KASPERSKY lab

Kaspersky Security Bulletin 2015

ЭВОЛЮЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БИЗНЕС-СРЕДЕ

GREAT

#KLReport

ОГЛАВЛЕНИЕ

В конце 2014 года мы опубликовали наше видение того, как будут развиваться события в мире кибер(без)опасности в 2015 году. Четыре из девяти наших прогнозов напрямую были связаны с угрозами для бизнеса, и три пункта из четырех уже сбылись:

- Киберпреступники осваивают целевые атаки APT-класса – да.
- Фрагментация и диверсификация атак APT-групп – да.
- Эскалация атак на банкоматы и PoS-терминалы – да.
- Атаки на виртуальные платежные системы – нет.

Давайте посмотрим, какими в 2015 году были наиболее значительные инциденты и какие новые тренды, связанные с информационной безопасностью в бизнес-среде, мы увидели.

ЦИФРЫ ГОДА

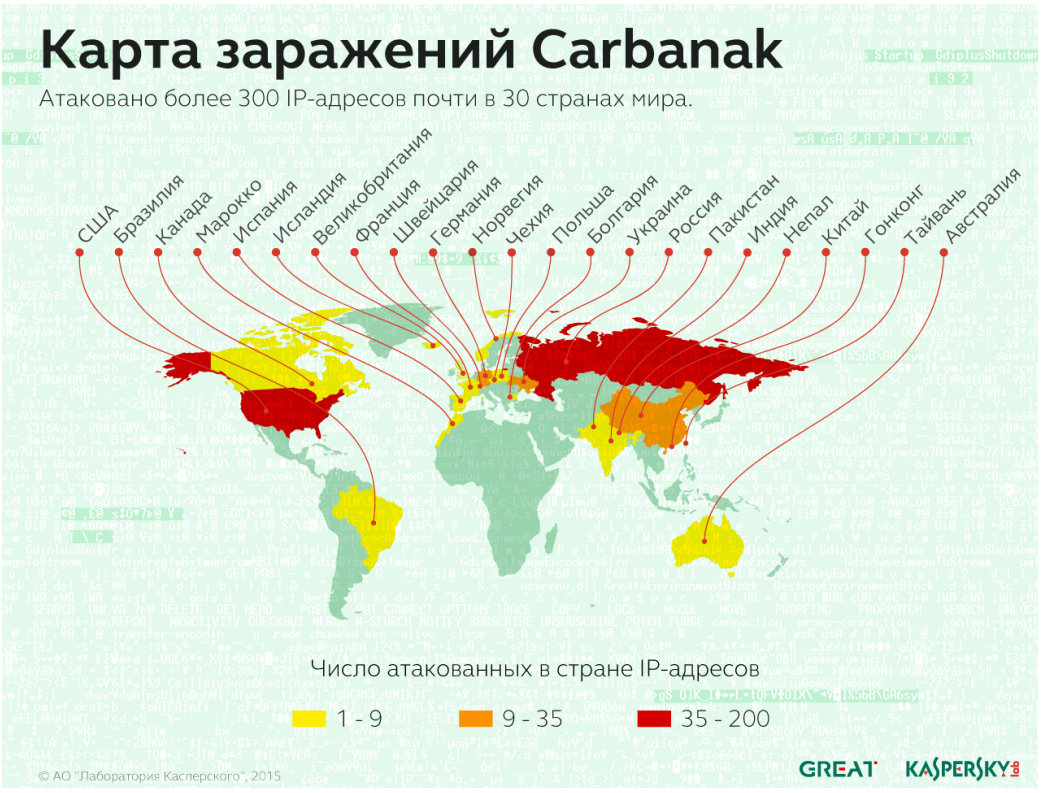
- В 2015 году на 58% корпоративных компьютеров была отражена хотя бы одна атака вредоносного ПО, что на 3 п.п. больше, чем в прошлом году.
- 29% компьютеров, т.е. почти каждый третий компьютер в бизнес-среде, подверглись хотя бы одной атаке через интернет.
- При атаках на бизнес эксплойты к офисным приложениям используются в три раза чаще, чем в атаках на домашних пользователей.
- Файловый антивирус сработал на 41% компьютеров корпоративных пользователей (детектировались объекты, обнаруженные на компьютерах или на съемных носителях, подключенных к компьютерам, — флешках, картах памяти, телефонах, внешних жестких дисках, сетевых дисках).

ЦЕЛЕВЫЕ АТАКИ НА БИЗНЕС: APT И ПРЕСТУПНИКИ

2015 год запомнится рядом атак APT-класса на бизнес. Арсенал и методы, использованные злоумышленниками, были очень похожи на то, с чем мы встречались при разборе APT-атак, но за атаками стояли не государственный структуры, а киберкриминал. Хотя киберпреступники и использовали не характерные для них методы, основная цель атак осталась неизменной — получение финансовой выгоды.

Ярким примером смещения фокуса целевых атак APT-класса на финансовые организации стала операция Carbanak. Это было настоящее ограбление банка в цифровую эру: злоумышленники проникали в сеть банка-жертвы и искали критически важную систему, с помощью которой из атакованной финансовой организации выводили денежные средства. Украв у банка значительную сумму (от 2,5 до 10 млн долларов), преступники искали следующую жертву.

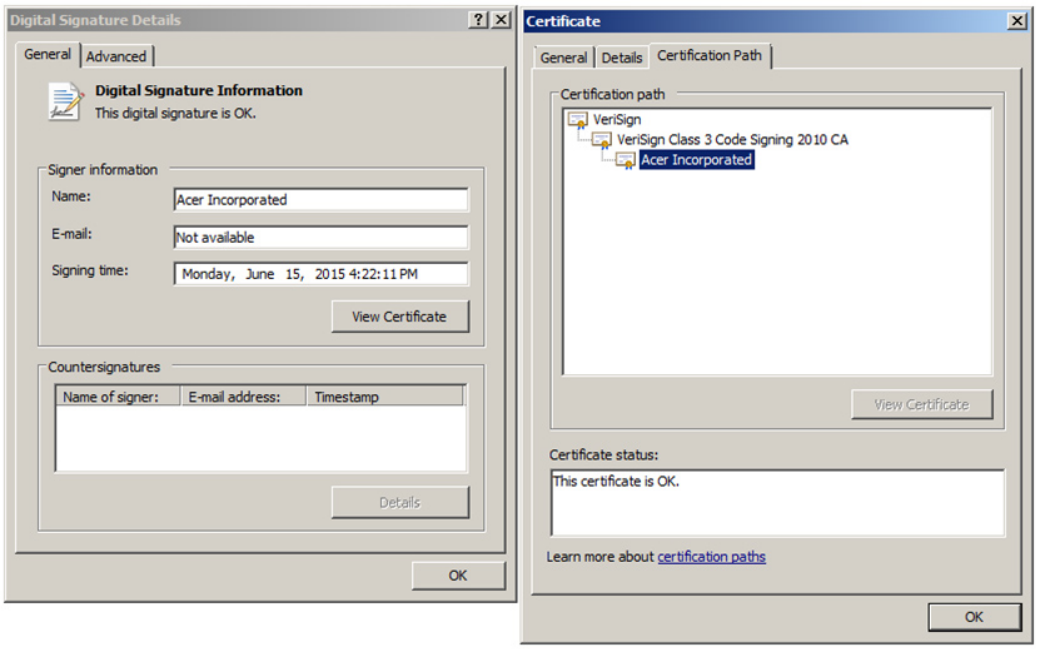
Большинство жертв вредоносной кампании располагалось в Восточной Европе. При этом кампания Carbanak нацелена также и на организации в США, Германии и Китае. Всего же по миру насчитывается более 100 жертв этой атаки, а суммарные убытки пострадавших организаций (в основном это были банки) могут достигать миллиарда долларов.



Не стоит забывать, что информация также может представлять большую ценность, особенно если ее можно использовать при заключении сделок или для игры на различных биржах товаров, ценных бумаг или валют, в том числе криптовалют. Примером целевой атаки, которая могла быть нацелена на получение подобной информации, является Wild Neutron (известна также как Jripbot и Morpho). Впервые эта кампания кибершпионажа получила широкую огласку в 2013 году — тогда от нее пострадало несколько известных компаний, включая Apple, Facebook, Twitter и Microsoft. После того, как эти инциденты получили огласку, организаторы кибершпионской операции свернули свою деятельность. Однако примерно через год «Лаборатория Касперского» зафиксировала возобновление активности Wild Neutron.

Наши исследования показали, что в ходе кампании кибершпионажа были заражены компьютеры пользователей в 11 странах и территориях, а именно в России, Франции, Швейцарии, Германии, Австрии, Словении, Палестине, ОАЭ, Казахстане, Алжире и США. Среди пострадавших — юридические фирмы, инвестиционные компании, организации, работающие с криптовалютой Bitcoin, группы компаний и предприятия, вовлеченные в сделки слияния и поглощения, IT-компании, учреждения здравоохранения, риэлтерские компании, а также индивидуальные пользователи.

Отметим, что в ходе кампании Wild Neutron использовался сертификат подписи кода, украденный у компании Acer.



Подпись компании Acer в установщике Wild Neutron

Тренд на диверсификацию APT-атак хорошо иллюстрирует изменение мишеней атак группировки Winnti. Долгое время считалось, что китайская киберпреступная группировка Winnti атакует только

компании, занимающиеся компьютерными играми. Однако начиная с весны 2015 года стала поступать информация, свидетельствующая о том, что злоумышленники, обкатавшие свои инструменты и методы, стараются получить выгоду от атак на новые мишени. Их интересы больше не ограничивается индустрией развлечений: группировка нацелилась на фармацевтические и телекоммуникационные компании. При анализе новой волны атак Winnti, как и в случае с Wild Neutron, было выявлено, что руткит Winnti подписан украденным сертификатом, принадлежащим одному из подразделений огромного японского конгломерата.

2015 год также отметился расширением географии – как атак, так и атакующих. Например, во время проведения расследования инцидента на Ближнем Востоке экспертами «Лаборатории Касперского» была обнаружена активность неизвестной ранее группировки, проводящей таргетированные атаки. Группа была названа «Соколы Пустыни» (Desert Falcons), она является первой арабской группировкой, проводящей полноценные операции по кибершпионажу. К моменту обнаружения насчитывалось около 300 жертв, среди которых были и финансовые организации.

А группировка Blue Termite атаковала организации и компании в Японии:

Информацию о целевых атаках на бизнес можно узнать в опубликованных «Лабораторией Касперского» отчетах: Carbanak, Wild Neutron, Winnti, DarkHotel 2015, Desert Falcons, Blue Termit, Grabit, более подробные результаты исследования предоставляется подписчикам Kaspersky Intelligence Service.

Анализ данных атак позволяет выделить несколько тенденций развития целевых атак на бизнес:

- Под прицел злоумышленников попали организации, выполняющие различные операции с деньгами: банки, фонды и компании, связанные с биржами, в том числе с биржами криптовалют.
- Атаки тщательно готовятся, злоумышленники исследуют интересы потенциальных жертв (сотрудников атакуемой компании) и выявляют сайты, которые они часто посещают, исследуют контакты жертвы, собирают информацию о поставщиках оборудования и услуг.
- Собранные при подготовке атаки данные активно используются. Атакующие взламывают выявленные легитимные сайты, аккаунты пользователей из бизнес-контактов сотрудников атакуемой компании. Такие сайты/аккаунты используются в течение нескольких часов — с них распространяется вредоносный код, после чего заражение прекращается. Такая схема дает злоумышленникам возможность повторно использовать взломанный ресурс через несколько месяцев.
- Активное использование подписанных файлов и легального ПО для сбора информации из атакованной сети.
- Диверсификация атак, атаки на малый и средний бизнес.
- Расширение географии атак, нацеленных на бизнес: крупная атака в Японии, APT группы из арабского мира.

Хотя атак класса APT, за которыми стоит киберкриминал, относительно немного, тенденции их развития несомненно влияют на подходы и методы, используемые в атаках на бизнес «рядовыми» киберпреступниками.

СТАТИСТИКА

Отметим, что общая статистика по корпоративным пользователям (география атак, рейтинг детектируемых объектов) в принципе совпадает со статистикой по домашним пользователям. Это неудивительно – бизнес-пользователи не существуют в изолированной среде, их компьютеры становятся объектами атак злоумышленников, которые распространяют вредоносные программы без учета специфики атакуемого. Таких атак/зловредов большинство, и данные по атакам, нацеленным именно на бизнес-пользователей, мало влияют на общую статистику.

В 2015 году хотя бы одна атака вредоносного ПО была отражена на 58% корпоративных компьютеров, что на 3 п.п. больше, чем в прошлом году.

Веб-угрозы (атаки через интернет)

В 2015 году 29%, т.е. практически каждый третий компьютер в бизнес-среде, подвергся хотя бы одной атаке через интернет.

TOP 10 вредоносных программ, атаки через интернет

Отметим, что в данном рейтинге представлены только вредоносные программы, мы исключили из него рекламные программы, которые действуют весьма назойливо и доставляют неприятности пользователю, но не наносят вреда компьютеру.

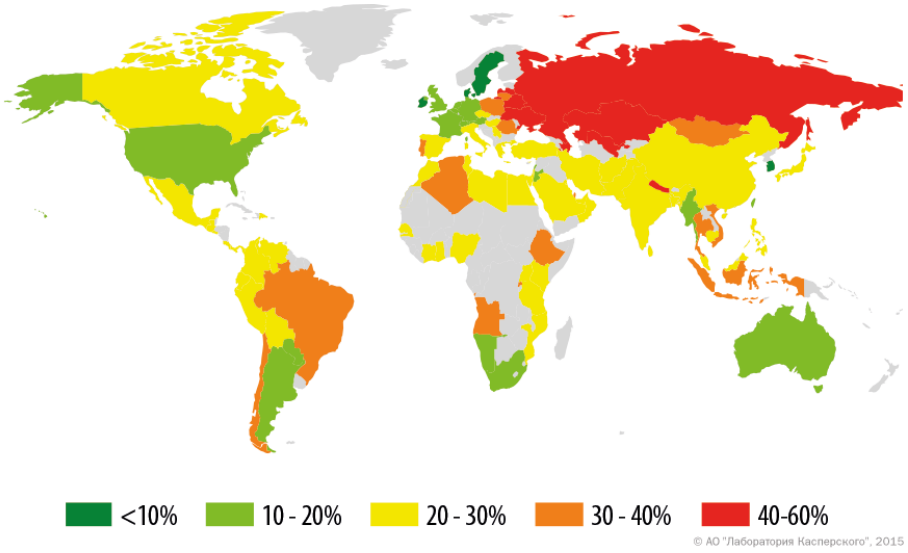
	Название*	% атакованных пользователей**
1	Malicious URL	57,0
2	Trojan.Script.Generic	24,7
3	Trojan.Script.Iframer	16,0
4	Exploit.Script.Blocker	4,1
5	Trojan-Downloader.Win32.Generic	2,5
6	Trojan.Win32.Generic	2,3
7	Trojan-Downloader.JS.Iframe.diq	2,0
8	Exploit.Script.Generic	1,2
9	Packed.Multi.MultiPacked.gen	1,0
10	Trojan-Downloader.Script.Generic	0,9

** Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных*

*** Процент пользователей, атакованных данным зловредом, от всех атакованных пользователей.*

Практически весь TOP 10 состоит из вердиктов, которые присваиваются объектам, использующимся в drive-by атаках, – это различные троянцы-загрузчики и эксплойты.

География веб-атак



География атак через веб-ресурсы, 2015 год
(процент атакованных корпоративных пользователей в стране)

Локальные угрозы

Файловый антивирус сработал на 41% компьютеров корпоративных пользователей (детектировались объекты, обнаруженные на компьютерах или на съемных носителях, подключенных к компьютерам, — флешках, картах памяти, телефонах, внешних жестких дисках, сетевых дисках).

TOP 10 вредоносных программ, локальные угрозы

Отметим, что в данном рейтинге представлены только вредоносные программы, мы исключили из него рекламные программы, которые действуют весьма назойливо и доставляют неприятности пользователю, но не наносят вреда компьютеру.

	Название*	% атакованных пользователей**
1	DangerousObject.Multi.Generic	23.1%
2	Trojan.Win32.Generic	18.8%
3	Trojan.WinLNK.StartPage.gena	7.2%
4	Trojan.Win32.AutoRun.gen	4.8%
5	Worm.VBS.Dinihou.r	4.6%
6	Net-Worm.Win32.Kido.ih	4.0%
7	Virus.Win32.Sality.gen	4.0%
8	Trojan.Script.Generic	2.9%
9	DangerousPattern.Multi.Generic	2.7%
10	Worm.Win32.Debris.a	2.6%

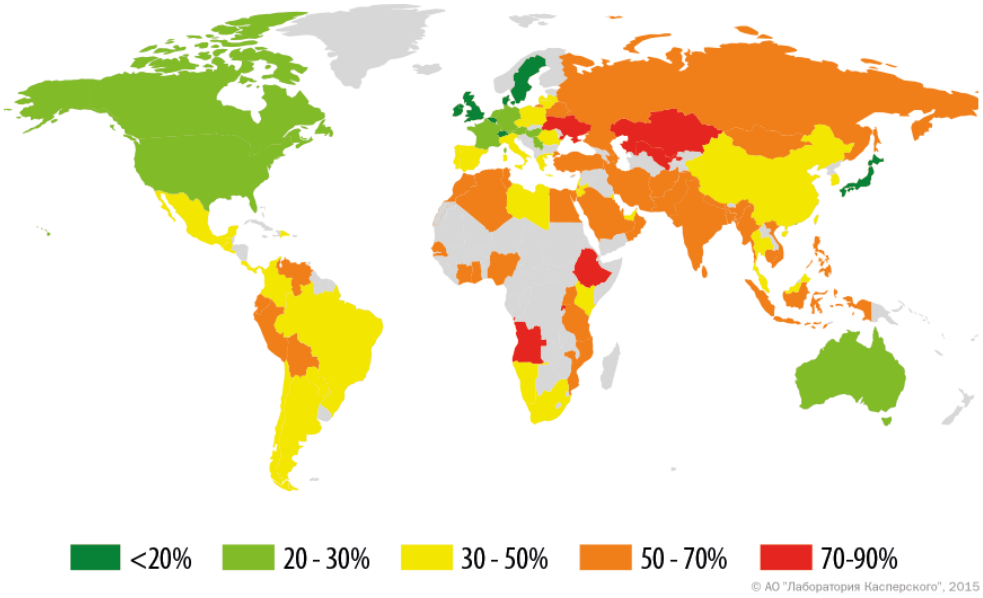
** Детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.*

*** Процент пользователей, атакованных данным зловредом, от всех атакованных пользователей.*

На первом месте различные вредоносные программы, обнаруженные с помощью облачных технологий и детектируемые как DangerousObject.Multi.Generic. Облачные технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, зато у антивирусной компании «в облаке» уже есть информация об объекте. В случае компаний, не желающих отсылать какую-либо статистику в облако, вместо отключения облачных технологий используют Kaspersky Private Security Network, таким образом компьютеры в сети получают защиту из облака.

Остальные представители рейтинга – это, в основном, самораспространяющиеся программы и их компоненты.

География локальных угроз



География обнаружения локальных угроз, 2015 год
(процент атакованных корпоративных пользователей в стране)

ОСОБЕННОСТИ АТАК НА БИЗНЕС

Общая статистика по корпоративным пользователям не отражает специфики атак на бизнес, на нее больше влияет вероятность заражения компьютера в стране или популярность того или иного зловреда у злоумышленников.

Однако более детальный анализ выявляет особенности атак на корпоративных пользователей:

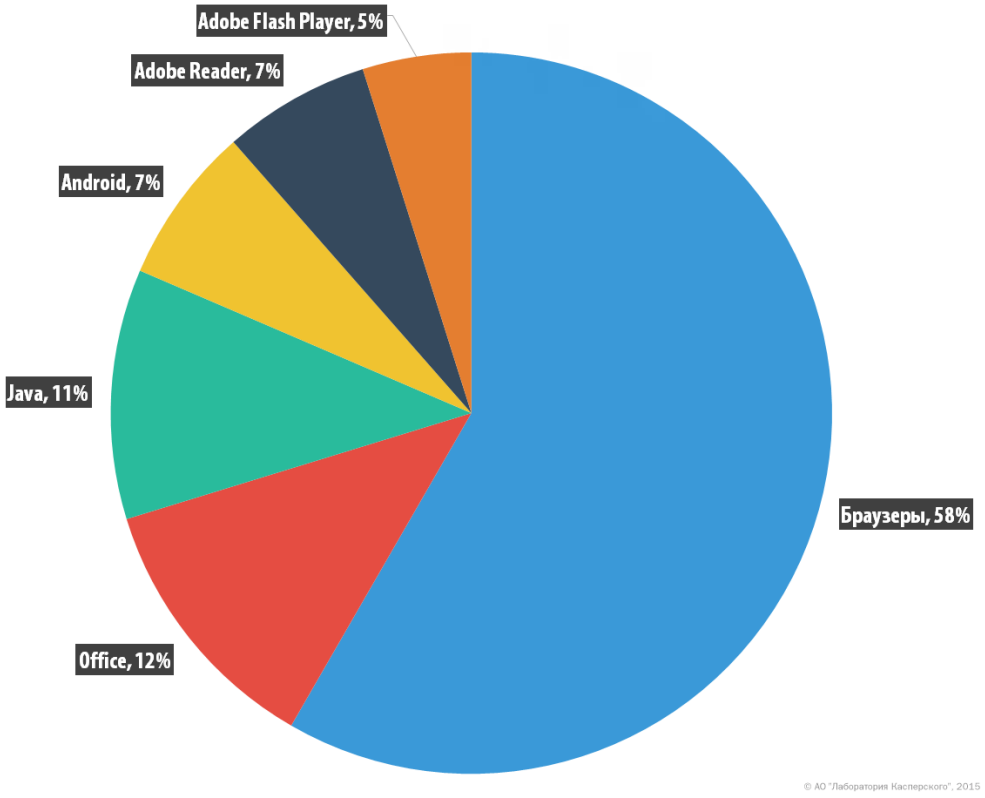
- в 3 раза чаще, чем в атаках на домашних пользователей, используются эксплойты к офисным приложениям,
- используются вредоносные файлы, подписанные валидными цифровыми сертификатами,
- в ходе атак используются доступные легальные программы, что позволяет атакующим дольше оставаться незамеченными.

Кроме того, мы отметили активный рост числа компьютеров корпоративных пользователей, атакованных программами-шифровальщиками.

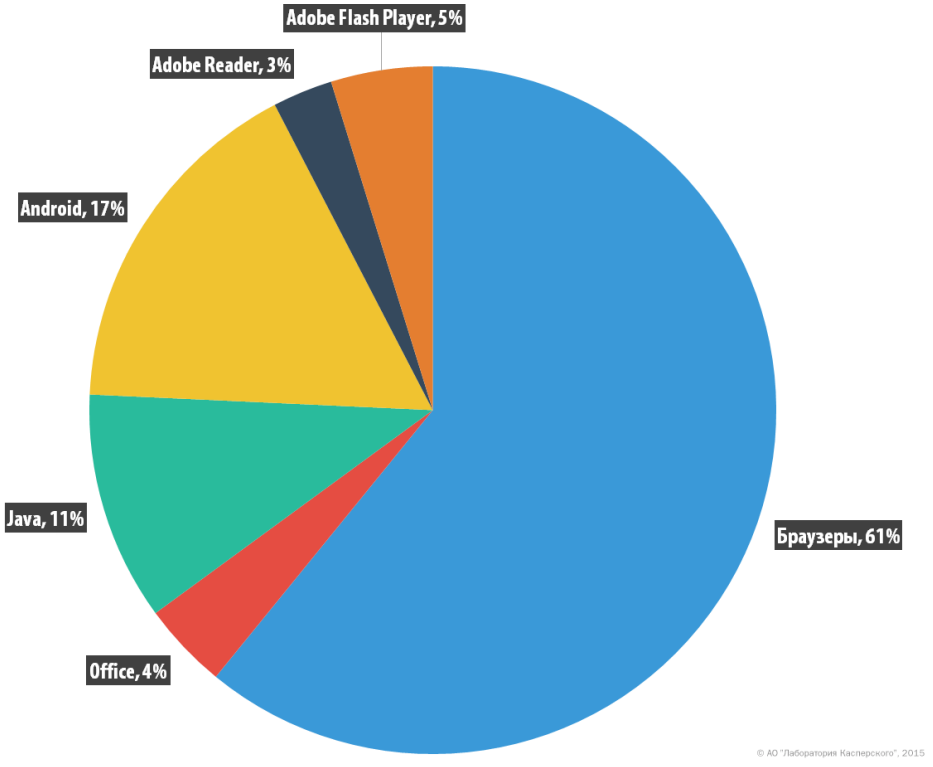
Речь в данном случае далеко не всегда идет об атаках класса APT: «рядовые» злоумышленники фокусируются на корпоративных пользователях — а иногда и на отдельно взятой компании.

Эксплойты в атаках на бизнес

Рейтинг уязвимых приложений построен на основе данных о заблокированных нашими продуктами эксплойтах, используемых злоумышленниками как в атаках через интернет и почту, так и при компрометации локальных приложений, в том числе на мобильных устройствах пользователей.



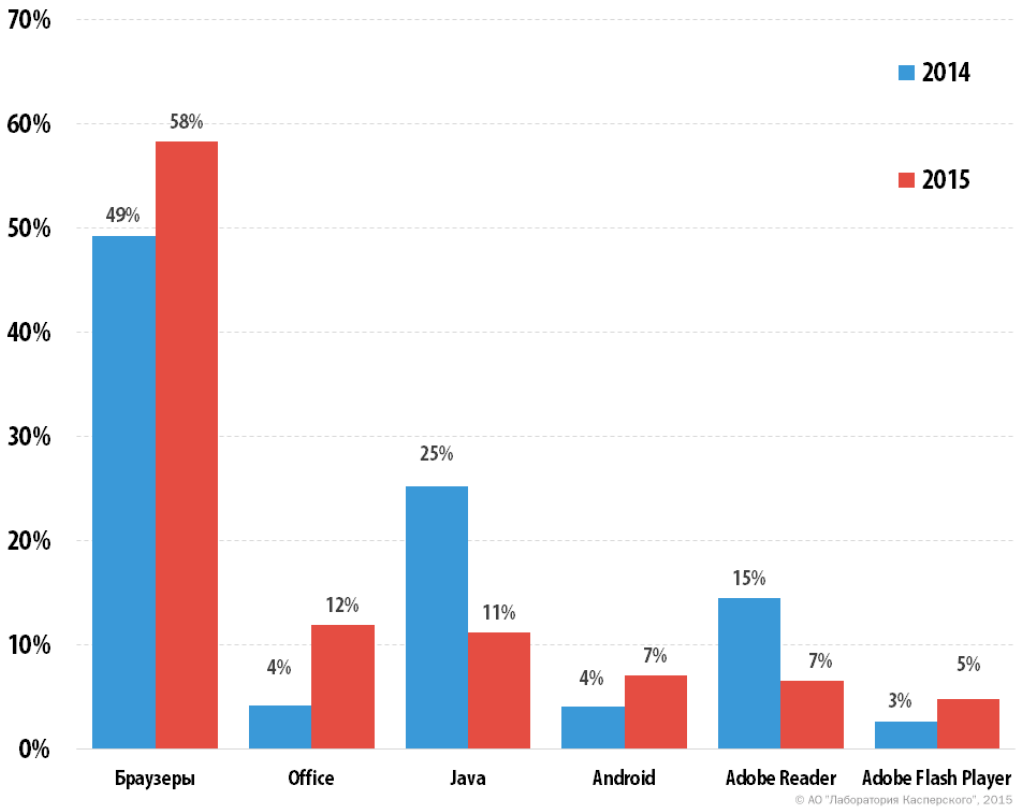
Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений (корпоративные пользователи, 2015 год)



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений (домашние пользователи, 2015 год)

При сравнении эксплойтов, использованных злоумышленниками для атак на домашних и корпоративных пользователей, в первую очередь бросается в глаза значительно более активное использование эксплойтов к офисным программам в атаках на бизнес. Если в атаках на домашних пользователей мы встречали их лишь в 4% случаев, то в атаках на корпоративных пользователей эксплойты для уязвимостей в офисных приложениях составляют 12% от всех обнаруженных за год эксплойтов.

Как и в атаках на домашних пользователей, в атаках на корпоративных пользователей среди атакуемых эксплойтами приложений на первом месте остается категория браузеры. При рассмотрении данной статистики необходимо учитывать, что технологии «Лаборатории Касперского» детектируют эксплойты на различных этапах. В категорию «браузеры» попадают также детектирования лэндинг-страниц, которые «раздают» эксплойты. По нашим наблюдениям, чаще всего это эксплойты к Adobe Flash Player.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, в 2014 и в 2015 году

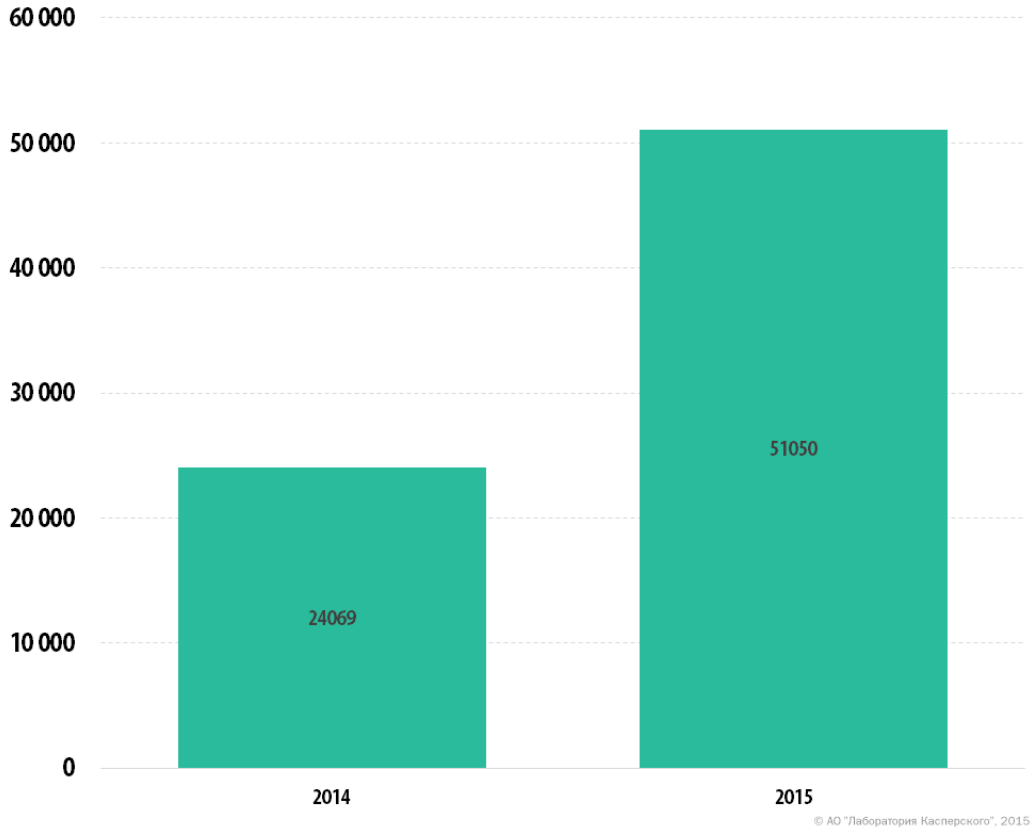
По сравнению с 2014 годом значительно снизилась доля Java- и PDF-эксплойтов — на 14 п.п. и 8 п.п. соответственно. Java-эксплойты стали пользоваться меньшей популярностью, несмотря на то, что в течение года было найдено несколько zero-day уязвимостей. При этом выросла доля атак с использованием уязвимостей в офисных программах (+8 п.п.), браузеров (+9 п.п.), Adobe Flash Player (+9 п.п.), а также Android (+3 п.п.).

Как показывает практика разбора инцидентов безопасности, даже в целевых атаках на корпорации злоумышленники чаще используют эксплойты к уже известным уязвимостям, что обусловлено медленной установкой патчей в корпоративной среде. Рост доли эксплойтов, нацеленных на уязвимые Android-приложения до 7% говорит об увеличивающемся интересе злоумышленников к корпоративным данным на мобильных устройствах сотрудников.

Шифровальщики

Троянцы-шифровальщики долгое время считались угрозой только для домашних пользователей. Теперь же, по нашим данным, злоумышленники, наживающиеся на шифровальщиках, все чаще стали обращать свое внимание на организации.

В 2015 году нашими решениями были обнаружены шифровальщики на более чем **50 тысячах машин** в корпоративных сетях, **что в 2 раза больше, чем годом ранее**. Важно также учитывать, что реальное количество инцидентов в разы больше: данная статистика учитывает только результаты сигнатурного и эвристического детектирования, а продукты «Лаборатории Касперского» в большинстве случаев детектируют троянцы-шифровальщики с помощью поведенческих методов.



Количество уникальных корпоративных пользователей, атакованных троянцами-шифровальщиками в 2014 и 2015 годах

Столь быстро растущий интерес злоумышленников к атакам на бизнес объясняется двумя причинами. Во-первых, сумма, полученная в качестве выкупа от организаций, может быть куда более значительной, чем от пользователей. А во-вторых, шанс, что выкуп будет заплачен, в случае пострадавшей организации выше – компании подчас просто не могут функционировать, если информация на нескольких критичных компьютерах или серверах зашифрована и недоступна.

Одним из самых интересных случаев на этом фронте в 2015 году стало появление первого Linux-шифровальщика (продукты «Лаборатории Касперского» детектируют его как «Trojan-Ransom.Linux.Cryptor»), нацеленного на веб-сайты, в том числе сайты интернет магазинов. Используя уязвимости в веб-приложениях, злоумышленники получали доступ к веб-сайтам и загружали на них вредоносную программу, зашифровывающую данные сервера. В большинстве случаев это приводило к выведению сайта из строя. За расшифровку преступники требовали выкуп в 1 биткойн. Количество зараженных веб-сайтов оценивается в 2 тысячи. Учитывая распространённость *nix-серверов в бизнес-среде, логично предположить, что атаки шифровальщиков, нацеленных на не-Windows платформы, могут получить продолжение в следующем году.

TOP 10 семейств троянцев-шифровальщиков

	Семейство	% атакованных пользователей*
1	Scatter	21
2	Onion	16
3	Cryakl	15
4	Snocry	11
5	Cryptodef	8
6	Rakhni	7
7	Crypmod	6
8	Shade	5
9	Mor	3
10	Crypren	2

** Процент пользователей, атакованных зловредами данного семейства, от всех атакованных пользователей.*

Практически все семейства криптолокеров, вошедшие в TOP 10, требуют в качестве выкупа биткойны.

На первом месте расположились троянцы семейства Scatter, шифрующие файлы на диске и оставляющие зашифрованные файлы с расширением .vault. Семейство Scatter – это многомодульные скриптовые многофункциональные зловреды. За короткое время оно успело значительно эволюционировать, обзаведясь помимо возможности шифрования файлов функциональностью Email-Worm и Trojan-PSW. На втором месте по распространенности

шифровальщики семейства Onion, известные тем, что их командные серверы находятся в сети Tor. На третьем месте – появившиеся еще в апреле 2014 года и написанные на Delphi шифровальщики семейства Cryakl.

В некоторых случаях есть возможность расшифровать данные, зашифрованные этими зловредами – в основном, когда в алгоритме есть какие-либо ошибки. Однако расшифровать данные, которые были зашифрованы последними версиями вредоносных программ, представленных в топе, на сегодняшний день невозможно.

Важно понимать, что для компании заражение подобной программой может обернуться остановкой бизнеса, в случае если будут зашифрованы критически важные данные или в результате шифрования данных будет заблокирована работа критически важного сервера. Следствием подобных атак могут стать огромные убытки, сравнимые с атаками вредоносных программ Wiper, нацеленных на уничтожение данных в компьютерных сетях компаний.

Для борьбы с этой угрозой необходимо применять ряд мер:

- использовать защиту от эксплойтов;
- обязательно включить поведенческие методы детектирования в защитном продукте (в продуктах «Лаборатории Касперского» за это отвечает компонент System watcher);
- настроить процесс резервного копирования данных.

АТАКИ НА POS-ТЕРМИНАЛЫ

Отдельной темой для бизнеса, особенно ведущего торговую деятельность, в 2015 году оказалась безопасность PoS-терминалов (Point Of Sale — точка продажи). По сути сейчас в качестве PoS-терминала может быть использован любой компьютер с подключенным специальным устройством для считывания карт и установленным специальным ПО. Злоумышленники ищут подобные компьютеры и заражают их зловредами, которые позволяют похищать данные карт, проведенных через терминал оплаты.

По всему миру продукты «Лаборатории Касперского» отразили более 11,5 тысяч попыток подобных атак. Сейчас в нашей коллекции 10 семейств программ, нацеленных на кражу данных с PoS-терминалов. 7 из них появились в этом году. Несмотря на небольшое количество попыток атак, не стоит недооценивать опасность, ведь одна успешная атака может скомпрометировать данные десятков тысяч кредитных карт. Столь большое число возможных жертв обусловлено тем, что PoS-терминалы не воспринимаются владельцами и администраторами как объекты, нуждающиеся в защите, поэтому зараженным терминал может оставаться очень долго, и все это время вредоносная программа будет отсылать злоумышленникам считанные терминалом данные кредитных карт.

Эта проблема особенно актуальна в странах, где не используются карты с EMV-чипом. Переход на карты с EMV-чипом должен значительно усложнить задачу получения данных для клонирования карт, но это вопрос достаточно длительного времени. Поэтому требуется принимать хотя бы минимальные меры по защите POS-устройств, благо для них достаточно легко реализуется политика безопасности «запрет запуска неизвестных программ по умолчанию».

Мы ожидаем, что в будущем киберпреступники начнут атаковать мобильные PoS-устройства под управлением Android.

ЗАКЛЮЧЕНИЕ

Наши данные показывают, что инструментарий атак на бизнес отличается от того, что применяют в атаках на домашних пользователей. В атаках на корпоративных пользователей значительно чаще используются эксплойты к офисным приложениям, вредоносные файлы часто оказываются подписанными валидными цифровыми сертификатами, плюс к этому злоумышленники стараются использовать в своих целях доступные легальные программы, чтобы дольше оставаться незамеченными. Кроме того, мы отметили активный рост числа компьютеров корпоративных пользователей, атакованных программами-шифровальщиками. Это касается не только атак класса APT: «рядовые» злоумышленники целенаправленно атакуют корпоративных пользователей, а иногда – сотрудников конкретных компаний.

Использование киберкриминальными группировками, атакующими бизнес, методов и программ из мира APT переводит эти атаки на другой уровень и делает их значительно более опасными. В первую очередь киберпреступники стали применять эти методы для проведения атак на банки с целью вывода крупных сумм денег. Этими же методами они могут выводить со счетов в банках и деньги компаний, получив доступ к сети организации.

В своих атаках криминал полагается на использование уже известных уязвимостей, что связанно с медленной установкой обновлений для ПО в организациях. Кроме того, злоумышленники активно используют подписанные вредоносные файлы и легальные инструменты для создания канала вывода информации: в ход идут известные программы для удаленного администрирования, SSH-клиенты, программы для восстановления паролей и т.д.

Все чаще объектами атак злоумышленников становятся серверы организаций. Помимо кражи данных, известны случаи, когда атакованные серверы использовались в качестве инструмента DDoS атак, или данные просто шифровались, и злоумышленники требовали выкуп. Последние события показали, что это утверждение справедливо как для Windows-, так и для Linux-серверов.

Многие организации, которые стали жертвами атак, столкнулись с требованиями злоумышленников заплатить выкуп за остановку DDoS-атаки, расшифровку данных или за неразглашение украденной информации. Когда организация сталкивается с этим, в первую очередь нужно обращаться в правоохранительные органы и к специалистам по компьютерной безопасности. Потому что, получив выкуп, преступники могут не сдержать слово, как в случае с DDoS-атакой на компанию ProtonMail, которая не остановилась после получения денег.

ПРОГНОЗЫ

Увеличение количества атак на финансовые организации, совершение финансовых махинаций на биржах

В будущем году мы ожидаем как увеличения количества атак на финансовые организации, так и изменения качества таких атак. Помимо перевода денег на свои счета с последующим обналичиванием, злоумышленники могут применять новые техники, в том числе связанные с манипуляцией данными на торговых площадках, где работают как с традиционными, так и с новыми финансовыми инструментами, такими как криптовалюты.

Атаки на инфраструктуру

Практически все ценные данные организаций подчас расположены не в самой организации, а на серверах в датацентрах. Получение доступа к этим элементам инфраструктуры и будет одним из важных векторов атак на компании в 2016 году.

Использование уязвимостей в IoT для проникновения в сети организаций

Практически во всех современных корпоративных сетях сегодня есть IoT устройства. Исследования, проведенные в 2015 году, показали, что существует ряд проблем с безопасностью этих устройств, чем очевидно попробуют воспользоваться злоумышленники, используя их в качестве первой ступени проникновения в сеть организации.

Более жесткие стандарты безопасности, кооперация с правоохранительными органами

Ответом регуляторов на увеличивающееся количество компьютерных инцидентов в бизнес-среде и в целом на изменение ландшафта киберугроз будет разработка новых и обновление уже принятых стандартов безопасности. Организации, заинтересованные в сохранности своих цифровых ценностей, будут активнее сотрудничать с правоохранительными органами, либо упомянутые выше стандарты их к этому обяжут. Это может привести к более эффективной работе по поимке киберпреступников, и в 2016 году мы узнаем о новых арестах.

ЧТО ДЕЛАТЬ?

2015 год показал, что киберпреступники активно стали использовать методы APT-атак для проникновения в сети компаний. Здесь мы говорим и о предварительной разведке с целью выявления слабых звеньев в инфраструктуре и получении информации о сотрудниках, и об использовании spearphishing и waterhole-атак, активном использовании эксплойтов для выполнения кода и получения прав администратора, а также об использовании в атаках помимо троянских программ легального ПО для удаленного администрирования, изучения сети и «восстановления» паролей. Все это требует развития методов и технологий защиты сетей предприятий.

Переходя к конкретным рекомендациям, первым делом, стоит обратить внимание на ТОР 35 стратегий по нейтрализации атак на предприятия, составленный управлением радиотехнической обороны Австралии. Проведя всесторонний детальный анализ локальных атак и угроз, ASD пришло к выводу, что не менее 85% целевых кибервторжений можно нейтрализовать применением четырех базовых стратегий. Три из этих стратегий связаны с использованием специализированных защитных решений (в состав продуктов «Лаборатории Касперского» входят технологические решения, охватывающие эти три важнейшие стратегии).

Четыре основные стратегии, снижающие вероятность успешной целевой атаки:

- Применение белых списков приложений позволяет заблокировать выполнение вредоносного ПО и неутвержденных программ.
- Установка исправлений для Java, Flash, программ просмотра PDF-файлов, веб-браузеров и пакета Microsoft Office.
- Исправление уязвимостей в операционной системе при помощи патчей.
- Ограничение прав административного доступа к операционной системе и приложениям, исходя из служебных обязанностей каждого пользователя.

Более подробную информацию о стратегиях ASD можно найти в документе о стратегиях нейтрализации угроз в энциклопедии Securelist.

Вторым важным фактором является использование данных об актуальных угрозах, т.е. сервисов Threat Intelligence (например, «Лаборатория Касперского» предоставляет услуги Kaspersky Intelligence Service). Своевременная настройка и проверка сети на основе этих данных позволяет защититься от атаки либо выявить атаку на ранних стадиях.

Основные же принципы обеспечения безопасности в корпоративных сетях остаются прежними:

- Обучение персонала, ведь информационная безопасность — это не только забота службы безопасности, но и обязанность каждого отдельно взятого сотрудника.
- Налаживание процессов безопасности: система безопасности должна адекватно отвечать на эволюционирующие угрозы.
- Использование новых технологий и методов: каждый дополнительный слой защиты позволяет снизить риск проникновения в сеть.

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

Следите за нами

Сайт «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy