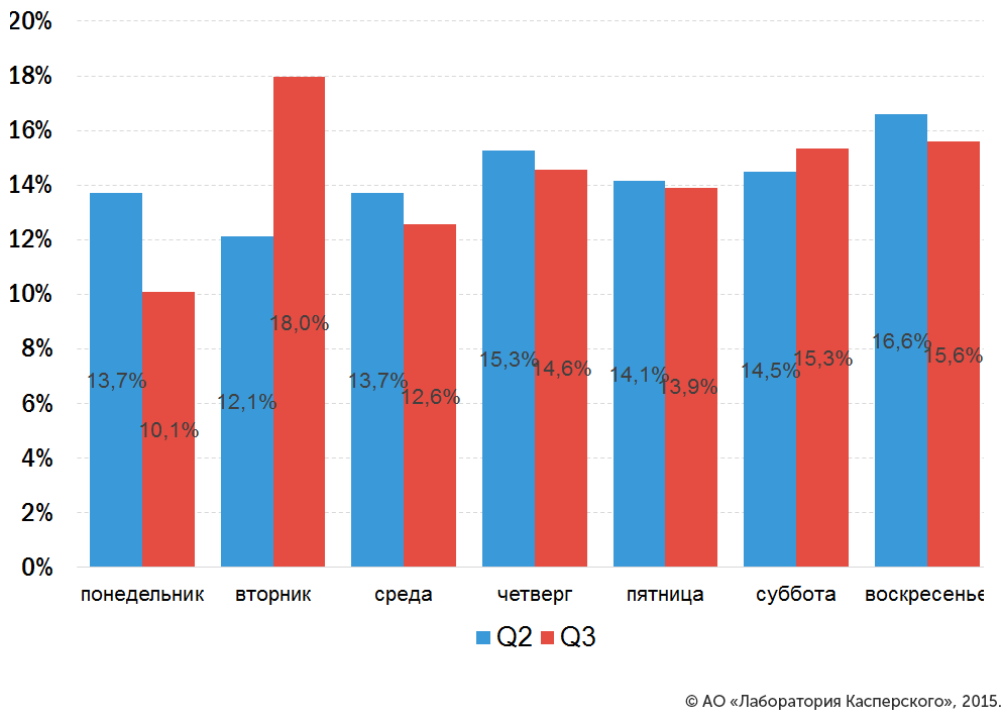


Динамика числа DDoS-атак, Q3 2015*

** В связи с тем, что DDoS-атаки могут продолжаться непрерывно несколько дней, в таймлайне одна атака может считаться несколько раз – по одному разу за каждый день.*

Больше всего атак — 1344 — пришлось на 24 сентября.

Самым активным днем недели по DDoS-активности стал вторник:



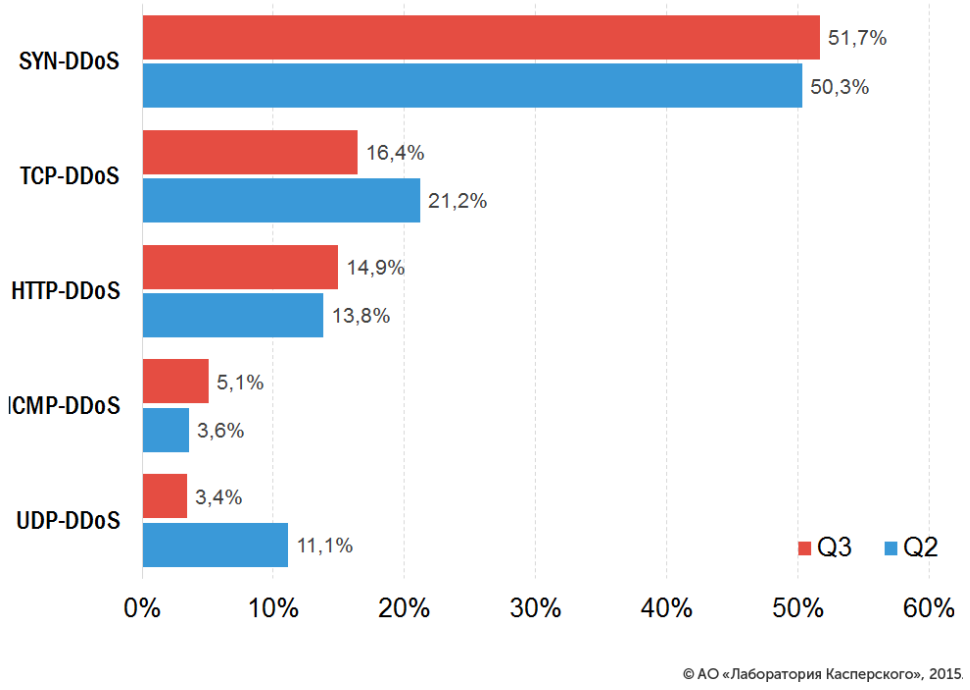
Распределение DDoS-атак по дням недели

Лидерство вторника обусловлено резким ростом количества атак в этот день недели 14 июля и 22 сентября. Отметим, что в эти дни были особенно активны ботнеты из Linux-серверов, зараженных ботом XOR-DDoS, которые атаковали ресурсы в Китае.

Типы и длительность DDoS-атак

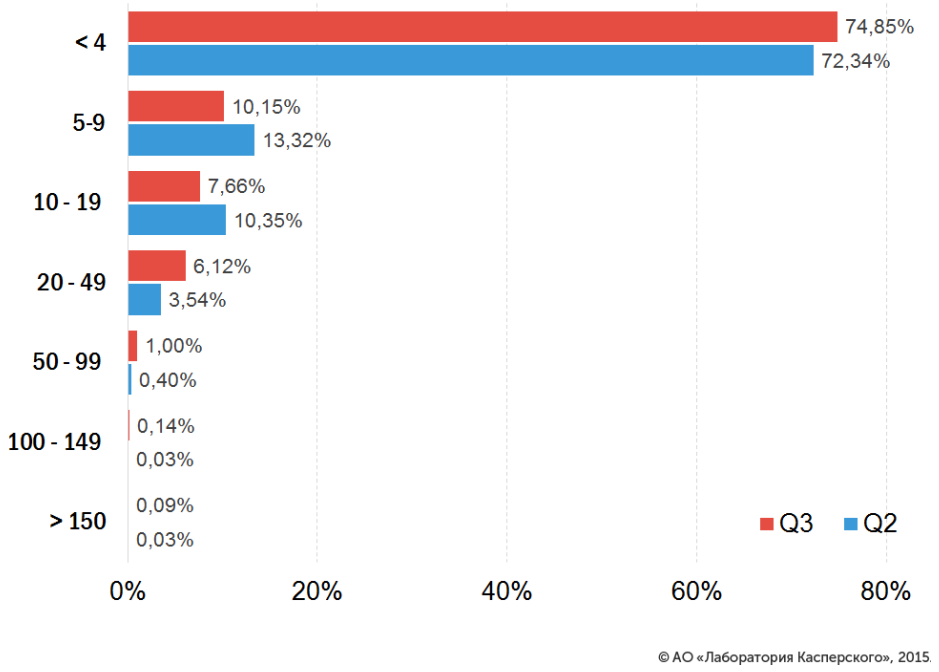
В третьем квартале 2015 года злоумышленники применяли ботов одного семейства для атак на 99,3% целей (в предыдущем квартале этот показатель составил 98,2%). Боты двух разных семейств (либо заказчики обращались к нескольким исполнителям) применялись для атак на лишь 0,7% целей, три и более семейств ботов – в атаках на 0,02% целей.

В третьем квартале более половины атак пришлось на SYN-DDoS (51,7% всех атак), доля TCP-DDoS составила 16,4%, HTTP-DDoS — 14,9%. На четвертое место поднялся метод ICMP-DDoS, чей показатель за два последних квартала увеличился более чем вдвое и составил 5,1%.



Распределение DDoS-атак по типам

Как и прежде, подавляющее большинство атак в третьем квартале 2015 года продолжалось менее суток, при этом заметно выросло количество атак продолжительностью в неделю и больше.



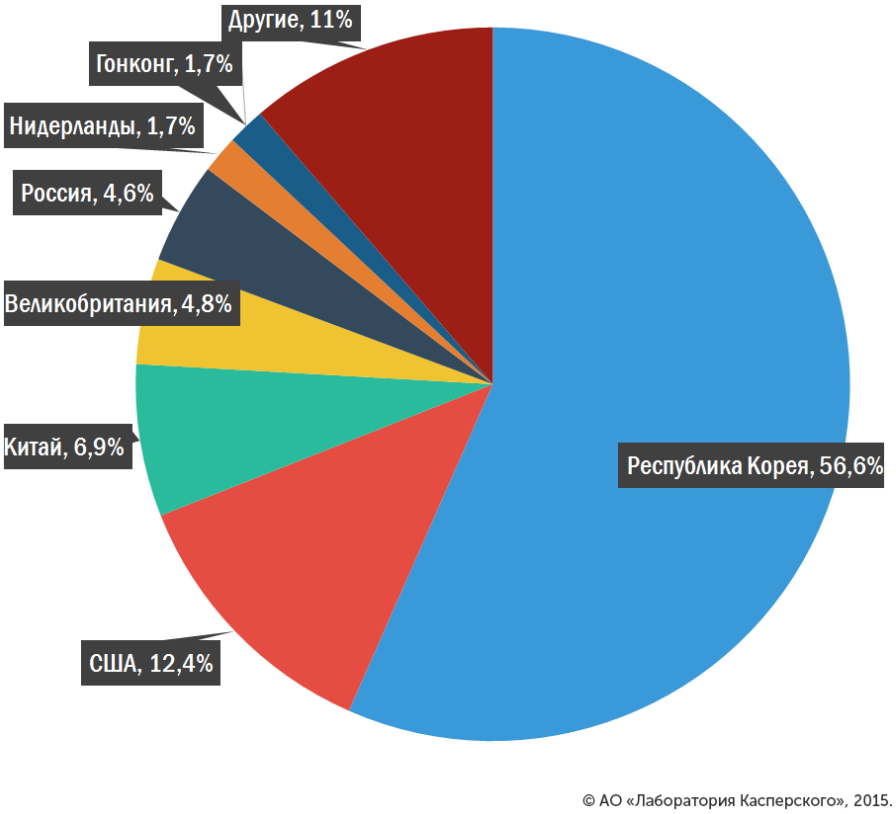
Распределение DDoS-атак по длительности, часы

Рекорд прошлого квартала по продолжительности атаки в 205 часов (8,5 дней) в этом квартале был решительно побит атакой, длившейся 320 часов (13,3 дня).

Командные серверы и типы ботнетов

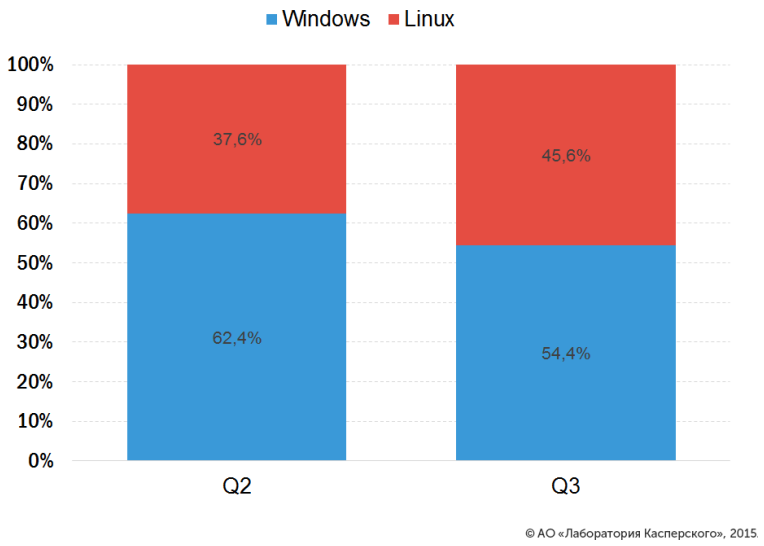
Во третьем квартале 2015 года Республика Корея безоговорочно лидирует по числу расположенных на ее территории командных серверов ботнетов, ее доля выросла с 34 до 56,6%. Отметим, что в этом квартале в Корее значительно увеличилось число командных серверов, управляющих ботами Nitol. Он стал активнее применять сервисы Dynamic DNS, в частности, no-ip.org и codns.com. Как уже было сказано выше, в то же время увеличился процент DDoS-атак, нацеленных на расположенные в Корее ресурсы.

Доля командных серверов на территориях США и Китая заметно снизилась — с 21 до 12,4% и с 14 до 6,9% соответственно.



Распределение командных серверов ботнетов по странам, Q3 2015

В третьем квартале 2015 года продолжились колебания в соотношении активности ботов, разработанных под операционные системы семейств Windows и Linux. После снижения доли во втором квартале, ботнеты на основе ОС Linux несколько отыграли свои позиции — доля атак с таких ботнетов выросла с 37,6 до 45,6%.



Соотношение атак с Windows- и Linux-ботнетов

В повышении активности Linux-ботнетов свою роль, по всей вероятности, сыграла недостаточная защищенность типичной Linux-машины, и, что важно, более высокая скорость интернет-канала, к которому она подключена. Это делает Linux более привлекательным для злоумышленников, несмотря на относительную сложность в разработке, приобретении и эксплуатации Linux-ботов.

Атаки на банки

Третий квартал ознаменовался возвращением на киберкриминальную сцену DDoS-вымогателей. Ряд крупных банковских организаций в различных странах становились целями DDoS-атак, а затем получали письма с требованием заплатить крупную сумму в криптовалюте (BTC) за прекращение атаки. Именно эта особенность позволяет предположить, что за атаками стоит группировка DD4BC, которая при проведении атак требует выкуп в биткойнах.

Предположительно, эта же группировка добралась и до России, где были атакованы некоторые российские финансовые организации. Часть атакованных российских банков находилась под защитой сервиса Kaspersky DDoS Prevention либо оперативно подключилась к сервису в самом начале DDoS-атак. Это позволило им избежать ущерба, веб-сайты банков и системы онлайн-банкинга продолжали нормально функционировать.

«Лаборатория Касперского» зафиксировала волну продолжительных DDoS-атак на системы онлайн-банкинга восьми известных финансовых организаций, некоторые банки подвергались DDoS-атакам неоднократно в течении квартала.

Во всех атаках злоумышленники использовали довольно сложную комбинацию атак типа Amplification – атак с коэффициентом усиления, которые позволяют вывести интернет-ресурс из строя при минимальных усилиях со стороны атакующих.

Использовались три вида атак на переполнение канала: NTP amplification, SSDP amplification и RIPv1 amplification мощностью до 40 Гбит/сек. В ряде случаев атаки дополнялись атакой по HTTPS мощностью до 150 мбит/сек с ботнета размером около 2000 атакующих хостов.

Длительность атак составила от 1 до 4 часов.

Злоумышленники не только требовали выкуп в биткойнах, но и угрожали банкам атаками беспрецедентной мощности в терабит. Однако на практике эти угрозы так и не были реализованы.

Можно предположить, что на конец сентября пиковые параметры зарегистрированных атак были максимумом возможностей атакующих, поскольку в случае одновременного проведения атак на несколько банков эксперты «Лаборатории Касперского» фиксировали именно эту совокупную мощность.

К сожалению, это не исключает возможности наращивания мощности атак в будущем.

Заключение

Соотношение атак с Windows- и Linux-ботнетов говорит об интересном тренде: злоумышленники стали активно использовать ботнеты, состоящие из зараженных серверов. Обусловлено это несколькими причинами:

- Во-первых, серверы имеют значительно больший интернет-канал, нежели домашние машины, что позволяет организовывать мощные атаки, имея под контролем всего несколько серверов.
- Во-вторых, уровень защищенности серверов не всегда высок, что и делает возможным их взлом. Если на сервере регулярно не устанавливаются security-патчи, то он очень быстро становится легкой добычей злоумышленников. Узнать о его существовании не составляет особого труда, как и проэксплуатировать известную уязвимость. Также не стоит забывать о возросшем арсенале доступных эксплойтов, которые появились вследствие обнаружения ряда уязвимостей в open-source продуктах, например, эксплойты к уязвимости ghost, которая до сих пор является актуальной.
- В-третьих, мощности серверного ботнета могут быть увеличены за счет взятия в аренду дополнительных серверов.

В такой ситуации становится критичной своевременная установка патчей на серверы, а для владельцев веб-ресурсов — действенная защита от DDoS-атак с серверных-ботнетов, от которых уже страдают различные компании.

О «Лаборатории Касперского»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

Securelist, ресурс экспертов «Лаборатории Касперского» с актуальной информацией о киберугрозах

Сайт «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy

Москва, 125212
Ленинградское шоссе, д.39А, стр.3
БЦ «Олимпия Парк»

Телефон: +7-495-797-8700
+7-495-737-3412
Факс: +7-495-797-8709