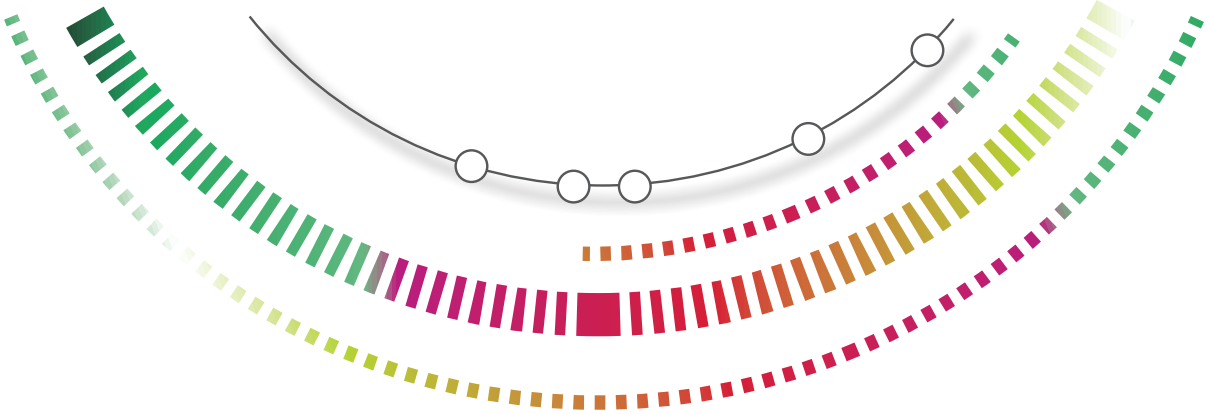
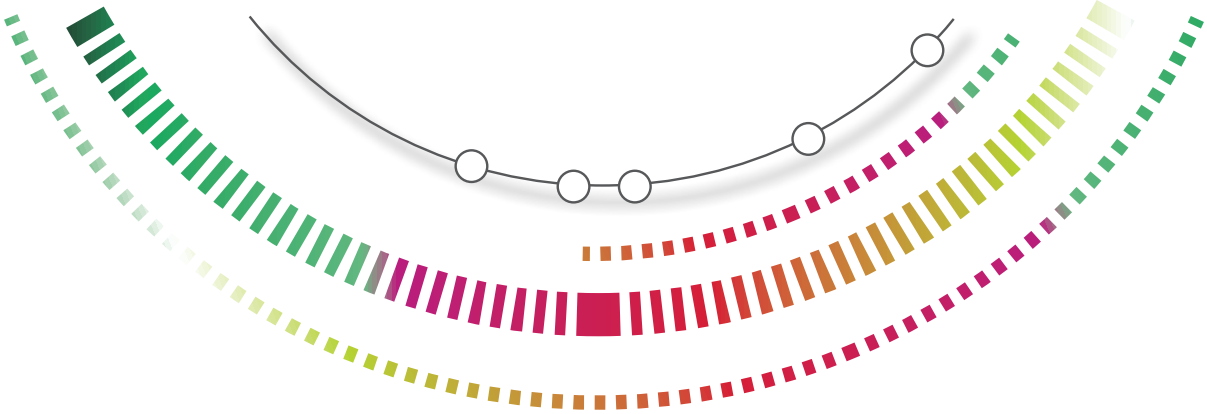
KASPERSKY SECURITY BULLETIN 2014

KASPERSKY lab



ОГЛАВЛЕНИЕ



ПРОГНОЗЫ НА 2015 ГОД

GREAT

Глобальный центр исследований и анализа угроз

КИБЕРПРЕСТУПНИКИ ОСВАИВАЮТ ЦЕЛЕВЫЕ АТАКИ APT-КЛАССА

Мы предполагаем, что в 2015 году деятельность киберпреступников перейдет на новую стадию, с широким внедрением приемов и методов, характерных для атак APT-класса, с целью незаконного получения финансовой выгоды онлайн.

В ходе недавнего исследования мы обнаружили атаку, в результате которой компьютер бухгалтера был взломан и использовался для организации крупного денежного перевода со счетов в финансовом учреждении. Это отражает появление новой интересной тенденции – проведения целевых атак, направленных непосредственно на банки.

Мы наблюдаем стремительный рост количества вредоносных инцидентов, в ходе которых компьютерные сети банков взламываются с использованием методов, применяемых в APT-атаках. Проникнув во внутреннюю сеть банка, злоумышленники скачивают информацию, позволяющую им похищать деньги у банка несколькими способами:

- Удаленно давать команду банкоматам на выдачу наличных.
- Осуществлять денежные переводы по системе SWIFT со счетов клиентов.
- Манипулировать системами онлайн-банкинга для скрытого осуществления денежных переводов.

Эти атаки свидетельствуют о развитии новой тенденции – все более широком применении киберпреступниками методов и приемов, характерных для атак APT-класса.

ФРАГМЕНТАЦИЯ И ДИВЕРСИФИКАЦИЯ АТАК APT-ГРУПП

В 2014 году повышенное внимание к APT-группировкам привело к раскрытию деятельности группы хакеров и предъявлению ей обвинений в кибершпионаже против американских компаний.

Поскольку эксперты в области информационной безопасности продолжают настаивать на предании гласности деятельности APT-группировок, поддерживаемых на государственном уровне, мы ожидаем, что в 2015 году крупные и активные APT-группировки будут делиться на небольшие группы, действующие независимо друг от друга. Это, в свою очередь, приведет к росту количества пострадавших компаний, поскольку мелкие группы диверсифицируют свои атаки. В то же время большие компании, которые ранее подвергались атакам двух-трех крупных APT-группировок (например, Comment Crew и Webky), столкнутся с более разнообразными атаками, исходящими из большего числа источников.

СТАРЫЙ КОД – НОВЫЕ (ОПАСНЫЕ) УЯЗВИМОСТИ

Недавние сообщения о преднамеренных манипуляциях и случайных ошибках в реализации криптографических протоколов (“goto fail”), а также обнаружение критических уязвимостей в важном ПО (Shellshock, Heartbleed, OpenSSL) привели к подозрительному отношению сообщества к непрошедшему аудит программному обеспечению. Реакцией на это стал независимый аудит ключевых программ и привлечение экспертов по IT-безопасности к анализу ПО с целью обнаружения критических уязвимостей, что равнозначно неофициальному аудиту. Из этого следует, что в 2015 году в старом коде будут обнаруживаться новые, опасные уязвимости, что сделает инфраструктуру интернета уязвимой для новых атак.

ЭСКАЛАЦИЯ АТАК НА БАНКОМАТЫ И POS-ТЕРМИНАЛЫ

В этом году было несколько нашумевших случаев атак на банкоматы, повлекших за собой ответные действия со стороны правоохранительных органов разных стран. В результате такой «рекламы» киберпреступники получили сигнал о том, что банкоматы – это спелый плод, который пора сорвать. Большинство банкоматов работает под управлением уязвимой операционной системы Windows XP, а кроме того, плохо защищено физически – это значит, что они, как правило, крайне уязвимы и являются крайне привлекательной мишенью для атак.

В 2015 году ожидается увеличение количества атак на банкоматы с использованием APT-техник для получения доступа к «мозгу» этих устройств. Следующим этапом станет взлом киберпреступниками компьютерных сетей банков и использование полученного доступа для манипуляции банкоматами в режиме реального времени.

АТАКИ НА MAC: БОТНЕТЫ OS X

Несмотря на попытки Apple сделать операционную систему Mac OS максимально закрытой, мы продолжаем наблюдать, как вредоносное ПО загружается на такие компьютеры через торренты и пиратские пакеты программ. Рост популярности устройств Mac OS X не дает покоя криминальному миру, делая создание вредоносных программ для этой платформы все более привлекательным занятием. Изначально закрытая экосистема усложняет для вредоносного ПО проникновение на эту платформу, но всегда находятся пользователи, которые с готовностью отменяют меры безопасности, применяемые в Mac OS X. Прежде всего, речь идет о тех, кто пользуется пиратским ПО.

Таким образом, злоумышленникам, желающим по разным причинам взломать OS X, нужно просто «привязать» свои вредоносные программы к пользующемуся спросом ПО (например, к генератору ключей) и праздновать победу. Из-за всеобщей убежденности в безопасности платформы OS X на такие системы редко устанавливают защитные решения, которые могли бы немедленно предупредить о заражении в случае проникновения вредоносной программы. В результате вредоносное ПО может незаметно хозяйничать в системе в течение длительного времени.

АТАКИ НА АВТОМАТЫ ДЛЯ ПРОДАЖИ БИЛЕТОВ

Инциденты, подобные взлому NFC-сервиса для пополнения транспортных карт общественного транспорта Чили, наглядно демонстрируют, что общественные ресурсы, например, транспортные системы, также представляют интерес для преступников. Некоторые хакеры атакуют эти системы не с целью извлечения прибыли, а лишь для того, чтобы получить пару бесплатных поездок и поделиться этой возможностью с остальными. Однако, как показали эти случаи, системы продажи билетов уязви-

мы (большинство работают на базе Windows XP). При этом во многих городах они напрямую работают с данными транзакций с использованием банковских карт. Мы ожидаем увеличения количества атак на эти системы, проводимых как из чистого азарта, так и с целью кражи реквизитов банковских карт.

АТАКИ НА ВИРТУАЛЬНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

Как подсказывает здравый смысл, киберпреступники ищут способы получить финансовую выгоду от своих смелых опытов наиболее простым и эффективным способом. И что может послужить для этого лучшей мишенью, чем виртуальные платежные системы в стадии их становления? Поскольку многие страны, например Эквадор, спешат внедрить виртуальные платежные системы, мы ожидаем, что преступники будут использовать все имеющиеся возможности, чтобы извлечь из них выгоду. В ход пойдут любые способы, будь то социальная инженерия, атаки на устройства конечных пользователей (во многих случаях, на мобильные телефоны) или взлом непосредственно компьютерных систем банков. При этом финансовое бремя этих атак понесут платежные системы.

Эти опасения также справедливы для нового сервиса Apple Pay, который использует систему NFC (Near Field Communications) для беспроводного проведения транзакций клиентов. Экспертам по IT-безопасности пора вплотную заняться этим рынком, и мы ожидаем появления предупреждений об уязвимостях в Apple Pay, виртуальных кошельках и других виртуальных платежных системах.

APPLE PAY

Предыдущие атаки были нацелены на платежные системы, использующие NFC, но из-за ограниченного распространения последних такие атаки приносили относительно небольшую прибыль. Apple Pay должен изменить ситуацию. Энтузиазм вокруг этой новой платежной платформы приведет к резкому росту ее использования, что неизбежно привлечет внимание киберпреступников, которые не упустят шанс извлечь выгоду из транзакций клиентов. Учитывая, что в архитектуре системы, созданной Apple, большое внимание уделяется безопасности (напри-

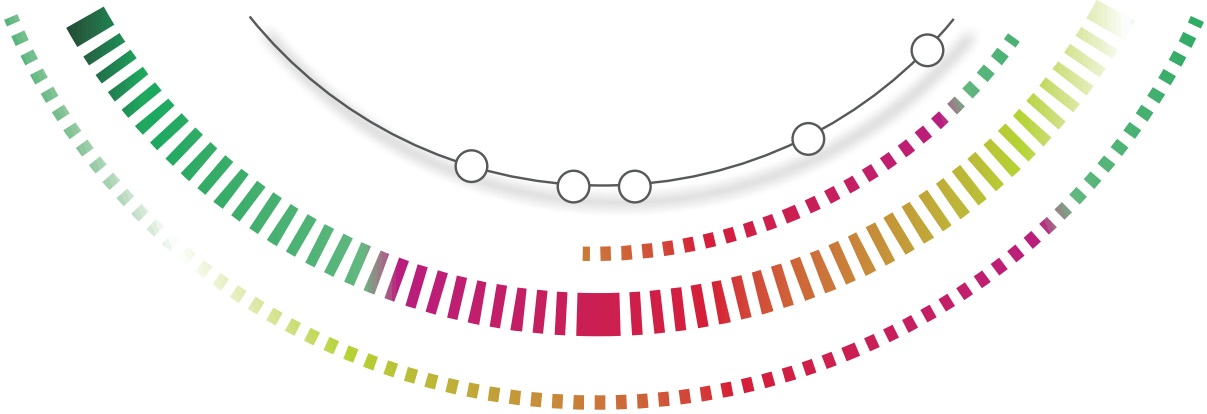
мер, применяется виртуализация транзакционных данных), пока мы можем лишь гадать, каким образом хакеры попытаются использовать эту систему в корыстных целях.

ВЗЛОМ «ИНТЕРНЕТА ВЕЩЕЙ»

Атаки на «Интернет вещей» (Internet of Things, IoT) до сих пор ограничивались пилотными проектами и опасениями (иногда сильно раздутыми), что хакеры попытаются создать ботнеты из «умных» телевизоров и холодильников с целью проведения вредоносных атак.

Мы ожидаем, что появление все большего числа подключенных к сети бытовых устройств станет поводом для более широкой дискуссии о безопасности и сохранности личных данных, особенно среди представителей компаний, занимающихся этими вопросами. В 2015 году «в дикой среде» обязательно будут встречаться вредоносные атаки на сетевые принтеры и другие подключенные устройства, которые злоумышленники будут использовать в качестве плацдарма для проведения дальнейших атак на корпоративную сеть. Мы полагаем, что IoT-устройства займут полноправное место в арсенале APT-групп, особенно при атаках на важные объекты инфраструктуры, где подключение к Интернету используется в промышленных и производственных процессах.

Что касается атак на индивидуальных пользователей, здесь взлом «Интернета вещей» ограничится демонстрацией слабых мест в реализации протоколов и возможностью внедрения рекламы (рекламного/шпионского ПО?) в программу, управляющую работой «умного» телевизора.



ОСНОВНАЯ СТАТИСТИКА ЗА 2014 ГОД

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN) как результат работы различных компонентов защиты от вредоносных программ. Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их передачу. В глобальном обмене информацией о вредоносной активности принимают участие миллионы пользователей продуктов «Лаборатории Касперского» из 213 стран и территорий мира.

Данные представлены за период ноябрь 2013 года – октябрь 2014 года.

Мария Гарнаева
Виктор Чебышев
Денис Макрушин
Роман Унучек
Антон Иванов

ЦИФРЫ ГОДА

— В 2014 году продукты «Лаборатории Касперского» заблокировали **6 167 233 068** вредоносных атак на компьютеры и мобильные устройства пользователей.

— Заблокировано **3 693 936** попыток заражения компьютеров на платформе Mac OS X.

— Отражено **1 363 549** атак на Android-устрйства.

— Решения «Лаборатории Касперского» отразили **1 432 660 467** атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.

— Для проведения атак через интернет злоумышленники воспользовались **9 766 119** уникальными хостами.

— **44%** веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США и Германии.

— В течение года **38,3%** компьютеров пользователей интернета хотя бы раз подвергались веб-атаке.

— Попытки запуска банковского вредоносного ПО отражены на компьютерах **1 910 520** пользователей.

— Нашим веб-антивирусом задетектировано **123 054 503** уникальных вредоносных объекта (скрипты, эксплойты, исполняемые файлы и т.д.).

— На компьютерах пользователей нашим файловым антивирусом задетектировано **1 849 949** вредоносных и потенциально нежелательных программ.

МОБИЛЬНЫЕ УГРОЗЫ

За отчетный период было обнаружено:

— **4 643 582** вредоносных установочных пакета;

— **295 539** новых мобильных вредоносных программ;

— **12 100** мобильных банковских троянцев.

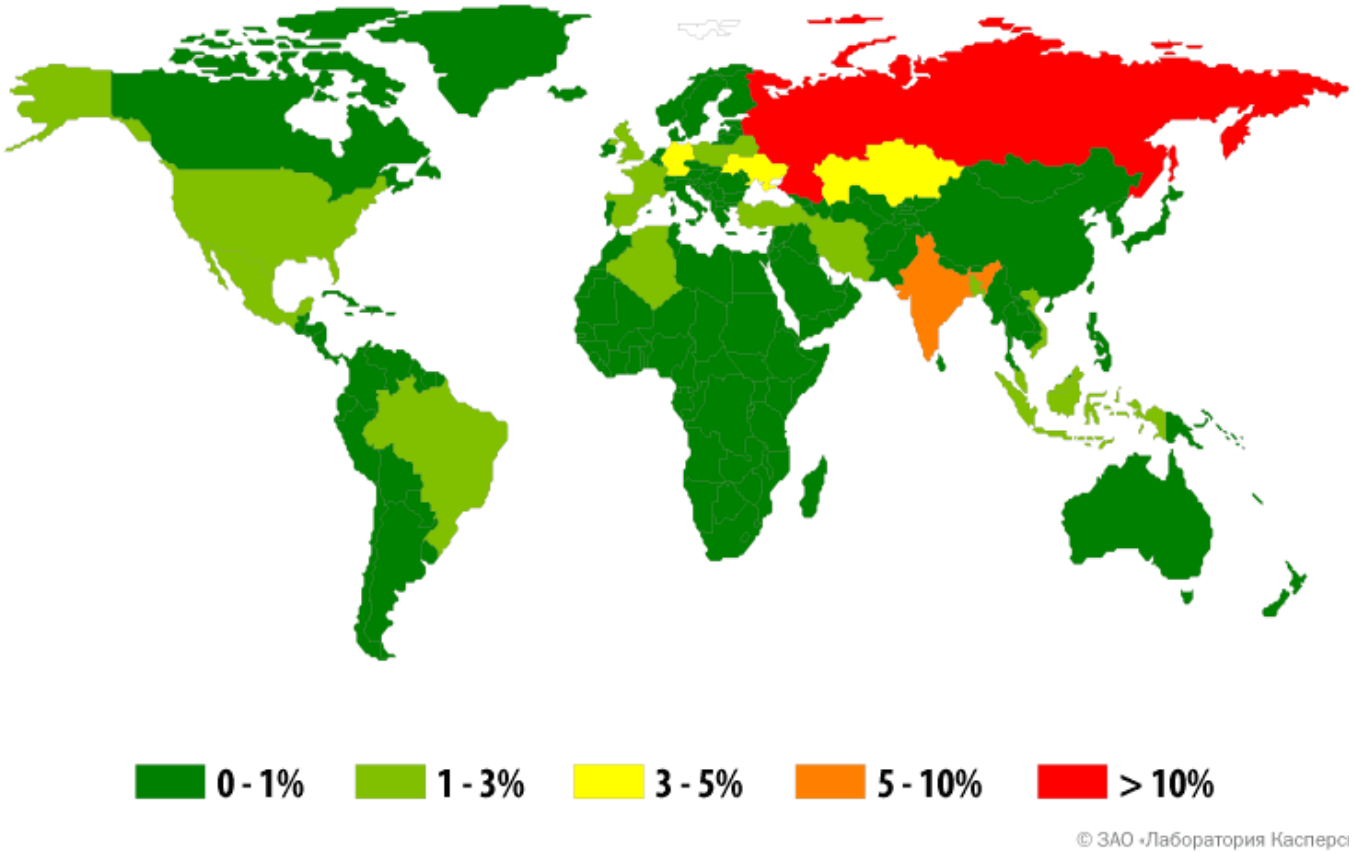
Всего в период с начала ноября 2013 по конец октября 2014 «Лаборатория Касперского» отразила **1 363 549** уникальных атак на Android устройства. За аналогичный период 2012-2013 годов было отражено **335 000** уникальных атак. Таким образом, число атак на Android устройства увеличилось в 4 раза.

В течение года с мобильными угрозами хотя бы раз столкнулись **19%** пользователей Android – практически каждый пятый.

В **53%** Android-атак были использованы мобильные троянцы, нацеленные на кражу денег пользователя (SMS-троянцы и троянцы-банкеры).

География мобильных угроз

Атаки мобильного вредоносного ПО зафиксированы более чем в **200** странах мира.



Процент от всех атакованных уникальных пользователей

TOP 10 стран по числу атакованных пользователей

	Страна	% атакованных пользователей*
1	Россия	45,7%
2	Индия	6,8%
3	Казахстан	4,1%
4	Германия	4,0%
5	Украина	3,0%
6	Вьетнам	2,7%
7	Иран	2,3%
8	Великобритания	2,2%
9	Малайзия	1,8%
10	Бразилия	1,6%

** Процент пользователей, атакованных в стране, от всех атакованных пользователей*

Число зафиксированных атак во многом зависит от числа пользователей в стране. Чтобы оценить опасность заражения мобильными зловредами в разных странах, мы посчитали, какой процент составляют

вредоносные приложения среди всех приложений, которые пытаются установить пользователи. Рейтинг стран по этому показателю отличается от приведенного выше.

TOP 10 стран по риску заражения

	Страна*	% вредоносных приложений
1	Вьетнам	2,34%
2	Польша	1,88%
3	Греция	1,70%
4	Казахстан	1,62%
5	Узбекистан	1,29%
6	Сербия	1,23%
7	Армения	1,21%
8	Чехия	1,02%
9	Марокко	0,97%
10	Малайзия	0,93%

** При расчетах мы исключили страны, в которых число скачиваний приложений менее 100 000*

В этом рейтинге лидирует Вьетнам: в этой стране из всех приложений, которые пытались установить пользователи, на вредоносные пришлось **2,34%**.

Россия, с большим отрывом опережающая все страны по числу атак, по риску заражения заняла **22**-е место с показателем **0,69%**.

В Испании риск заражения составляет **0,54%**, в Германии – **0,18%**, в Великобритании – **0,16%**, в Италии – **0,09**, в США – **0,07%**. Среди всех стран лучше всего ситуация в Японии, где вредоносные приложения составляют всего **0,01%** от всех приложений, которые пытались установить пользователи.

TOP 20 мобильных угроз 2014

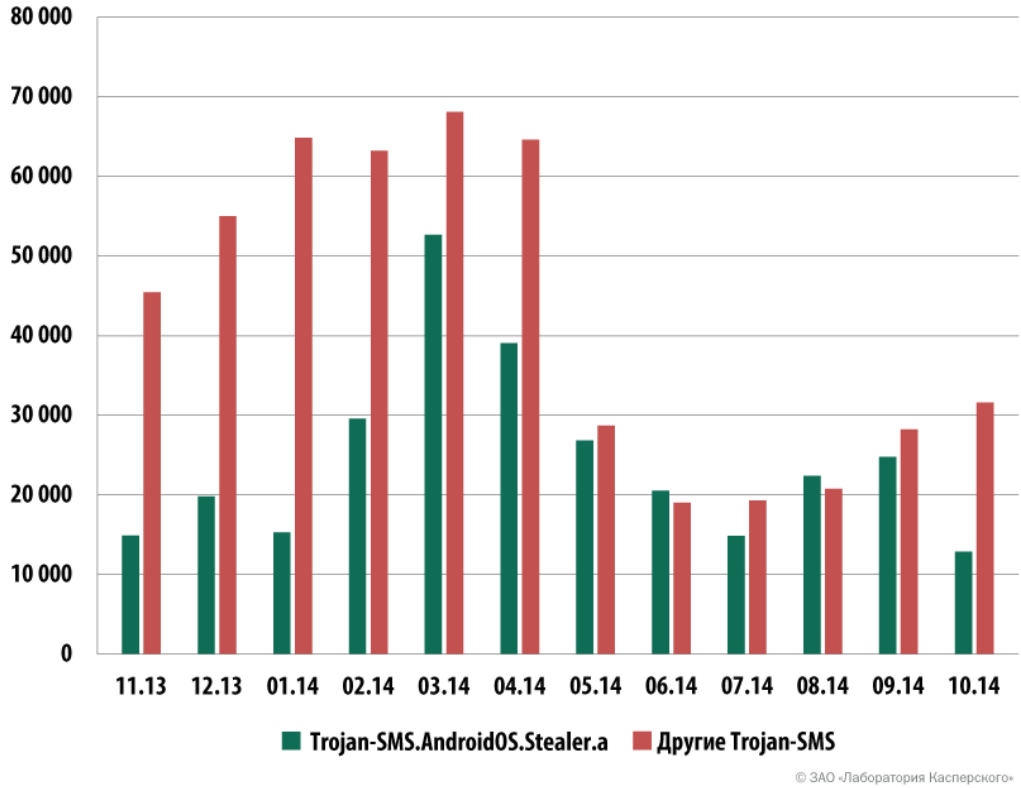
	Название	% атак
1	Trojan-SMS.AndroidOS.Stealer.a	18,0%
2	RiskTool.AndroidOS.MimobSMS.a	7,1%
3	DangerousObject.Multi.Generic	6,9%
4	RiskTool.AndroidOS.SMSreg.gc	6,7%
5	Trojan-SMS.AndroidOS.OpFake.bo	6,4%
6	AdWare.AndroidOS.Viser.a	5,9%
7	Trojan-SMS.AndroidOS.FakeInst.a	5,4%
8	Trojan-SMS.AndroidOS.OpFake.a	5,1%
9	Trojan-SMS.AndroidOS.FakeInst.fb	4,6%

	Название	% атак
10	Trojan-SMS.AndroidOS.Erop.a	4,0%
11	AdWare.AndroidOS.Ganlet.a	3,8%
12	Trojan-SMS.AndroidOS.Agent.u	3,4%
13	Trojan-SMS.AndroidOS.FakeInst.ff	3,0%
14	RiskTool.AndroidOS.Mobogen.a	3,0%
15	RiskTool.AndroidOS.CallPay.a	2,9%
16	Trojan-SMS.AndroidOS.Agent.ao	2,5%
17	Exploit.AndroidOS.Lotoor.be	2,5%
18	Trojan-SMS.AndroidOS.FakeInst.ei	2,4%
19	Backdoor.AndroidOS.Fobus.a	1,9%
20	Trojan-Banker.AndroidOS.Faketoken.a	1,7%

Десять из первых двадцати программ в этом рейтинге – SMS-троянцы семейств Stealer, OpFake, FakeInst, Agent и Erop.

В течение всего года Trojan-SMS.AndroidOS.Stealer.a занимал лидирующие позиции среди всех семейств мобильного вредоносного ПО. По итогам года этот троянец также лидирует.

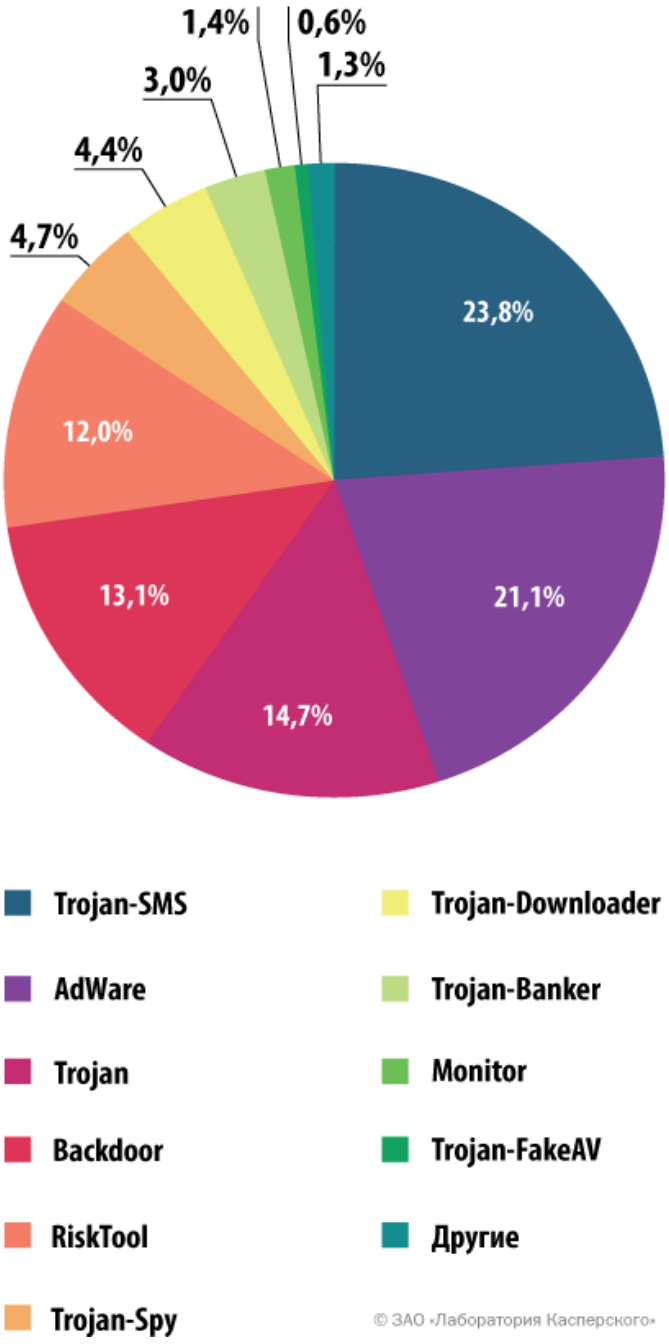
Распространялся этот SMS-троянец весьма активно. С мая 2014 года количество атак Stealer сопоставимо с суммарным количеством атак с использованием других распространённых SMS-троянцев.



Количество пользователей, атакованных Trojan-SMS.AndroidOS.Stealer.a и остальными SMS-троянцами (ноябрь 2013 – октябрь 2014)

SMS-троянцы: уменьшение числа атак

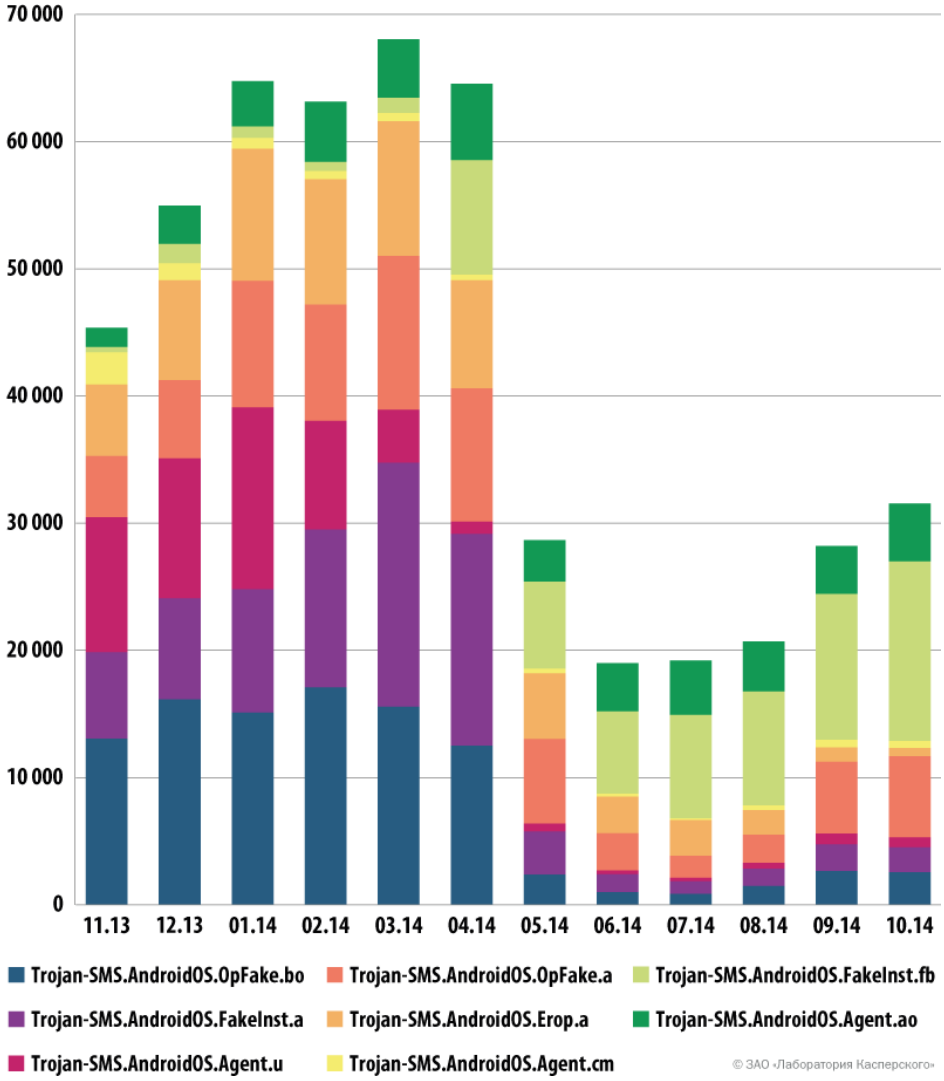
SMS-троянцы по-прежнему доминируют в потоке мобильного вредоносного ПО – в нашей коллекции на них приходится **23,9%**.



Распределение мобильных угроз по типам (коллекция «Лаборатории Касперского»)

Однако, как видно на диаграмме динамики атак выше, во втором полугодии 2014 года количество атак с использованием SMS-троянцев в целом уменьшилось. В результате за год их показатель сократился на **12,3%**.

Рассмотрим подробнее динамику распространения самых популярных у злоумышленников SMS-троянцев (за исключением Stealer.a).



Количество пользователей, атакованных популярными SMS-троянцами (ноябрь 2013 – октябрь 2014)

Зафиксированный в мае резкий спад числа детектов SMS-троянцев обусловлен изменением ситуации с платными сообщениями в России, где атаки с использованием SMS-троянцев особенно популярны у злоумышленников. Дело в том, что с мая 2014 года сотовых операторов в России обязали использовать механизм Advise of Charge (AoC): теперь, когда с мобильного устройства отсылается сообщение на платный номер, оператор обязан уведомить о стоимости услуги/сервиса владельца устройства, который должен подтвердить оплату.

В результате бизнес с использованием SMS-троянцев стал менее прибыльным и откровенно криминальным. Теперь, чтобы получить выгоду, злоумышленникам надо использовать троянцы, которые отправляют SMS на платные номера, перехватывают запрос от оператора и от имени пользователя посылают оператору подтверждение.

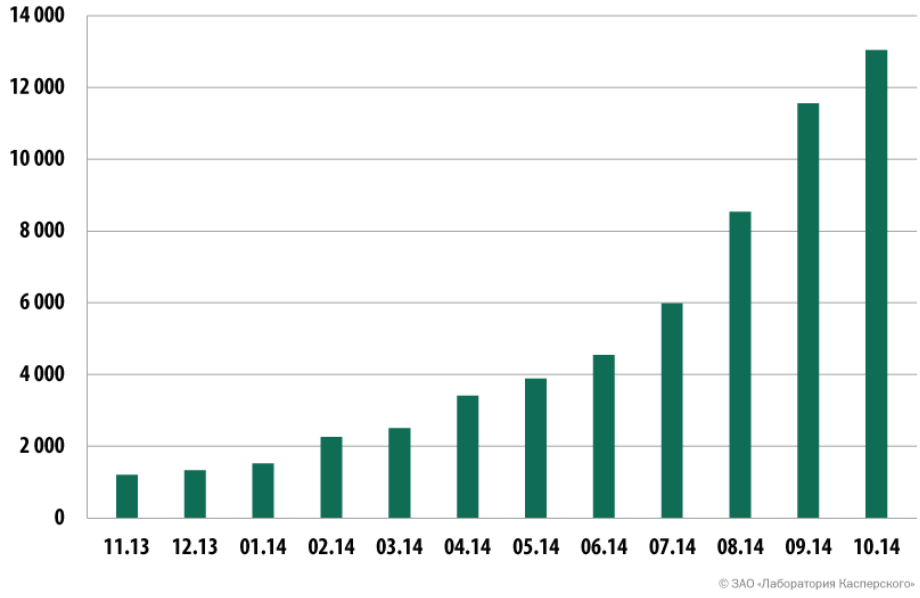
Как следствие, от этого бизнеса отказались некоторые полулегальные партнерские программы, которые ранее занимались распространением приложений с функциональностью SMS-троянцев, где были плохо прописаны условия оказания платной услуги, либо цены на подписку или услугу просто не указывались.

Можно предположить, что оказавшиеся не у дел российские создатели SMS-троянцев будут вынуждены искать новые способы заработка. Часть из них может переключиться на атаки пользователей других стран, часть на более серьезные вредоносные программы, такие как банкеры. Будем надеяться, что найдутся и те, кто не рискнет перейти черту и займется легальной деятельностью.

Изменения динамики распространения хорошо видны на примере таких популярных у злоумышленников SMS-троянцев как OpFake.bo, FakeInst.a и OpFake.a. Их показатели уменьшились с **10-20** тысяч атакованных пользователей в месяц до **1-2** тысяч.

Мобильные банковские троянцы

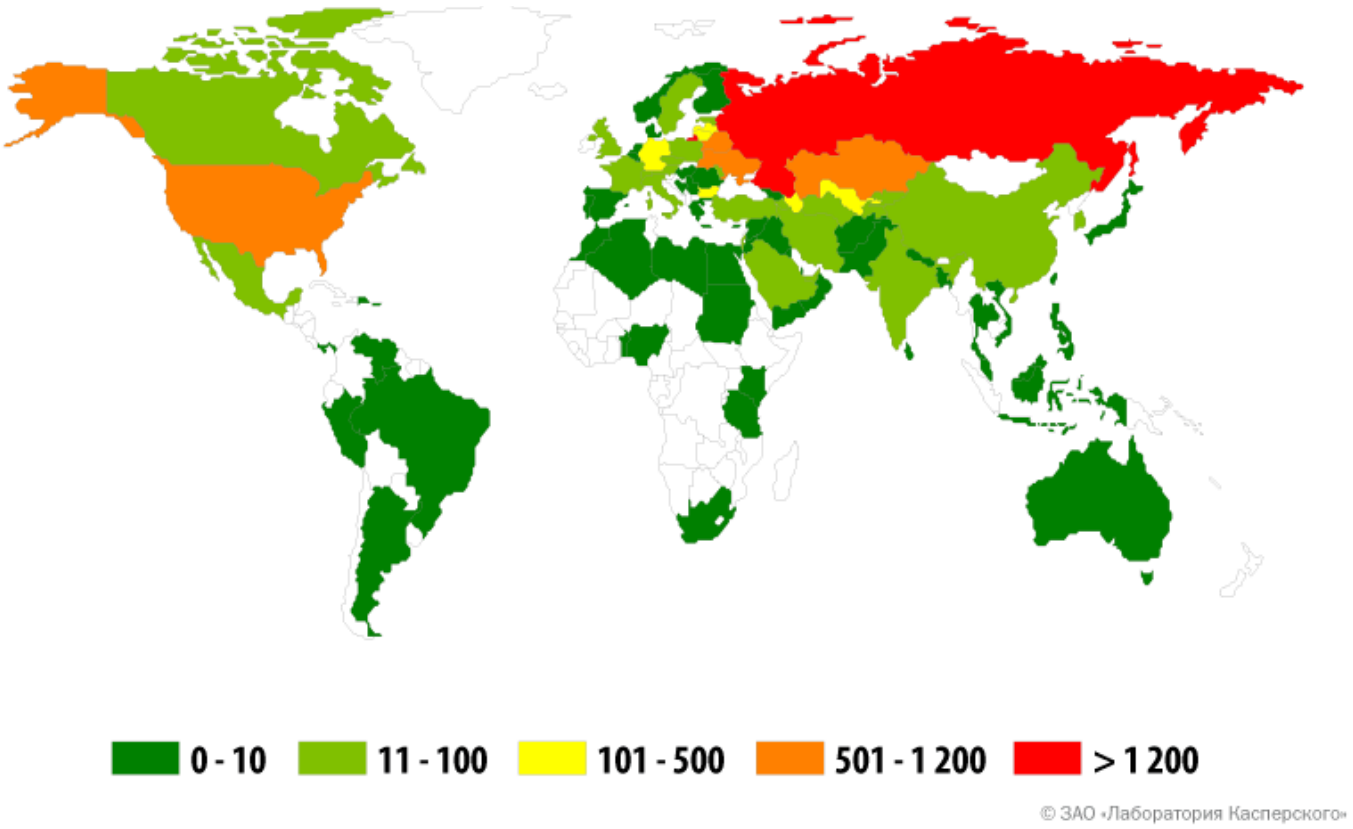
За отчетный период мы обнаружили **12 100** мобильных банковских троянцев – в 9 раз больше, чем в 2013 году.



Количество мобильных банковских троянцев в коллекции «Лаборатории Касперского» (ноябрь 2013 - октябрь 2014)

Мобильными банковскими троянцами хотя бы раз в течение года были атакованы **45 032** пользователя.

Растет количество атакованных стран: атаки мобильных банковских троянцев хотя бы раз были зафиксированы в **90** странах мира.



География мобильных банковских угроз
(количество атакованных пользователей, ноябрь 2013 – октябрь 2014)

TOP 10 стран, атакуемых банковскими троянцами

	Страна	Количество атакованных пользователей	% от всех атак*
1	Россия	39561	87,85%
2	Казахстан	1195	2,65%
3	Украина	902	2,00%
4	США	831	1,85%
5	Белоруссия	567	1,26%
6	Германия	203	0,45%
7	Литва	201	0,45%
8	Азербайджан	194	0,43%
9	Болгария	178	0,40%
10	Узбекистан	125	0,28%

** Процент пользователей, атакованных в стране, по отношению ко всем атакованным пользователям*

Традиционным лидером этого рейтинга остается Россия.

УГРОЗЫ ДЛЯ MAC OS X

В 2014 году продукты «Лаборатории Касперского», предназначенные для защиты компьютеров на платформе Mac OS X, заблокировали **3 693 936** попыток заражения.

Эксперты «Лаборатории Касперского» обнаружили **1499** новых вредоносных программ для Mac OS X, что на **200** зловредов меньше по сравнению с прошлым годом.

Атаке подвергался каждый второй пользователь продуктов компании.

В течение года каждый Mac-пользователь в среднем **9** раз сталкивался с какой-либо угрозой для Mac OS X.

TOP 20 угроз для Mac OS X

	Название	% атак*
1	AdWare.OSX.Geonei.b	9,04%
2	Trojan.Script.Generic	5,85%
3	Trojan.OSX.Vsrch.a	4,42%
4	Trojan.Script.Iframer	3,77%
5	AdWare.OSX.Geonei.d	3,43%
6	DangerousObject.Multi.Generic	2,40%
7	AdWare.OSX.Vsrch.a	2,18%
8	Trojan.Win32.Generic	2,09%
9	AdWare.OSX.FkCodec.b	1,35%
10	Trojan.OSX.Yontoo.i	1,29%
11	Trojan-PSW.Win32.LdPinch.ex	0,84%
12	AdWare.Win32.Yotoon.heur	0,82%
13	Trojan.OSX.Yontoo.j	0,80%
14	Exploit.Script.Generic	0,76%
15	AdWare.OSX.Bnodlero.a	0,58%
16	AdWare.JS.Agent.an	0,57%
17	Trojan.OSX.Yontoo.h	0,52%
18	Exploit.PDF.Generic	0,51%
19	AdWare.Win32.MegaSearch.am	0,5%
20	Trojan.Win32.AutoRun.gen	0,43%

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

Практически половину мест в нашем TOP 20, включая первое место, заняли рекламные программы – AdWare. Как правило, подобные зловреды попадают на компьютер пользователя вместе с легальной программой, если та была загружена не с официального сайта производителя, а с одного из хранилищ ПО. Вместе с программой на компьютер пользователя устанавливается AdWare-модуль, который может добавить рекламные ссылки в закладки браузера, изменить установленную по умолчанию поисковую систему, добавить контекстную рекламу и т.д.

Любопытно, что на 8-м месте расположился зловред Trojan.Win32.Generic, работающий в ОС семейства Windows. Скорее всего, речь идет о проникновении троянца в виртуальную машину, на которой установлена Windows.

В течение 2014 года эксперты обнаружили несколько интересных зловредов для Mac OS X, о которых стоит упомянуть отдельно.

— **Backdoor.OSX.Callme** – бэкдор предоставляет злоумышленнику удаленный доступ к системе и заодно ворует список контактов, видимо, для поиска новых жертв. Распространяется в теле специально сконструированного документа MS Word, который при запуске устанавливает через уязвимость в систему бэкдор.

— **Backdoor.OSX.Laoshu** – зловред каждую минуту делает скриншоты экрана. Этот бэкдор оказался подписанным доверенным сертификатом разработчика, поэтому, возможно, создатели готовились разместить его в AppStore.

— Backdoor.OSX.Ventir – многомодульный троянец-шпион с функцией скрытого удалённого управления. Он несёт в себе драйвер перехвата нажатий клавиатуры logkext, исходный код которого доступен публично.

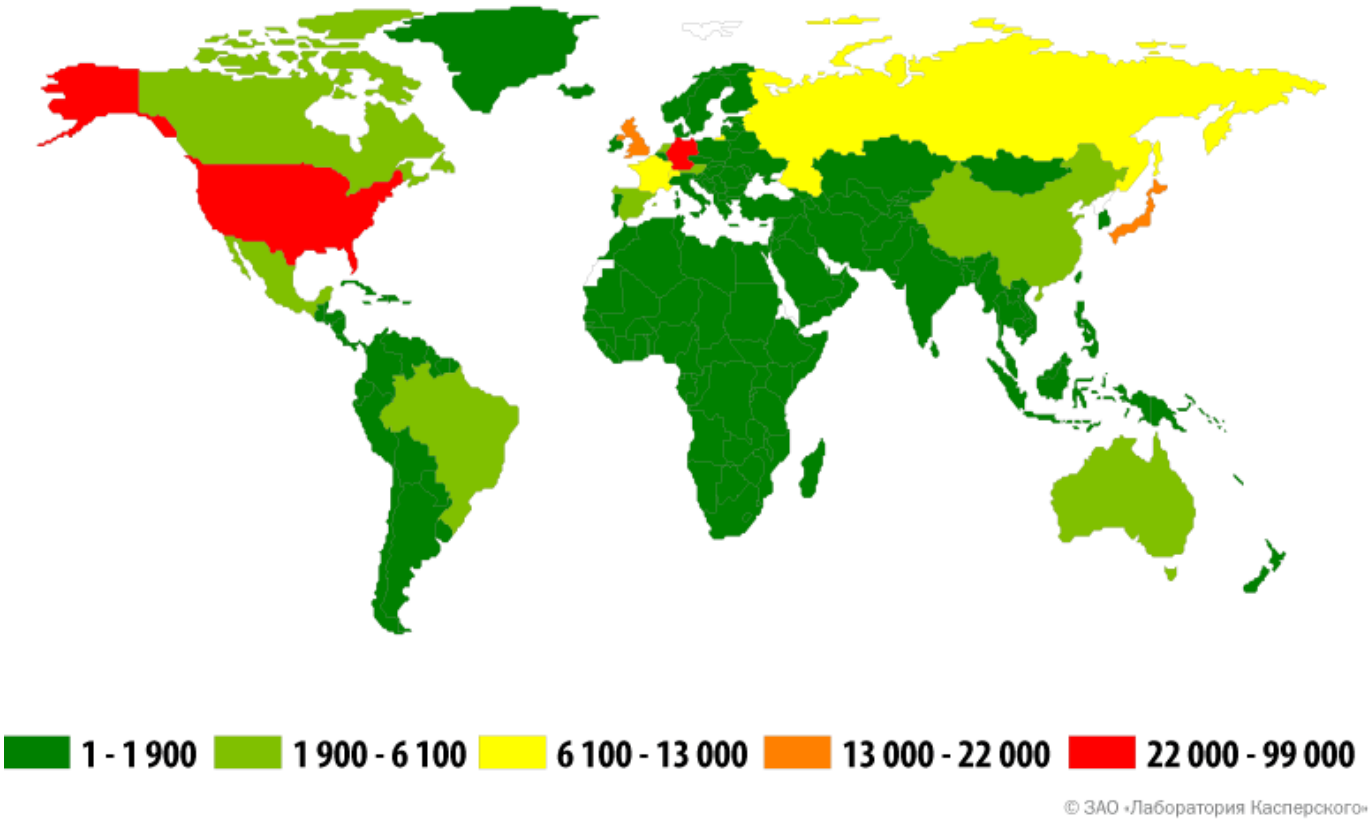
— Trojan.OSX.IOSinfector – установщик мобильной версии Trojan-Spy.IPhoneOS.Mekir (OSX/Crisis).

— Trojan-Ransom.OSX.FileCoder – первый шифровальщик файлов на OS X. Условно рабочий прототип, автор которого по каким-то причинам решил забросить разработку зловреда.

— Trojan-Spy.OSX.CoinStealer – первый похититель биткоинов для OS X, маскирующийся под несколько разных биткоин-утилит с открытым исходным кодом. На самом деле устанавливает вредоносное расширение браузера и/или пропатченный вариант bitcoin-qt.

— Trojan-Downloader.OSX.WireLurker – необычный зловред, занимающийся кражей данных жертвы. Атакует не только Mac-компьютеры, но и подключенные к ним устройства на iOS; существует и Windows-версия зловреда. Распространялся через известный китайский магазин приложений для для OS X и iOS.

География угроз



География атак на пользователей Mac OS X в 2014 году (по количеству атакованных пользователей)

TOP 10 атакуемых стран

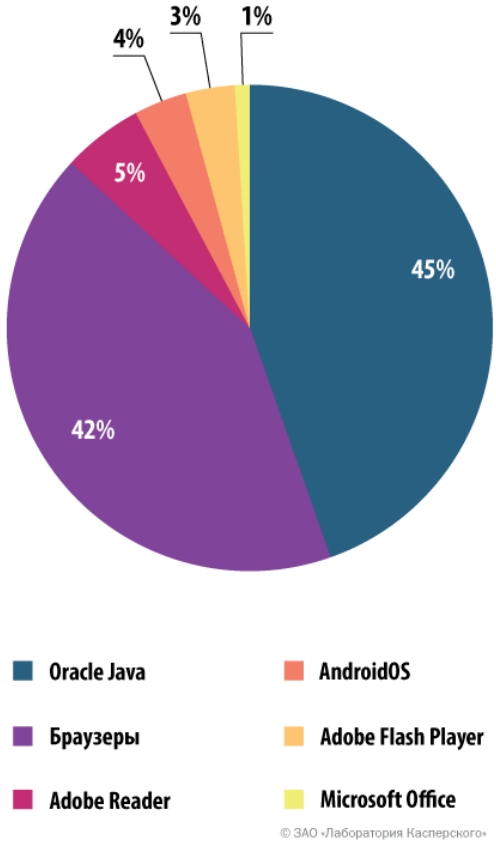
	Страна	Количество атакованных пользователей	% атак*
1	США	98 077	39,14%
2	Германия	31 466	12,56%
3	Япония	13 808	5,51%
4	Великобритания	13 763	5,49%
5	Российская Федерация	12 207	4,87%
6	Франция	9 239	3,69%
7	Швейцария	6 548	2,61%
8	Канада	5 841	2,33%
9	Бразилия	5 558	2,22%
10	Италия	5 334	2,13%

** Процент пользователей, атакованных в стране, от всех атакованных пользователей*

На первой позиции в нашем рейтинге разместились **США** (39,14%), большое количество атак на жителей этой страны можно объяснить популярностью в ней компьютеров Apple. На втором месте **Германия** (12,56%), на третьем – **Япония** (5,51%).

УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

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



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, 2014 год

В 2014 году чаще прочих злоумышленники пытались эксплуатировать уязвимости в Oracle Java. Однако по сравнению с прошлым годом доля этого приложения уменьшилась в два раза – с **90,5%** до **45%**. Мы фиксировали падение популярности Java-уязвимостей на протяжении всего 2014 года – скорее всего, это связано с закрытием старых уязвимостей и отсутствием информации о новых.

Второе место в нашем рейтинге заняла категория «Браузеры» (**42%**), она включает эксплойты для Internet Explorer, Google Chrome, Mozilla Firefox и др. В 2014 году эта категория занимала лидирующую позицию по итогам подсчета показателей последних трех кварталов, но так и не смогла догнать лидера по итогам отчетного периода, поскольку Java-эксплойтов было очень много в конце 2013 - начале 2014 года.

На третьем месте расположились эксплойты для уязвимостей в Adobe Reader (5%). Такие уязвимости эксплуатируются в ходе drive-by атак через интернет, а PDF-эксплойты входят в состав множества эксплойт-паков.

В течение года мы отмечали снижение количества атак с использованием эксплойтов-паков. Это может быть обусловлено сразу несколькими причинами, в частности, арестами некоторых их разработчиков. Кроме того, многие эксплойт-паки перестали атаковать компьютеры, защищенные продуктами «Лаборатории Касперского» (эксплойт-паки проверяют атакуемый компьютер и прекращают атаку, если на нем стоит решение «Лаборатории Касперского»). Несмотря на все перечисленное, эксплуатация уязвимостей остается одним из основных способов доставки вредоносного ПО на компьютер пользователя.

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ (АТАКИ ЧЕРЕЗ WEB)

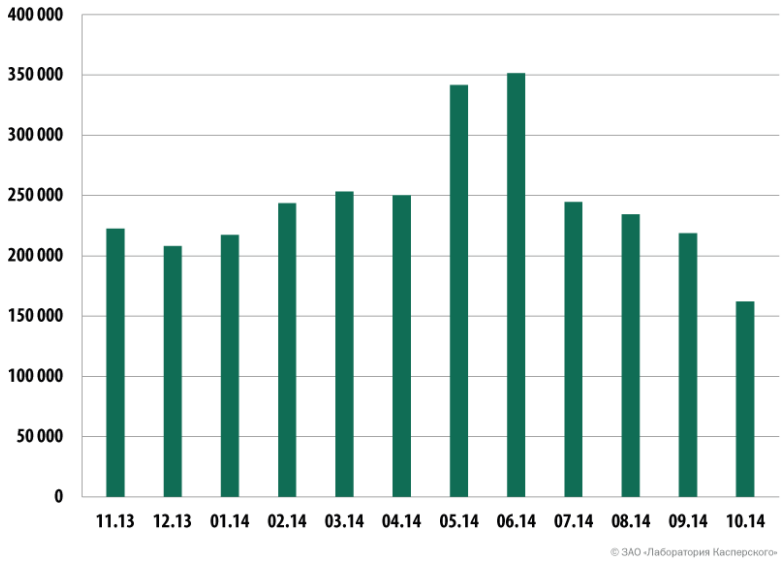
Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей Windows в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями (например, форумы), а также взломанные легитимные ресурсы.

В 2014 году количество атак с интернет-ресурсов, размещенных в разных странах мира, составило **1 432 660 467**. Таким образом, наши продукты защищали пользователей при серфинге в интернете в среднем **3 925 097** раз в день.

Основной способ атаки – через эксплойт-паки – дает злоумышленникам практически гарантированную возможность заражения компьютеров, если на них не установлена защита и имеется хотя бы одно популярное и уязвимое (не обновленное) приложение.

Онлайн-угрозы в банковском секторе

За отчетный период решения «Лаборатории Касперского» отразили попытки запуска вредоносного ПО, предназначенного для кражи денежных средств через онлайн-доступ к банковским счетам, на компьютерах **1 910 520** пользователей.

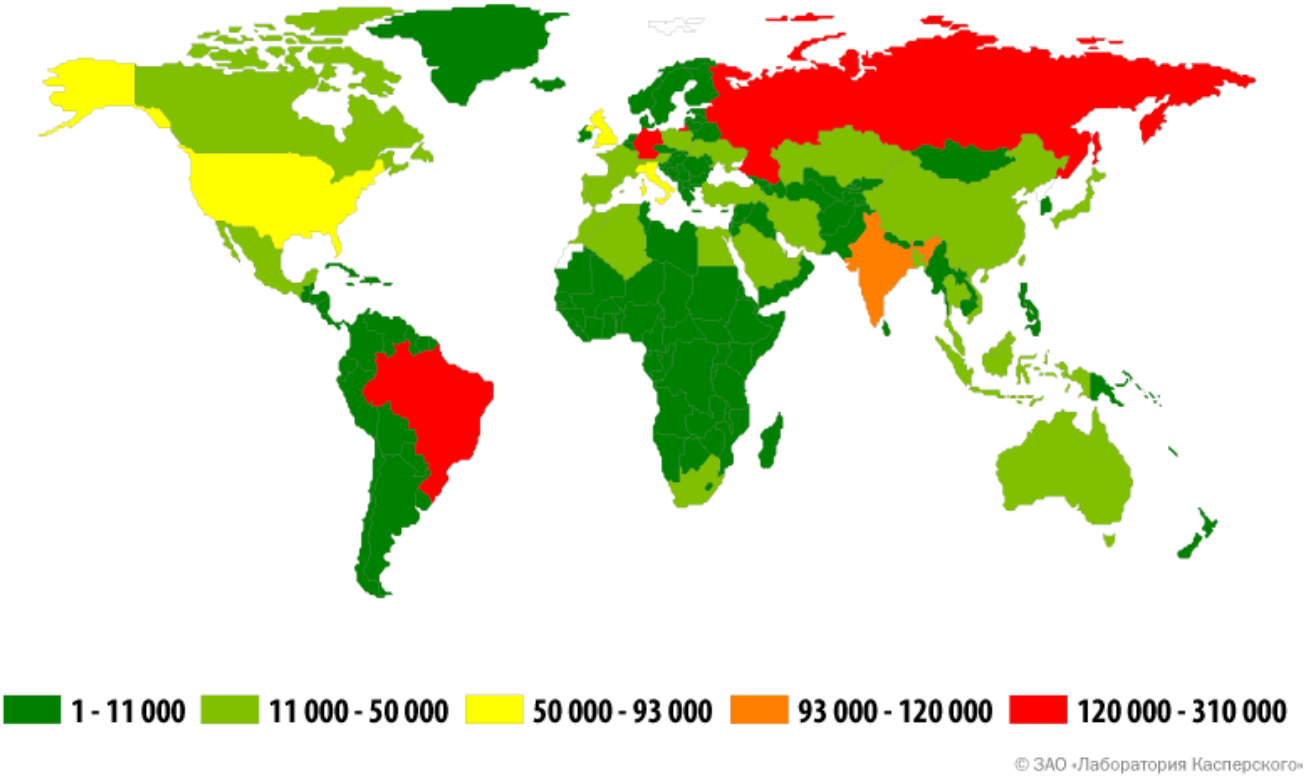


Число компьютеров, атакованных банковским вредоносным ПО, ноябрь 2013 – октябрь 2014

Отметим, что количество атак резко возросло в мае и июне 2014 года. Данный факт связан с началом сезона отпусков, когда растет финансовая активность пользователей онлайн-банкинга, а также главным спортивным событием года – Чемпионатом мира по футболу в Бразилии, в ходе которого преступники использовали финансовое вредоносное ПО для кражи платежных данных туристов.

Всего защитными продуктами «Лаборатории Касперского» было зарегистрировано **16 552 498** уведомлений о попытках заражения вредоносными программами, предназначенными для кражи денежных средств через онлайн-доступ к банковским счетам.

География атак



География атак банковского вредоносного ПО, 2014 год

ТОР 10 стран по числу атакованных пользователей

	Страна	Количество атакованных пользователей
1	Бразилия	299 830
2	Российская федерация	251 917
3	Германия	155 773
4	Индия	98 344
5	США	92 224
6	Италия	88 756

	Страна	Количество атакованных пользователей
7	Великобритания	54 618
8	Вьетнам	50 040
9	Австрия	44 445
10	Алжир	33 640

TOP 10 семейств банковского вредоносного ПО

TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в 2014 году (по количеству атакованных пользователей):

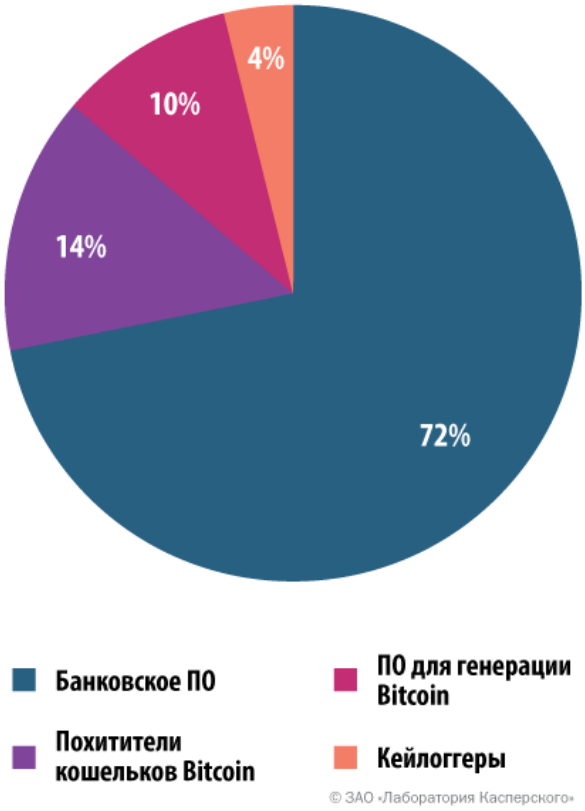
	Название	Количество атакованных пользователей
1	Trojan-Spy.Win32.Zbot	742794
2	Trojan-Banker.Win32.ChePro	192229
3	Trojan-Banker.Win32.Lohmys	121439
4	Trojan-Banker.Win32.Shiotob	95236
5	Trojan-Banker.Win32.Agent	83243
6	Trojan-Banker.AndroidOS.Faketoken	50334
7	Trojan-Banker.Win32.Banker	41665
8	Trojan-Banker.Win32.Banbra	40836
9	Trojan-Spy.Win32.SpyEyes	36065
10	Trojan-Banker.HTML.Agent	19770

Самым распространенным банковским троянцем остается ZeuS (Trojan-Spy.Win32.Zbot). В течение года он лидировал в квартальной статистике, потому неудивительно, что по итогам года он также занял первое место в нашем TOP 10. Вторую позицию занимает Trojan-Banker.Win32.ChePro, третью – Trojan-Banker.Win32.Lohmys. Оба семейства обладают одинаковой функциональностью и распространяются посредством спам-сообщений, тема которых связана с онлайн-банкингом (например, «Счет из интернет-банкинга»). Внутри письма находится документ Word с вложенной картинкой, при нажатии на которую запускается вредоносный код.

Банковский троянец Trojan-Banker.Win32.Shiotob занял четвертое место. Он осуществляет мониторинг трафика с целью перехвата платежных данных и, как многие другие зловреды, распространяется преимущественно посредством спам-сообщений.

Подавляющее большинство зловредов из TOP 10 используют технику внедрения произвольного HTML-кода в отображаемую браузером веб-страницу и перехвата платежных данных, вводимых пользователем в оригинальные и вставленные веб-формы.

Хотя в 2014 году почти три четверти атак, нацеленных на деньги пользователей, осуществлялись при помощи банковского вредоносного ПО, финансовые угрозы этим не ограничиваются.



Распределение атак, нацеленных на деньги пользователей, по типам вредоносного ПО, 2014 год

Второй по популярности угрозой является похищение Bitcoin-кошельков (14%). Далее следует еще одна угроза, связанная с криптовалютой – заражение компьютера с целью его использования для генерации биткойнов, т.е. Bitcoin-майнинг (10%).

Угрозы в интернете: TOP 20

Всего в течение года нашим веб-антивирусом было задетектировано **123 054 503** уникальных вредоносных объекта (скрипты, эксплойты, исполняемые файлы и т.д.).

Мы выделили двадцать угроз, которые в 2014 году чаще всего встречались в интернете. На них пришлось **95,8%** всех атак.

	Название*	**% от всех атак****
1	Malicious URL	73,70%
2	Trojan.Script.Generic	9,10%
3	AdWare.Script.Generic	4,75%

	Название*	% от всех атак**
4	Trojan.Script.Iframer	2,12%
5	Trojan-Downloader.Script.Generic	2,10%
6	AdWare.Win32.BetterSurf.b	0,60%
7	AdWare.Win32.Agent.fflm	0,41%
8	AdWare.Win32.Agent.aiyc	0,38%
9	AdWare.Win32.Agent.allm	0,34%
10	Adware.Win32.Amonetize.heur	0,32%
11	Trojan.Win32.Generic	0,27%
12	AdWare.Win32.MegaSearch.am	0,26%
13	Trojan.Win32.AntiFW.b	0,24%
14	AdWare.JS.Agent.an	0,23%
15	AdWare.Win32.Agent.ahbx	0,19%
16	AdWare.Win32.Yotoon.heur	0,19%
17	AdWare.JS.Agent.ao	0,18%
18	Trojan-Downloader.Win32.Generic	0,16%
19	Trojan-Clicker.JS.Agent.im	0,14%
20	AdWare.Win32.OutBrowse.g	0,11%

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

*** Процент от всех веб-атак, которые были зафиксированы на компьютерах уникальных пользователей.*

Как и прежде, в TOP 20 представлены вердикты, которые присваиваются объектам, использующимся в drive-by атаках, а также рекламным программам и ссылкам из черного списка (первое место – **73,7%**).

Отметим, что по сравнению с прошлым годом увеличилось количество позиций в рейтинге, занятых рекламными программами – с 5 до 12. На рекламные программы, попавшие в TOP 20, пришлось **8,2%** – на 7,01 п.п. больше, чем в 2013 году. Увеличение количества рекламных программ, агрессивные способы их распространения и их противодействие детектированию антивирусов определяют тренд 2014 года.

Вердикт Trojan-Clicker.JS.Agent.im также имеет отношение к рекламной и всяческой «потенциально нежелательной» деятельности. Так детектировались скрипты-редиректоры, размещенные на сервисе Amazon Cloudfront, и перенаправляющие пользователей на страницы с рекламой. Ссылки на эти скрипты вставляются рекламными программами и различными расширениями для браузеров, в основном, на страницы поисковых запросов пользователей. Скрипты могут также перенаправлять пользователей на вредоносные страницы с размещенной на них рекомендацией обновления Adobe Flash и Java – это популярный у злоумышленников прием распространения вредоносных программ.

Страны - источники веб-атак: TOP 10

Данная статистика показывает распределение по странам источников заблокированных антивирусом веб-атак на компьютеры пользователей (веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т.д.). Отметим, что каждый уникальных хост мог быть источником одной и более веб-атак.

Для определения географического источника веб-атак использовалась методика сопоставления доменного имени с реальным IP-адресом, на котором размещен данный домен, и установление географического местоположения данного IP-адреса (GEOIP).

Для проведения **1 432 660 467** атак через интернет злоумышленники воспользовались **9 766 119** уникальными хостами, что на **838 154** (на **8%**) меньше, чем в 2013 году.

87% нотификаций о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира – это на 5 п.п. больше, чем в 2013 году.

Распределение по странам источников веб-атак, ноябрь 2013 – октябрь 2014

Состав стран в первой десятке не изменился по сравнению с 2013 годом, однако поменялось их расположение. Россия сместилась со второй позиции на четвертую, Германия поднялась с четвертого на второе

место. Украина поднялась с шестого на пятое место, вытеснив с него Великобританию, которая в результате оказалась на шестой строчке рейтинга.

44% веб-атак проводились с ресурсов, расположенных в США и Германии.

Страны, в которых пользователи подвергались наибольшему риску заражения через интернет

Чтобы оценить степень риска заражения через интернет, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали, насколько часто в течение года пользователи продуктов «Лаборатории Касперского» в каждой стране сталкивались со срабатыванием веб-антивируса. Полученные данные являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

20 стран, в которых отмечен наибольший риск заражения компьютеров через интернет

	Страна*	**% уникальных пользователей****
1	Россия	53,81%
2	Казахстан	53,04%
3	Азербайджан	49,64%
4	Вьетнам	49,13%
5	Армения	48,66%
6	Украина	46,70%
7	Монголия	45,18%
8	Белоруссия	43,81%
9	Молдавия	42,41%
10	Киргизия	40,06%
11	Германия	39,56%
12	Алжир	39,05%
13	Катар	38,77%
14	Таджикистан	38,49%
15	Грузия	37,67%
16	Саудовская Аравия	36,01%
17	Австрия	35,58%
18	Литва	35,44%

	Страна*	% уникальных пользователей**
19	Шри Ланка	35,42%
20	Турция	35,40%

Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

** При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).*

*** Процент уникальных пользователей, подвергшихся веб-атакам, от всех уникальных пользователей продуктов ЛК в стране.*

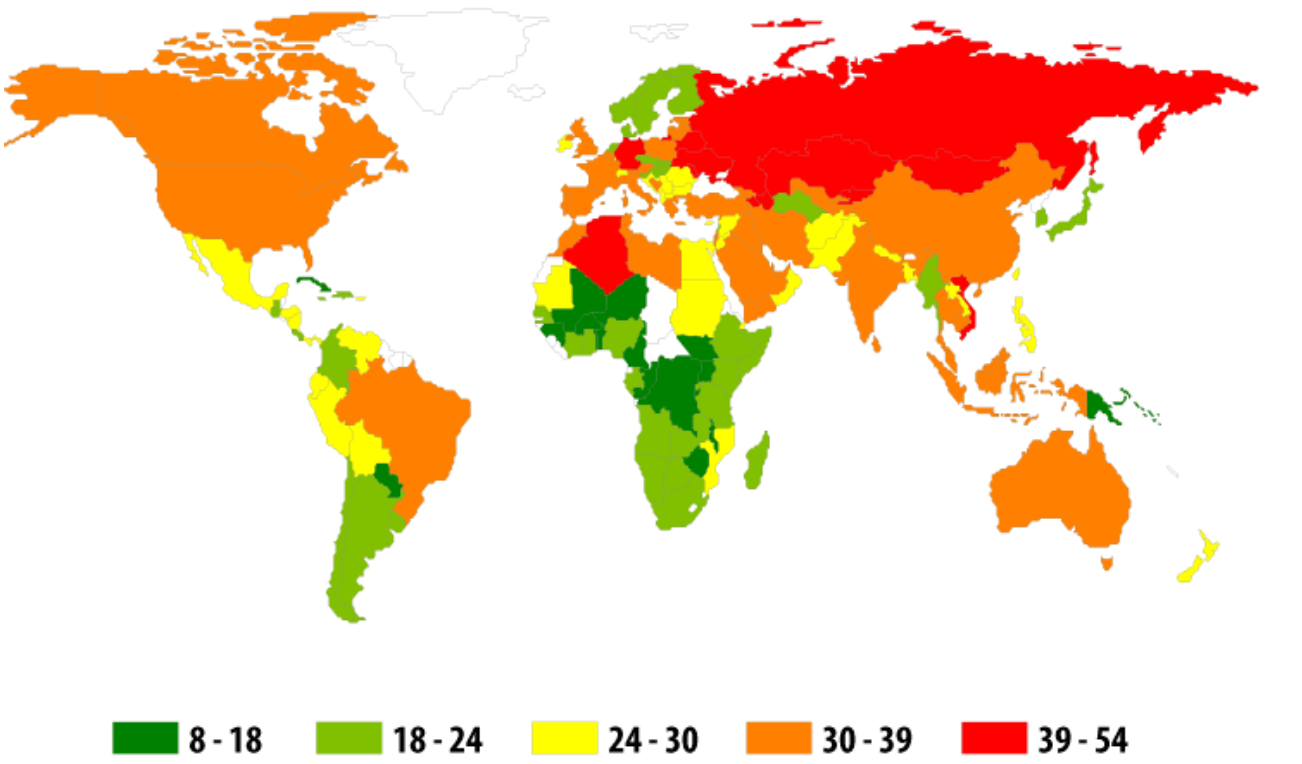
В 2014 году в этом рейтинге сменился лидер: наибольший риск заражения через интернет в России, где веб-атакам подверглись **53,81%** пользователей.

Лидер прошлого года Азербайджан опустился на третье место (49,64%).

Покинули TOP 20 Индия, Узбекистан, Малайзия, Греция и Италия. Среди новичков – Монголия, Катар, Саудовская Аравия, Литва и Турция.

Все страны мира по степени риска заражения при серфинге в интернете можно распределить на три группы.

1. Группа повышенного риска. В эту группу с результатом выше 41% вошли первые девять стран из TOP 20. Эта группа уменьшилась: по итогам 2013 года в нее входило **15** стран.
2. Группа риска. В эту группу с показателями 21-40,9% попали **111** стран, в том числе: Киргизия (40,1%), Германия (39,6%), Катар (38,8%), Таджикистан (38,5%), Грузия (37,7), Саудовская Аравия (36%), Турция (35,4%), Франция (34,9%), Индия (34,8%), Испания (34,4%), США (33,8%), Канада (33,4%), Австралия (32,5%), Бразилия (32,1%), Польша (31,7%), Италия (31,5%), Израиль (30,2%), Китай (30,1%), Великобритания (30%), Египет (27,8%), Мексика (27,5%), Филиппины (27,2%), Хорватия (26,2%), Пакистан (26,1%), Румыния (25,7%), Япония (21,2%), Аргентина (21, 1%).
3. Группа самых безопасных при серфинге в интернете стран (0-20,9%) В эту группу попали **39** стран. В нее входят Швеция (19,5%), Дания (19,2%), Уругвай (19,5%) и ряд африканских стран.



В 2014 году при серфинге в интернете веб-атакам хотя бы раз подверглись **38,3%** компьютеров пользователей интернета.

В среднем уровень опасности интернета за год снизился на 3,3 п.п. Это может быть обусловлено несколькими факторами:

— Во-первых, свой вклад в борьбу с вредоносными сайтами стали вносить браузеры и поисковые системы, разработчики которых обеспокоились безопасностью пользователей.

— Во-вторых, многие эксплойт-паки стали проверять, стоит ли у пользователя наш продукт. Если продукт стоит, то эксплойты не пытаются атаковать компьютер пользователя.

— В-третьих, все чаще пользователи отдают предпочтение для серфинга в интернете мобильным устройствам и планшетам.

Кроме того, немного уменьшилось число атак с использованием эксплойт-паков – аресты их разработчиков не проходят зря. Однако не стоит ждать радикального изменения ситуации с эксплойтами они по-прежнему являются основным способом доставки вредоносных программ, в том числе в случае таргетированных атак. Интернет по-прежнему является основным источником вредоносных объектов для пользователей большинства стран мира.

ЛОКАЛЬНЫЕ УГРОЗЫ

Исключительно важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают объекты, которые проникли на компьютеры пользователей Windows не через интернет, почту или сетевые порты.

В этом разделе мы анализируем статистические данные, полученные на основе работы антивируса, сканирующего файлы на жестком диске в момент их создания или обращения к ним, и данные по сканированию различных съемных носителей информации.

Вредоносные объекты, обнаруженные на компьютерах пользователей: TOP 20

В 2014 году нашим файловым антивирусом было задетектировано **1 849 949** вредоносных и потенциально нежелательных программ.

	Название	% уникальных атакованных пользователей*
1	DangerousObject.Multi.Generic	26,04%
2	Trojan.Win32.Generic	25,32%
3	AdWare.Win32.Agent.ahbx	12,78%
4	Trojan.Win32.AutoRun.gen	8,24%
5	Adware.Win32.Amonetize.heur	7,25%
6	Virus.Win32.Sality.gen	6,69%
7	Worm.VBS.Dinihou.r	5,77%
8	AdWare.MSIL.Kranet.heur	5,46%
9	AdWare.Win32.Yotoon.heur	4,67%
10	Worm.Win32.Debris.a	4,05%
11	AdWare.Win32.BetterSurf.b	3,97%
12	Trojan.Win32.Starter.lgb	3,69%
13	Exploit.Java.Generic	3,66%
14	Trojan.Script.Generic	3,52%
15	Virus.Win32.Nimnul.a	2,80%
16	Trojan-Dropper.Win32.Agent.jkcd	2,78%
17	Worm.Script.Generic	2,61%
18	AdWare.Win32.Agent.aljt	2,53%

	Название	% уникальных атакованных пользователей*
19	AdWare.Win32.Kranet.heur	2,52%
20	Trojan.WinLNK.Runner.ea	2,49%

Данная статистика представляет собой детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

** Процент уникальных пользователей, на компьютерах которых файловый антивирус детектировал данный объект, от всех уникальных пользователей продуктов «Лаборатории Касперского», у которых происходило срабатывание антивируса.*

Первое место занимает вердикт DangerousObject.Multi.Generic (26,04%), используемый для вредоносных программ, обнаруженных с помощью облачных технологий. Эти технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, но в облаке антивирусной компании уже есть информация об объекте. По сути, так детектируются самые новые вредоносные программы.

Из топа выбыл знаменитый червь Net-Worm.Win32.Kido. Продолжает падать доля вирусов: например, Virus.Win32.Sality.gen в прошлом году встречался у **13,4%** пользователей, в 2014 – у **6,69%**.

Рекламные программы становятся все более распространенными, что отражено как в этом рейтинге, так и в рейтинге веб-детектов. Количество пользователей, столкнувшихся с рекламными программами, по сравнению с прошлым годом выросло почти в два раза и составило **25 406 107** человек. При этом рекламные программы становятся не только все более навязчивыми, но и более опасными. Некоторые «переходят границу» категории потенциально нежелательных, и им присваивается более «суровый» вердикт. Пример такой программы – Trojan-Dropper.Win32.Agent.jkcd (16-е место, 2,78%): она не только донимает пользователя навязчивым показом рекламы и изменяет поисковую выдачу, но и может скачать на компьютер вредоносную программу.

Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения

Для каждой из стран мы подсчитали, насколько часто в течение года пользователи в ней сталкивались со срабатыванием файлового антивируса. Учитывались вредоносные программы, найденные непосредственно на компьютерах пользователей или же на съемных носителях, подключенных к компьютерам, – флешках, картах памяти фотоаппаратов, телефонов, внешних жестких дисках. Эта статистика отражает уровень зараженности персональных компьютеров в различных странах мира.

TOP 20 стран по уровню зараженности компьютеров

	Страна*	%**
1	Вьетнам	69,58%
2	Монголия	64,24%
3	Непал	61,03%
4	Бангладеш	60,54%
5	Йемен	59,51%
6	Алжир	58,84%
7	Ирак	57,62%
8	Лаос	56,32%
9	Индия	56,05%
10	Камбоджа	55,98%
11	Афганистан	55,69%
12	Египет	54,54%
13	Саудовская Аравия	54,37%
14	Казахстан	54,27%
15	Пакистан	54,00%
16	Сирия	53,91%
17	Судан	53,88%
18	Шри-Ланка	53,77%
19	Мьянма	53,34%
20	Турция	52,94%

Настоящая статистика основана на детектирующих вердиктах файлового антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

** При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).*

*** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.*

Первая четверка лидеров не изменилась по сравнению с прошлым годом: первое место по-прежнему занимает Вьетнам; Монголия и Бангладеш поменялись местами – Бангладеш опустился со второго на четвертое место, Монголия поднялась с четвертого на второе.

Покинули TOP 20 Джибути, Мальдивы, Мавритания, Индонезия, Руанда и Ангола. Среди новичков – Йемен, Саудовская Аравия, Казахстан, Сирия, Мьянма и Турция.

В среднем в группе стран из TOP 20 вредоносный объект хотя бы раз был обнаружен на компьютере — на жестком диске или на съемном носителе, подключенном к нему, — у **58,7%** пользователей KSN, предоставляющих нам информацию, тогда как в 2013 году – у **60,1%**.

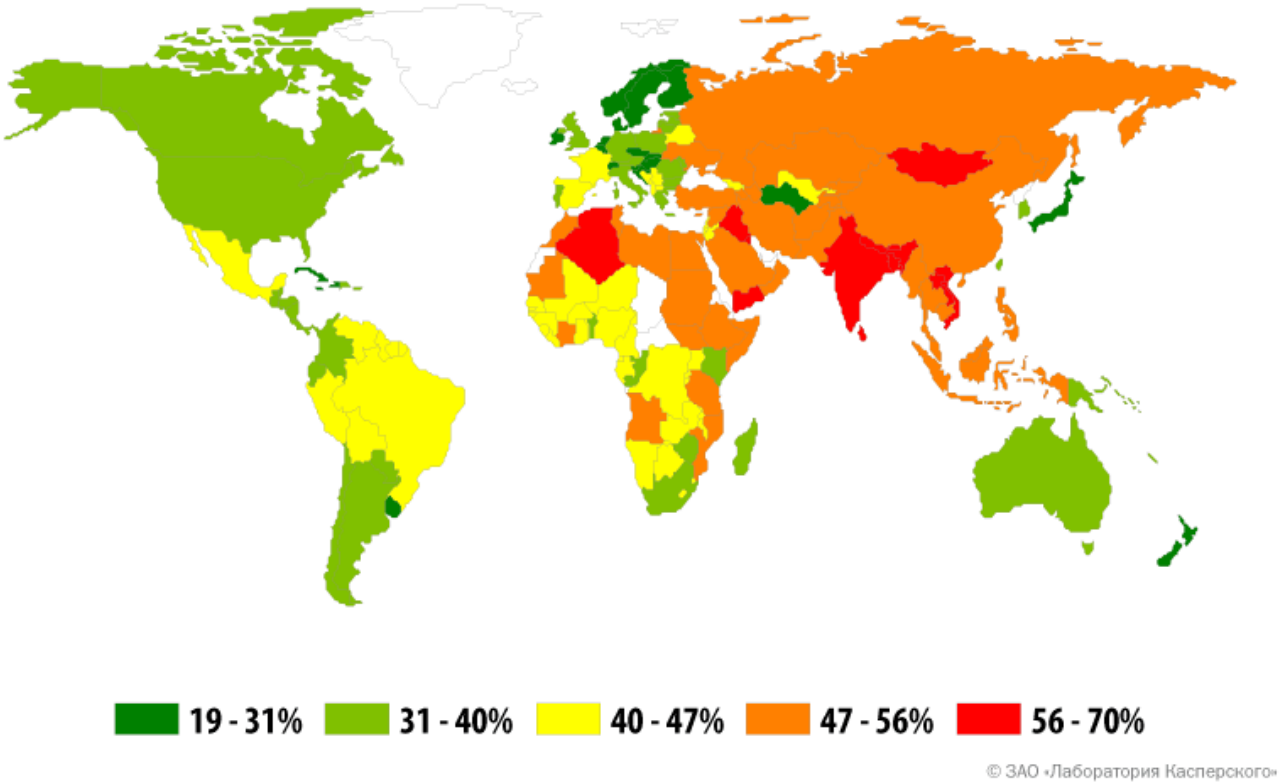
В случае локальных угроз мы можем разделить все страны мира на несколько категорий.

1. Максимальный уровень заражения (более 60%): 4 страны, лидирующие в рейтинге, — Вьетнам (69,6%), Монголия (64,2%), Непал (61,0%) и Бангладеш (60,5%).

2. Высокий уровень заражения (41-60%): 83 страны мира, в том числе Индия (56,0%), Казахстан (54,3%), Турция (52,9%), Россия (52,0%), Китай (49,7%), Бразилия (46,5%), Белоруссия (45,3%), Мексика (41,6%), Филиппины (48,4%).

3. Средний уровень заражения (21-40,9%): 70 стран, в том числе Испания (40,9%), Франция (40,3%), Польша (39,5%), Литва (39,1%), Греция (37,8%), Португалия (37,7%), Корея (37,4%), Аргентина (37,2%), Италия (36,6%), Австрия (36,5%), Австралия (35,3%), Канада (34,8%), Румыния (34,5%), США (34,4%), Великобритания (33,8%), Швейцария (30,8%), Гонконг (30,4%), Ирландия (29,7%), Уругвай (27,8%), Нидерланды (26,4%), Норвегия (25,1%), Сингапур (23,5%), Япония (22,9%), Швеция (23%), Дания (21,3%).

4. Наименьший уровень заражения (0-20,9%): 3 страны мира: Финляндия (20%), Куба (19,1%) и Сейшельские острова (19%).



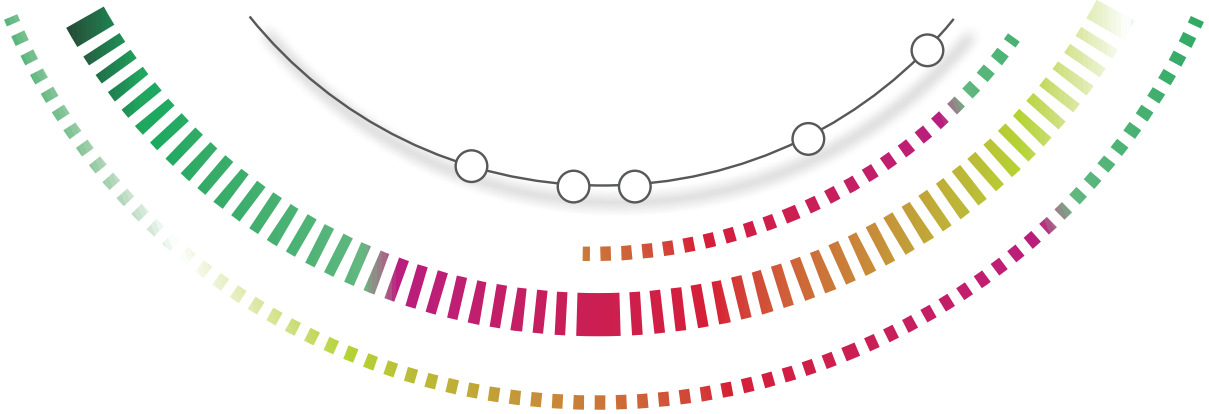
В десятку самых безопасных по уровню локального заражения стран попали:

	Страна	**%***
1	Сейшельские острова	19,03%
2	Куба	19,08%
3	Финляндия	20,03%
4	Дания	21,34%
5	Япония	22,89%
6	Швеция	22,98%
7	Чехия	23,13%
8	Сингапур	23,54%
9	Мартиника	25,04%
10	Норвегия	25,13%

** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.*

По сравнению с 2013 годом в списке произошли изменения – появились Мартиника, Сингапур и Швеция; покинули рейтинг Словакия, Словения и Мальта.

В среднем в десятке самых безопасных стран мира хотя бы раз в течение года было атаковано **23%** компьютеров пользователей. По сравнению с прошлым годом этот показатель увеличился на **4,2%**.



10 ВАЖНЕЙШИХ ИНЦИДЕНТОВ 2014 ГОДА В СФЕРЕ IT-БЕЗОПАСНОСТИ

Конец года – время размышлений, подведения итогов уходящего года перед попыткой заглянуть в будущее. Предлагаем читателям наш традиционный обзор ключевых инцидентов, которые сформировали ландшафт киберугроз в 2014 году.

Дэвид Эмм

ЦЕЛЕВЫЕ АТАКИ И ВРЕДОНОСНЫЕ КАМПАНИИ

Целевые атаки стали неотъемлемой частью общей ситуации в области киберугроз, поэтому нет ничего удивительного в том, что мы рассказываем о них в своем годовом отчете.

Сложная кибершпионская кампания, получившая название «Careto», или «Маска» (Careto – испанское жаргонное слово, означающее «рожа» или «маска»), была нацелена на кражу конфиденциальных данных у определенных организаций. В числе жертв оказались государственные учреждения, посольства, энергетические компании, исследовательские институты, частные инвестиционные компании и активисты из 31 страны мира. В состав Careto входил сложный троянец-бэкдор, способный перехватывать различные каналы обмена иформацией и собирать самые разные данные на зараженных компьютерах, в том числе ключи шифрования, настройки VPN, ключи SSH, RDP-файлы, а также некоторые неизвестные типы файлов, возможно, имеющие отношение к заказным инструментам шифрования правительственного или военного уровня.

Код бэкдора имеет развитую модульную структуру, что позволяет атакующим добавлять любой нужный им функционал. Существуют версии бэкдора для Windows и Mac OS X; мы также нашли в некоторых модулях указания на существование версий для Linux, iOS и Android.

Как и всегда со столь сложными кампаниями, атрибуция затруднена. Использование в коде испанского языка не помогает, поскольку по-испански говорят во многих странах. Кроме того, не исключено, что это «отвлекающий маневр», призванный повести экспертов по ложному следу. В любом случае, чрезвычайно высокий уровень профессионализма тех, кто стоит за этой кампанией, не характерен для киберпреступных групп – это один из признаков, говорящих о возможной поддержке Careto на государственном уровне. Как и другие кампании, связанные с целевыми атаками, Careto в течение достаточно долгого времени оставалась в тени: судя по всему, группа активно действует с 2007 года.

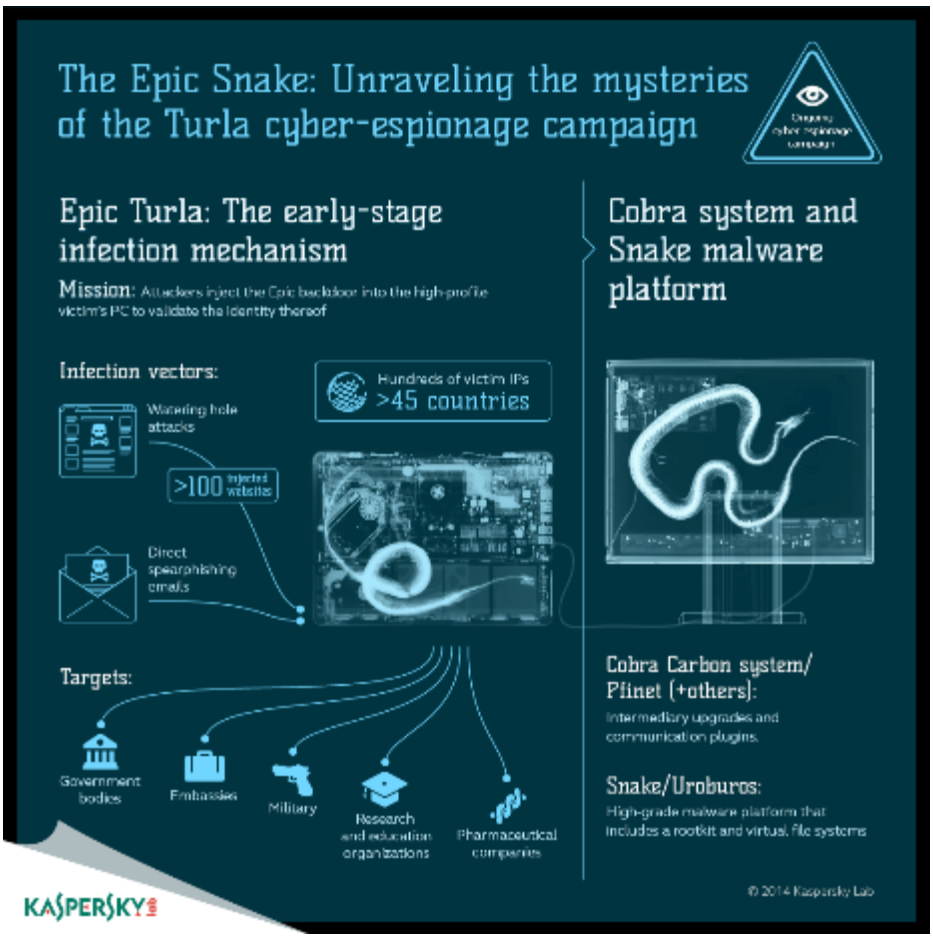
В начале марта эксперты в области безопасности много обсуждали кибершпионскую кампанию Epic Turla. По мнению экспертов компании G DATA вредоносная программа, возможно, была создана российскими спецслужбами. А исследование, проведенное BAE Systems, установило связь между ней и вредоносной программой, известной под названием «Agent.btz», которая была создана в 2007 году и использовалась в 2008 году для заражения локальных сетей американского военного командования на Ближнем Востоке.

В центре внимания нашего первоначального анализа Epic Turla было использование вредоносной программой USB-накопителей для хранения украденных данных, которые невозможно отправить на командный сервер злоумышленников напрямую через интернет. Червь записывает файл под названием thumb.dd на все USB-накопители, подключенные к зараженному компьютеру. Если впоследствии накопитель подключается к другому компьютеру, файл thumb.dd копируется на этот компьютер. Epic Turla – не единственная вредоносная программа, «знающая» о файле thumb.dd. В частности, он входит в число файлов модуля USB Stealer в Red October. Если заглянуть еще дальше назад, Gauss и miniFlame «знали» о thumb.dd и искали этот файл на USB-накопителях. Схему, на которой показаны точки соприкосновения этих шпионских кампаний можно найти здесь. Вероятно, по всему миру разбросаны десятки тысяч флешек с файлом thumb.dd, созданным этой вредоносной программой.

В нашем последующем анализе Epic Turla мы объяснили, как злоумышленники использовали социальную инженерию для распространения вредоносного ПО, а также охарактеризовали общую структуру кампании. Киберпреступники используют адресную рассылку электронных писем, обманным путем побуждая жертв установить на свои компьютеры бэкдор. Некоторые из фишинговых писем содержат эксплойты нулевого дня. Один из них использует уязвимость в Adobe Acrobat Reader, другой – уязвимость в Windows XP и Windows Server 2003, позволяю-

щую повысить привилегии в системе. Преступники также применяют атаки типа watering-hole, с помощью которых доставляют на компьютеры жертв Java-эксплойты, эксплойты для Adobe Flash и эксплойты для Internet Explorer, а также обманным путем побуждают жертв запустить вредоносные инсталляторы, замаскированные под Flash Player. В зависимости от IP-адреса жертвы атакующие выбирают для доставки на ее компьютер эксплойты для Java или браузера, подписанный экземпляр фальшивого ПО Adobe Flash Player или поддельную версию Microsoft Security Essentials. Очевидно, что выбор сайтов отражает интересы злоумышленников (а также их жертв).

При этом наш анализ показал, что применение бэкдора Epic Turla – лишь первая стадия заражения. Он используется для установки более сложного бэкдора, известного как Cobra/Carbon system (в некоторых антивирусных продуктах он именуется Pfinet). Существование уникального набора информации, необходимого для управления работой обоих бэкдоров, говорит о наличии ясной и прямой связи между ними. Первый применяется для закрепления в зараженной системе и подтверждения высокого статуса жертвы. Убедившись в том, что жертва представляет для них интерес, киберпреступники устанавливают на зараженный компьютер вредоносный комплекс более высокого уровня – Carbon System. Обзорную информацию о кампании Epic Turla можно найти здесь:



В июне мы рассказали о выполненном нами анализе атаки на клиентов крупного европейского банка, в результате которой всего за неделю было украдено полмиллиона евро. Мы дали этой атаке название «Luuuk» по названию папки, в которой размещена панель управления командным сервером. Нам не удалось получить вредоносную программу, с помощью которой заражались компьютеры жертв, но, судя по всему, злоумышленники использовали банковский троянец, который с помощью атаки Man-in-the-Browser осуществлял вредоносную веб-инъекцию, после чего воровал учетные данные жертв. Исходя из информации, найденной в лог-файлах, вредоносная программа воровала имена пользователей, пароли и одноразовые пароли в режиме реального времени. Атакующие использовали украденные учетные данные для проверки баланса принадлежащих жертвам счетов и автоматического проведения вредоносных транзакций; вероятно, вредоносная программа при этом работала в фоновом режиме одновременно с легитимной сессией онлайн-банкинга.

Украденные средства автоматически переводились на заранее подготовленные счета «дропов» («денежных мулов»). Большой интерес представляла применяемая злоумышленниками классификация «денежных мулов». Существовало четыре группы «дропов», формируемых на основе размера денежных сумм, которые могли быть перечислены на счета представителей каждой группы, – вероятно, в зависимости от уровня доверия, которым они пользовались. Всего нам удалось идентифицировать 190 жертв, большая часть которых находилась в Италии и Турции. Суммы, украденные у каждой жертвы, составляли от €1 700 до €39 000. Всего было украдено более €500 000.

Несмотря на то, что киберпреступники удалили все относящиеся к вредоносной деятельности компоненты вскоре после начала нашего расследования, мы считаем, что это было скорее обновлением инфраструктуры, чем полным свертыванием деятельности. Киберпреступники, стоящие за этой кампанией, высокопрофессиональны и очень активны. Кроме того, они, по-видимому, принимают превентивные меры для защиты своей деятельности, а будучи обнаруженными, меняют тактику и заметают следы. «Лаборатория Касперского» продолжает расследование данной кампании, о которой мы сообщили пострадавшему от атак банку и соответствующим правоохранительным органам.

В конце июня возобновила активность кампания по проведению целевых атак, известная как MiniDuke, которая впервые появилась в начале 2013 года. Исходная кампания отличалась от других по ряду параметров. Она использовала нестандартный бэкдор, написанный на «old-school» языке ассемблера. Управление атакой осуществлялось через необычную командную инфраструктуру с применением нескольких резервных каналов, таких как учетные записи в Twitter. Разработчики скрытно передавали обновленные версии исполняемых файлов, маскируя их под GIF-изображения.

В число целей новой кампании, известной как CosmicDuke и TinyBaron, входят государственные структуры, дипломатические ведомства, энергетические компании, военные и операторы телекоммуникационных систем. Но вопреки обыкновению, список жертв также включает лиц, вовлеченных в сбыт и перепродажу запрещенных веществ, в т.ч. стероидов и гормонов. Почему, нам неизвестно. Возможно, гибко настраиваемый бэкдор продавался в качестве «легального» шпионского ПО; может быть, он был выставлен на продажу на подпольном рынке и был приобретен несколькими конкурирующими фармацевтическими компаниями для слежки друг за другом.

Вредоносная программа выдает себя за популярные приложения, работающие в фоновом режиме, используя для этого соответствующие имена и описания файлов, пиктограммы и даже размеры файлов. Сам бэкдор скомпилирован с помощью BotGenStudio – настраиваемого фреймворка, позволяющего злоумышленникам включать и отключать компоненты на этапе сборки бота. Вредоносная программа не только крадет файлы с определенными расширениями, но также собирает пароли, историю браузеров, данные о сети, списки контактов, информацию, отображаемую на экране (снимки экрана делаются раз в пять минут) и другие конфиденциальные данные. Каждой жертве присваивается уникальный идентификатор, что позволяет отправлять конкретным жертвам индивидуально подобранные для них обновления.

Вредоносная программа защищена с помощью специального обфусцированного загрузчика, очень сильно загружающего процессор в течение 3-5 минут, прежде чем выполнить основной код. Это не только значительно затрудняет анализ кода, но и отвлекает значительные ресурсы, необходимые защитному ПО для эмуляции выполнения вредоносной программы. Помимо собственного обфускатора вредоносная

программа широко использует шифрование и сжатие на основе алгоритмов RC4 и LZRW. Реализация этих алгоритмов имеет небольшие отличия от стандартной – мы считаем, что эти изменения сделаны специально, с целью ввести исследователей в заблуждение. Внутренняя конфигурация вредоносной программы зашифрована, сжата и сериализована как сложная реестрообразная структура, которая имеет разные типы записей, включая строковые, целочисленные и внутренние ссылки. Краденные данные, загружаемые на командный сервер, разбиваются на маленькие кусочки (около 3 КБ), которые затем сжимаются, шифруются и помещаются в контейнер для загрузки на сервер. Если исходный файл достаточно велик, то он может быть помещен в несколько сотен разных контейнеров, которые выгружаются независимо. Потом, по всей вероятности, кусочки данных собираются, расшифровываются, распаковываются и собираются на стороне атакующего. Создание такого сложного хранилища может показаться излишним, однако все эти уровни дополнительной обработки гарантируют, что очень немногие исследователи смогут добраться до оригинальных данных. Кроме того, такой метод обеспечивает достаточно надежную защиту от сетевых ошибок.

В июле мы опубликовали подробный анализ кампании по проведению целевых атак, которой мы дали название Crouching Yeti. Эта кампания также известна под названием Energetic Bear, поскольку эксперты из CrowdStrike высказали мысль о том, что злоумышленники находятся в России. Мы, со своей стороны, не считаем, что имеется достаточно данных для того, чтобы подтвердить или опровергнуть этот тезис. Эта кампания, активно проводимая с конца 2010 года, до сих пор была нацелена на следующие секторы: энергетика/машиностроение, промышленность, фармацевтика, строительство, образование и информационные технологии. На сегодняшний день число жертв этой кампании превышает 2 800; нам удалось идентифицировать 101 пострадавшую от нее организацию – прежде всего в США, Испании, Японии, Германии, Франции, Италии, Турции, Ирландии, Польше и Китае.

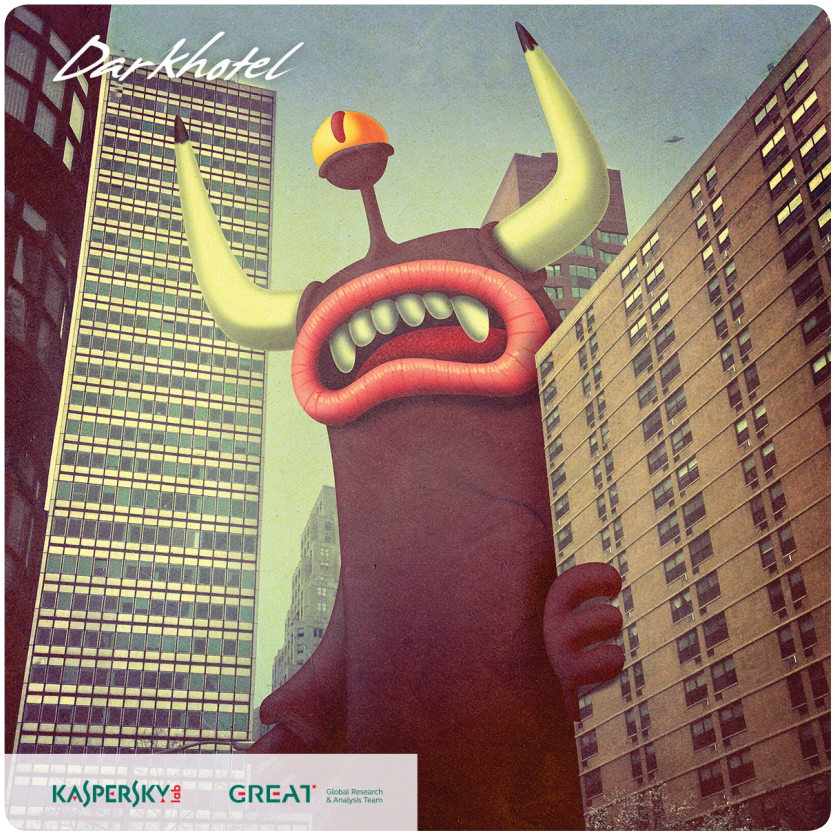
В ходе атак группа Crouching Yeti применяет несколько видов вредоносных программ (все они предназначены для ОС Windows), с помощью которых она заражает компьютеры жертв, расширяет свое присутствие в сетях интересующих ее организаций и крадет конфиденциальные данные, в том числе интеллектуальную собственность и другую важную информацию. Используемая организаторами атак вредоносная программа включает специализированные модули, предназначенные для сбора данных в определенных промышленных IT-средах. Зараженные машины соединяются с большой сетью взломанных сайтов, на которых размещены вредоносные модули и информация о жертвах, и с которых на зараженные компьютеры передаются команды. Для заражения жертв злоумышленники применяют три метода: использование легитимного инсталлятора с внедренной в него вредоносной DLL-библиотекой, адресный фишинг и атаки типа watering hole.

Компьютерные технологии стали неотъемлемой частью нашей жизни, и нет ничего удивительного в том, что у вооруженных конфликтов по всему миру появилось “киберизмерение”. Это особенно верно для Ближнего Востока, где геополитические конфликты стали в последние годы еще более напряженными. В августе мы писали об усилении вредоносной активности в Сирии с начала 2013 года. Жертвы этих атак находятся не только на территории Сирии: соответствующее вредоносное ПО обнаружено также в Турции, Саудовской Аравии, Ливане, Палестине, ОАЭ, Израиле, Марокко, Франции и США. Нам удалось определить IP-адреса

командных серверов киберпреступников, находящихся на территории Сирии, России, Ливана, США и Бразилии. В общей сложности мы обнаружили 110 файлов, 20 доменов и 47 IP-адресов, связанных с этими атаками.

Очевидно, что группы, осуществляющие эти атаки, хорошо организованы. До сих пор атакующие применяли только существующее вредоносное ПО, а не создавали собственный вредоносный код (но при этом они используют различные приемы обфускации для обхода сигнатурных методов обнаружения). По нашему мнению, вероятен дальнейший рост как количества, так и сложности вредоносного ПО, применяемого в регионе.

В ноябре мы опубликовали свой анализ APT-атаки Darkhotel – кампании, продолжающейся уже почти десятилетие и насчитывающей тысячи жертв в разных странах мира. Жертвы 90 процентов известных нам заражений находятся в Японии, на Тайване, в Китае, России и Гонконге, однако случаи заражения были также обнаружены в Германии, США, Индонезии, Индии и Ирландии.



Степень адресности атак в рамках данной кампании варьируется. Во-первых, злоумышленники применяют адресные рассылки электронных писем и эксплойты нулевого дня, чтобы проникнуть в IT-инфраструктуру организаций разных отраслей, в том числе военно-промышленного комплекса (ВПК), государственных и общественных организаций. Во-вторых, они распространяют вредоносное ПО неизбирательно через японские ресурсы P2P-обмена файлами. В-третьих, используя двухэтапный механизм заражения, они осуществляют целевые атаки на руководителей компаний, путешествующих за границей и останавливающихся в гостиницах в определенных странах. На первом этапе атакующие идентифицируют своих жертв. На втором – загружают дополнительное вредоносное ПО на компьютеры наиболее значительных жертв с целью кражи конфиденциальных данных с зараженных компьютеров.

НАШИ ДОМА И ДРУГИЕ УЯЗВИМОСТИ

Эксплуатация неисправленных уязвимостей остается одним из наиболее активно используемых киберпреступниками механизмов установки вредоносного кода на компьютеры жертв. Этот механизм эффективен благодаря наличию уязвимостей в широко используемом программном обеспечении, а также тому, что отдельные пользователи и компании не устанавливают исправления, закрывающие известные уязвимости в приложениях.

В этом году уязвимости были обнаружены в двух широко используемых open source протоколах. Эти уязвимости получили названия Heartbleed и Shellshock, соответственно. Heartbleed – ошибка в протоколе шифрования OpenSSL, позволяющая злоумышленнику читать содержимое памяти и перехватывать личные данные в системах, использующих уязвимые версии протокола. OpenSSL широко используется для защиты данных, передаваемых через интернет (в том числе информации, которой пользователь обменивается с веб-страницами, электронных писем, сообщений в интернет-мессенджерах), и данных, передаваемых по каналам VPN (Virtual Private Networks), поэтому потенциальный ущерб от этой уязвимости был огромным. Как часто бывает при возникновении риска раскрытия личных данных, пользователи в массовом порядке бросились менять пароли. Конечно, эта мера имела смысл, только если провайдер онлайн-сервиса установил необходимое исправление, закрывающее уязвимость в OpenSSL, обеспечив таким образом безопасность своих систем, – в противном случае, новый пароль, каким бы он ни был, подвергался бы такой же опасности со стороны злоумышленников, пытающихся использовать данную уязвимость. Два месяца спустя после обнаружения Heartbleed мы поделились своим видением последствий этой ошибки.

В сентябре в сообществе IT-безопасности был объявлен высший уровень тревоги: была выявлена уязвимость Shellshock (также известная как Bash). Уязвимость позволяет злоумышленнику удаленно прикрепить к переменной вредоносный файл, который выполняется при вызове командного интерпретатора Bash (Bash – это командная оболочка, используемая в Linux и Mac OS X по умолчанию). Очень серьезный характер данной уязвимости в сочетании с тем, что ее исключительно легко эксплуатировать, вызвал серьезную озабоченность. Некоторые сравнивали ее с уязвимостью Heartbleed. Однако в отличие от нее, ShellShock обеспечивал полный контроль над системой, а не только возможность красть данные из памяти уязвимого компьютера. Злоумышленники недолго думали, как использовать эту уязвимость – мы

уже разбирали первые случаи ее эксплуатации вскоре после обнаружения. В большинстве случаев злоумышленники удаленно атаковали веб-серверы, на которых размещены CGI-скрипты, написанные в Bash или передающие значения скриптам оболочки. Однако может оказаться, что уязвимость может влиять и на инфраструктуру, основанную на Windows. К сожалению, проблема не ограничивается веб-серверами. Bash широко применяется в прошивках популярных устройств, которые мы привыкли использовать каждый день: маршрутизаторов, домашних устройств, беспроводных точек доступа и т.д. Некоторые из них может быть сложно или даже невозможно перепрошить.

Мы все теснее связаны с интернетом – иногда в буквальном смысле: возможность соединения с Сетью реализована во многих бытовые устройствах. Эта тенденция, известная под названием «интернет вещей», в последнее время привлекает все больше внимания. Иногда «интернет вещей» может показаться чем-то далеким, не имеющим отношения к реальной жизни. Однако он ближе, чем бы думаем. Очень вероятно, что в современном доме вы найдете несколько устройств, подключенных к локальной сети, и это будут не только традиционные компьютеры, планшеты и сотовые телефоны, но и такие устройства, как Smart TV, принтер, игровая консоль, сетевой накопитель, медиаплеер или спутниковый ресивер.

Один из наших экспертов по IT-безопасности – Дэвид Джэкоби – исследовал свой собственный дом на предмет его кибербезопасности. Он проанализировал несколько устройств – сетевые накопители (NAS), Smart TV, маршрутизатор и спутниковый ресивер – и проверил, насколько они уязвимы при атаке. Результаты оказались ошеломляющими. Дэвид

нашел 14 уязвимостей в сетевых накопителях, подключенных к сети, одну уязвимость в Smart TV и несколько скрытых функций в маршрутизаторе, которые можно использовать для удаленного контроля над устройством. Подробную информацию о проведенном Дэвидом исследовании можно найти здесь.

Всем нам важно понимать потенциальный риск, связанный с использованием сетевых устройств, – он актуален и для частных пользователей, и для компаний. Нужно также иметь в виду, что сильные пароли и ПО, защищающее от вредоносных программ, еще не гарантируют полной безопасности личной информации. Есть много вещей, которые мы не контролируем; в определенном смысле, мы находимся в руках производителей устройств и разработчиков ПО. К примеру, не во всех устройствах есть автоматическая проверка на наличие обновлений, и пользователи сами должны скачивать новые версии прошивки и устанавливать их, а это не всегда просто. Еще хуже то, что не всегда возможно обновить устройство: во время исследования оказалось, что поддержка большей части исследованных устройств прекращена более чем за год до проведения исследования.

ПРОДОЛЖАЮЩИЙСЯ ЭКСПОНЕНЦИАЛЬНЫЙ РОСТ КОЛИЧЕСТВА МОБИЛЬНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

В последние годы мы столкнулись со значительным ростом количества мобильных вредоносных программ. В течение периода с 2004 по 2013 год мы проанализировали почти 200 000 образцов мобильного вредоносного кода. При этом в одном только 2014 году число проанализированных образцов составило 295 539. Но это еще не вся картина. Эти образцы кода перепаковываются и вновь используются: в 2014 году мы обнаружили 4 643 582 установочных пакета мобильного вредоносного кода (в дополнение к 10 000 000 установочных пакетов, обнаруженных в 2004-13 годах). Среднемесячное число атак с использованием мобильного вредоносного ПО выросло на порядок – с 69 000 атак в месяц в августе 2013 года до 644 000 в марте 2014 года (см. Исследование «Лаборатории Касперского» и ИНТЕРПОЛа: Мобильные киберугрозы, октябрь 2014 г.).

На долю вредоносных программ, способных к краже денежных средств, сейчас приходится 53% всех обнаружений мобильного вредоносного ПО. Один из наиболее заметных примеров – программа Svpeng, предназначенная для кражи средств у клиентов трех крупнейших российских банков. Троянец дожидается, пока пользователь откроет окно приложения для онлайн-банкинга и заменяет его своим с целью выудить у жертвы необходимые для авторизации логин и пароль. Кроме того, он пытается украсть данные банковской карты – для этого он перекрывает приложение Google Play своим окном, в котором запрашивает реквизиты карты. Еще один пример – вредоносная программа Waller, которая, в дополнение к поведению, характерному для SMS-троянца, крадет средства из электронных кошельков QIWI на зараженных устройствах.

Киберпреступники также используют все более разнообразные способы «зарабатывания» денег на своих жертвах, беря на вооружение приемы, хорошо зарекомендовавшие себя на персональных компьютерах. Это относится, в частности, к троянцам-вымогателям. Фальшивые антивирусы – еще один пример переноса традиционного подхода на мобильные устройства. И, наконец, в этом году появился первый троянец, командный сервер которого размещен в сети Tor. Бэкдор Torec представляет собой измененную версию популярного Tor-клиент Orbot. Преимущество такого командного сервера для злоумышленников, конечно же, состоит в том, что его невозможно закрыть.

До недавнего времени почти все вредоносное ПО, предназначенное для iOS, было рассчитано на устройства, подвергшиеся «джейлбрейку». Однако появившаяся недавно вредоносная программа WireLurker продемонстрировала, что iOS неспособна обеспечить полную защиту от вредоносных атак.

Мобильные устройства стали неотъемлемой частью нашей жизни, и неудивительно, что создание мобильного вредоносного ПО – это киберпреступный бизнес, в который вовлечены разработчики вредоносных программ, специалисты по тестированию, разработчики приложений, веб-разработчики и операторы ботнетов.

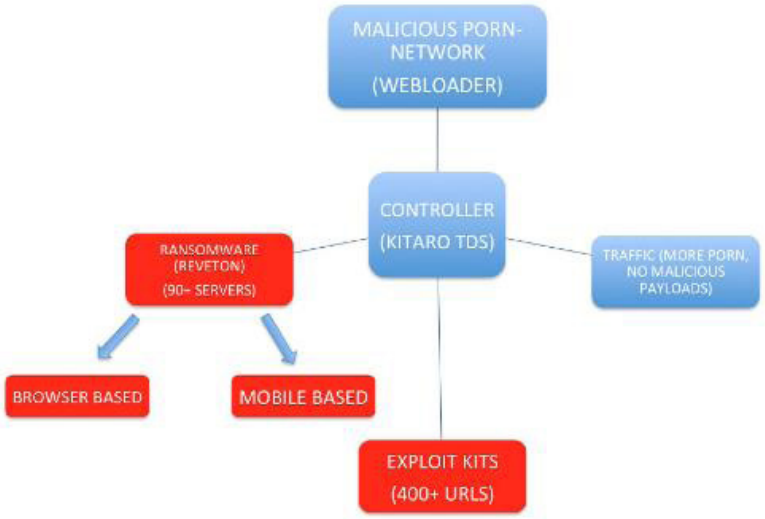
КОШЕЛЕК ИЛИ ФАЙЛ(Ы)

Число программ-вымогателей в последние годы быстро росло. Некоторые из них просто блокируют доступ к компьютеру жертвы и требуют выкуп за восстановление нормального доступа к нему. Но многие программы-вымогатели идут дальше и шифруют данные на компьютере. Недавний пример – вымогатель ZeroLocker. Он шифрует почти все виды файлов на компьютере-жертве и добавляет к зашифрованным файлам расширение .encrypt (при этом он не шифрует файлы, находящиеся в папках, названия которых содержат слова Windows, WINDOWS, Program Files, ZeroLocker и Destroy, а также файлы размером более 20 Мб). Троянец использует для шифрования файлов 160-битный AES-ключ. После шифрования файлов зловред запускает утилиту cipher.exe, которая удаляет с диска все неиспользуемые данные. И то, и другое значительно усложняет восстановление файла. За расшифровку файлов киберпреступники, стоящие за ZeroLocker, первоначально требуют сумму в биткойнах, эквивалентную $300. Если жертва затягивает с платежом, сумма вырастает сначала до $500, а затем и до $1000.

Еще одна программа-вымогатель, недавно проанализированная нами, – это Onion. Этот троянец не только использует сеть Tor, чтобы скрыть свои командные серверы, но и способен взаимодействовать с Tor в полном объеме без какого бы то ни было участия пользователя. Другие программы этого типа взаимодействуют с сетью Tor, запуская легитимный файл tor.exe (иногда путем внедрения кода в другие процессы). У Onion, в отличие от них, весь код, необходимый для реализации взаимодействия с анонимной сетью, совмещен с вредоносным кодом. Onion также использует необычный криптографический алгоритм, из-за которого расшифровка файла невозможна, даже если удается перехватить трафик между троянцем и командным сервером. Этот троянец не только использует асимметричное шифрование, но еще и применяет криптографический протокол, известный как протокол Диффи-Хеллмана (Elliptic Curve Diffie-Hellman). Это делает расшифровку невозможной без личного мастер-ключа, который никогда не выходит за пределы сервера, контролируемого киберпреступниками.

В этом году сфера применения вымогателей-блокировщиков расширилась, включив в себя устройства под управлением Android. Например, первая модификация мобильного зловреда Svpeng, обнаруженная в начале 2014 года, блокирует работу телефона якобы за просмотр его владельцем детской порнографии. За разблокировку мобильного телефона злоумышленники требовали уплатить «штраф» в размере 500 долларов. Более поздняя модификация вредоносной программы,

обнаруженная в июне 2014 года, полностью блокирует мобильное устройство, так что его можно отключить только с помощью долгого нажатия кнопки выключения – но троянец стартует сразу же после повторного запуска системы. Эта версия требует заплатить 200 долларов за разблокировку телефона и нацелена преимущественно на пользователей в США, но зловред атаковал также пользователей из Великобритании, Швейцарии, Германии, Индии и России. Для получения денег создатели троянца используют ваучеры MoneyPak. На экране требования выкупа демонстрируется фотография жертвы, сделанная фронтальной камерой. Еще один троянец под названием Koler, обнаруженный в мае 2014 года, использует такой же подход – блокирует доступ к устройству и требует заплатить за разблокирование телефона выкуп от 100 до 300 долларов. Как и Svpeng, этот троянец выводит на экран сообщение от имени «полиции», причем оно локализовано для жителей более чем 30 стран мира.



Инфраструктура распространения Koler

Первый шифрующий пользовательские данные Android-троянец под названием Pletor появился в мае 2014 года. Он шифрует содержимое карты памяти смартфона – медиафайлы и документы – с помощью алгоритма шифрования AES, а затем выводит на экран требование о выкупе. Для получения денег от пользователей используются системы QIWI VISA WALLET, MoneXy или обычный перевод денег на номер телефона. Этот троянец нацелен прежде всего на граждан России и Украины (хотя жертвы есть и в других странах бывшего СССР) и требует выкуп в рублях или гривнах (сумма соответствует приблизительно 300 евро).

Использование троянцев-вымогателей имеет смысл для киберпреступников постольку, поскольку жертвы готовы платить выкуп за разблокирование данных. Не делайте этого! Регулярно сохраняйте резервные копии своих данных – тогда, если вы и столкнетесь с троянцем-вымогателем (или аппаратной ошибкой, которая лишит вас доступа к файлам), вы не потеряете свои данные.

ДЗЫНЬ! ПРИМЕНЕНИЕ ВРЕДОНОСНОГО ПО ДЛЯ ПОЛУЧЕНИЯ ДЕНЕГ ИЗ БАНКОМАТОВ

Вредоносное ПО для банкоматов – не новое явление. Первая подобная вредоносная программа под названием Skimer была обнаружена в 2009 году. Она была нацелена на банкоматы в Восточной Европе, работающие под управлением операционной системы на базе Windows. Киберпреступники использовали недокументированные функции банкомата для получения распечатки реквизитов карт, которые вставлялись в зараженный аппарат, а также для вскрытия кассет с денежными купюрами с помощью специальной карточки доступа. Позже мы столкнулись с использованием вредоносного ПО для банкоматов в 2010 году в Бразилии: вредоносная программа SPSniffer собирала ПИН-коды в устаревших банкоматах, пинпады (панели для ввода ПИН-кода) которых не использовали надежную криптографическую защиту. А в прошлом году мы анализировали еще одно семейство вредоносных программ для банкоматов (Atmer), предназначенное для кражи денег из банкоматов в Мексике.

В этом году по просьбе одной финансовой организации мы провели криминалистическое расследование новой атаки киберпреступников, направленной против банкоматов в Азии, Европе и Латинской Америке. Преступники проводят операцию в два этапа. Сначала они получают физический доступ к банкомату и устанавливают с загрузочного компакт-диска вредоносную программу, получившую название Tyupkin; затем они перезагружают банкомат, чтобы загрузить вредоносную программу, которая позволяет им управлять работой банкомата. После этого вредоносная программа запускает бесконечный цикл ожидания пользовательского ввода.

Чтобы усложнить обнаружение, Tyupkin принимает команды только в определенное время ночью в воскресенье и понедельник. В это время участники атаки могут ввести на клавиатуре банкомата комбинацию цифр, связаться по телефону с оператором вредоносного ПО, ввести еще один набор цифр и забрать деньги, выданные банкоматом в результате этих манипуляций.

Видеоматериалы с камер наблюдения, установленных в местах размещения зараженных банкоматов, позволили определить, каким образом преступники извлекали из них денежные средства. Для каждой сессии создается уникальный ключ – комбинация цифр, генерируемая из случайного числа. Это позволяет гарантировать, что те, кто не входит в данную преступную группировку, не смогут случайно присвоить плоды реализации мошеннической схемы. Затем оператор вредоносной программы получает по телефону инструкции от другого члена банды, знающего алгоритм, позволяющий сгенерировать сессионный ключ из показанного на экране числа. Это позволяет предотвратить попытки «денежных мулов», забирающих купюры из банкомата, совершить самостоятельный набег. После ввода верного ключа банкомат показывает количество средств, доступное в каждой кассете, предлагая оператору выбрать, из какой кассеты будут украденыденьги. Далее банкомат выдает 40 банкнот из выбранной кассеты.

Рост числа атак на банкоматы в последние годы – естественное развитие более распространенного метода кражи средств, основанного на физической установке скиммеров для считывания данных с карт, вставляемых в банкоматы. К сожалению, многие банкоматы работают под управлением операционных систем, имеющих известные бреши в защите, что делает физическую защиту таких устройств крайне важной. Мы призываем все банки пересмотреть меры физической защиты своих банкоматов.

WINDOWS XP: ЗАБЫТ, НО НЕ ИСЧЕЗ?

Поддержка Windows XP прекращена с 8 апреля. Это означает, что больше не выпускается никаких обновлений и исправлений безопасности; более недоступны никакие варианты техподдержки – ни платные, ни бесплатные; нет онлайн-обновлений технического контента. Увы, но при этом пользователей Windows XP еще достаточно много: по нашим данным, на Windows XP приходится около 18% случаев заражений. Получается, что прекращение обновлений безопасности оставило большое количество пользователей абсолютно беззащитными перед атаками. По сути, все уязвимости, обнаруженные начиная с апреля, относятся к классу zero-day, т.е. исправлений для них нет и не будет. Положение осложнится, когда производители приложений перестанут выпускать обновления к версиям программ под Windows XP. Каждое непропатченное приложение станет еще одной уязвимой точкой, расширяющей возможности для успешной атаки. Этот процесс уже фактически начался: последняя версия Java уже не поддерживает Windows XP.

Может показаться, что простым и очевидным решением было бы обновиться до более новой версии Windows. Но хотя компания Microsoft заблаговременно и неоднократно предупреждала об окончании поддержки Windows XP, нетрудно понять, почему для некоторых компаний миграция на новую операционную систему может представлять сложность: вдобавок к затратам на собственно миграцию, могут понадобиться инвестиции в новое аппаратное обеспечение и даже замена специализированных приложений, разработанных на заказ, поскольку они не будут работать под более новой операционной системой. С учетом всего этого неудивительно, что некоторые организации платят за продолжение поддержки XP.

Естественно, антивирус обеспечит защиту. Однако это справедливо, только если под «антивирусом» мы имеем в виду комплексный продукт класса Internet security, который при помощи проактивных технологий защищает от новых, неизвестных угроз, в частности предотвращает эксплуатацию уязвимостей. Базового антивирусного продукта, работа которого преимущественно основана на проверке известного вредоносного ПО по базам сигнатур угроз, будет недостаточно. Также необходимо помнить, что со временем производители защитных решений будут внедрять в свои продукты новые технологии, которые могут оказаться несовместимыми с Windows XP.

Все пользователи, по-прежнему использующие Windows XP, должны относиться к этому лишь как к временной мере и планировать стратегию миграции. Без сомнения, Windows XP, пока его использует достаточно много пользователей, будет привлекать создателей вредоносного ПО, поскольку операционная система, для которой более не выпускается обновлений безопасности, даст им гораздо больше возможностей нагреть руки. Любой компьютер в корпоративной сети, работающий под Window XP, представляет собой «слабое звено» системы безопасности и может быть использован для проведения целевой атаки на компанию; в случае взлома такой компьютер становится плацдармом для дальнейшего проникновения злоумышленников в корпоративную сеть.

Без сомнения, миграция на новую операционную систему – дело дорогостоящее и неудобное как для индивидуальных пользователей, так и для организаций. Однако потенциальный риск от использования небезопасной операционной системы перевешивает такие соображения, как финансовые затраты и неудобства.

ЧТО СКРЫВАЕТСЯ ПОД СЛОЯМИ ЛУКОВИЦЫ

Tor (сокращение от The Onion Router, «луковый маршрутизатор») – это программный продукт, разработанный для сохранения анонимности пользователей при посещении интернета. Tor существует уже довольно долго, но много лет использовался в основном специалистами и энтузиастами. Однако в этом году популярность сети Tor резко возросла, в основном из-за того, что пользователи стали больше задумываться о конфиденциальности. Tor стал полезным решением для тех, кто по каким-либо причинам боится слежки или утечек конфиденциальной информации. Наши исследования выявили, что сеть Tor также привлекательна для киберпреступников – последние по достоинству оценили анонимность, которую она предоставляет.

В 2013 г. мы впервые заметили, что киберпреступники стали активно использовать Tor для размещения своей вредоносной инфраструктуры. Кроме собственно вредоносных программ, мы также обнаружили много других сопутствующих ресурсов – командных серверов, панелей управления и пр. Размещая свои серверы в сети Tor, киберпреступники усложняют их распознавание, помещение в черный список и ликвидацию. Также существует черный рынок на базе Tor – на нем, помимо прочего, торгуют вредоносными программами и краденными личными данными. Расплачиваются обычно биткоинами, благодаря чему киберпреступников нельзя выследить. Таким образом, Tor позволяет злоумышленникам обеспечить скрытную работу своих вредоносных программ, осуществлять торговлю услугами и отмывать нелегальные доходы.

В июле был опубликован наш анализ троянца-вымогателя, получившего название Onion («лук») и положившего начало принципиально новому использованию Tor.

Разработчики вредоносных программ для Android также начали использовать Tor. Троянец Torec – вредоносная модификация популярного Tor-клиента Orbot, использует домен в псвевдозоне .onion в качестве командного сервера. Некоторые разновидности троянца-вымогателя Pletor также используют сеть Tor для обмена данными с киберпреступниками.

И все же киберпреступникам не всегда удается безнаказанно проворачивать свои дела, даже если они используют Tor. Это продемонстрировала недавняя международная операция правоохранительных органов, направленная против ряда киберпреступных сервисов на основе Tor (‘Operation Onymous’).

Встает вопрос: как проводившим операцию правоохранительным органам удалось взломать сеть, которая считается «непробиваемой»? Ведь, по крайней мере в теории, выяснить физическое местонахождение веб-сервера, на котором размещен посещаемый пользователем скрытый сервис, должно быть невозможно. На практике же оказывается, что существуют способы взлома скрытого сервиса, не требующие атаки на архитектуру самой сети Tor – см. наше обсуждение здесь. Сервис на основе Tor может быть полноценно защищенным, только если он должным образом сконфигурирован, не содержит уязвимостей и ошибок конфигурации, а веб-приложение также не имеет слабых мест.

ХОРОШИЙ, ПЛОХОЙ, ЗЛОЙ

К сожалению, программы не всегда можно четко разделить на хорошие и плохие. Всегда существует риск того, что программы, разработанные в легитимных целях, могут злонамеренно использоваться киберпреступниками. На Kaspersky Security Analyst Summit 2014, который прошел в феврале, специалисты обсуждали, как некорректно реализованные технологии для защиты от кражи в прошивке популярных моделей ноутбуков и некоторых стационарных компьютеров могут стать грозным оружием в руках киберпреступников. Поводом для исследования послужили неоднократные аварийные завершения системных процессов на личном ноутбуке сотрудника «Лаборатории Касперского», связанные с нестабильной работой модулей программного продукта Computrace разработчика Absolute Software.

Наш коллега этот программный продукт не устанавливал и даже не знал, что он присутствует на ноутбуке. Это нас обеспокоило: согласно техническому описанию производителя (Absolute Software), установка программы должна производиться владельцем компьютера или соответствующей IT-службой. К тому же, в то время как владелец компьютера, как правило, может необратимо удалить или заблокировать большинство предустановленных программ, Computrace разработан так, что сохраняется после профессиональной очистки системы и даже после замены жесткого диска. Более того, мы не могли проигнорировать этот случай как единичный, потому что мы обнаружили следы активности Computrace на компьютерах других наших аналитиков и на некоторых корпоративных компьютерах. В результате мы решили провести глубинный анализ программы.

При первом рассмотрении мы ошибочно решили, что Computrace представляет собой вредоносную программу, поскольку в нем использовались многие приемы и уловки, популярные в современном вредоносном ПО. Действительно, в прошлом Computrace детектировался как вредоносная программа, хотя в настоящее время большинство производителей защитных решений включают исполняемые файлы Computrace в белые списки.

Мы полагаем, что Computrace был разработан с благими намерениями; однако наше исследование показало, что в данном ПО имеются уязвимости, позволяющие киберпреступникам использовать его в неблаговидных целях. Мы не обнаружили никаких свидетельств того, что модули Computrace на проанализированных нами компьютерах были активированы тайно. С другой стороны, очевидно, что агенты Computrace

активны на большом количестве компьютеров. На наш взгляд, производители техники и Absolute Software должны уведомить владельцев таких компьютеров и объяснить им, как деактивировать эту программу, если они не захотят ее использовать. В противном случае, эти «беспризорные» агенты будут продолжать незаметно работать на компьютерах пользователей, делая их уязвимыми для атак киберпреступников.

В июне мы опубликовали результаты исследования «легальной» шпионской программы Remote Control System (RCS), разработанной итальянской компанией HackingTeam. Мы обнаружили характерный признак, позволяющий отслеживать ее командные серверы, что позволило нам просканировать все пространство IPv4 и выявить IP-адреса всех командных серверов RCS. Всего их обнаружилось 326; большинство были размещены в США, Казахстане и Эквадоре. Для некоторых IP-адресов на основе информации WHOIS было установлено, что они имеют отношение к государственным организациям. Конечно, мы не можем быть уверены, что серверы, расположенные в определенной стране, используются соответствующими спецслужбами той же страны, однако это было бы логично, так как позволило бы избежать юридических проблем с другими странами и риска изъятия серверов. Мы также обнаружили некоторое количество модулей мобильных вредоносных программ производства HackingTeam для Android, iOS, Windows Mobile и BlackBerry. Все они управляются при помощи сходных файлов конфигурации, что как правило свидетельствует о принадлежности к одному семейству. Разумеется, мы в первую очередь заинтересовались модулями для самых популярных мобильных платформ – Android и iOS.

Модули устанавливаются при помощи инфекторов – специальных исполняемых программ для Windows или Mac OS, которые запускаются на уже зараженных компьютерах. Модуль для iOS работает только на устройствах, подвергшихся джейлбрейкингу. Это ограничивает возможности зловреда по распространению, но используемый RCS метод заражения означает, что атакующая сторона может запустить утилиту для джейлбрейкинга (такую как Evasi0n) с зараженного компьютера, к которому подключен телефон, если только устройство не заблокировано. Модуль для iOS позволяет атакующей стороне получить доступ к данным, хранящимся на устройстве (в т.ч. к электронной почте, списку контактов, истории звонков, веб-страницам в кэше), незаметно включить микрофон и делать регулярные снимки камерой. Это позволяет злоумышленникам получить полный контроль над всей средой – как внутри, так и вокруг компьютера жертвы.

Модуль для Android защищен оптимизатором/обфускатором Dexguard, так что его анализ был затруднен. Тем не менее, мы смогли определить, что его функциональность соответствует таковой модуля для iOS, а также поддерживает перехват данных от следующих приложений: com.tencent.mm, com.google.android.gm, android.calendar, com.facebook, jp.naver.line.android и com.google.android.talk.

Эти новые данные показывают, насколько продвинуты такие инструменты наблюдения. Мы придерживаемся в их отношении однозначной политики: мы стараемся обнаружить и нейтрализовать любую вредоносную атаку, независимо от ее источника и целей. Для нас не существует таких понятий, как «правильное» и «неправильное» вредоносное ПО. В прошлом мы уже выпускали публичные предупреждения о рисках, связанных с так называемыми «легальными» шпионскими программами. Абсолютно недопустимо, чтобы такие инструменты наблюдения попали в руки злоумышленников; именно поэтому индустрия IT-безопасности не может делать исключения, когда речь идет о детектировании вредоносного ПО.

КОНФИДЕНЦИАЛЬНОСТЬ И БЕЗОПАСНОСТЬ

Противоречия между конфиденциальностью личных данных и соображениями безопасности продолжают широко обсуждаться в прессе.

Не вызывает большого удивления то, что в этом году среди обычного потока публикаций о компьютерных взломах и утечках конфиденциальных данных наибольший шум вызвала кража и последующая публикация откровенных фотографий голливудских знаменитостей. Эта история иллюстрирует совместную ответственность сервис-провайдеров и индивидуальных пользователей за обеспечение безопасности данных, хранимых онлайн. Похоже, что кража стала возможной из-за бреши в системе безопасности iCloud: интерфейс функции 'Find My iPhone' («найти мой айфон») не предусматривал ограничения количества попыток ввода пароля, что позволяло злоумышленникам взламывать пароли к устройствам жертв методом простого перебора. Вскоре после этого инцидента Apple закрыла эту брешь. Однако эта атака не была бы успешной, если бы жертвы не использовали слабые пароли. Мы проводим онлайн все большую часть своей жизни, однако многие не задумываются, какие последствия может иметь хранение личных данных в онлайн-сервисах. Безопасность облачного сервиса зависит от провайдера. Как только мы доверяем свои данные какому-либо стороннему ресурсу, мы теряем часть контроля над ним. Важно тщательно отбирать те данные, которые мы храним в облаке, и четко определять, какие данные автоматически копируются в облако с наших устройств.

В целом, тема паролей всплывает регулярно. Если мы выбираем пароль, который легко угадать, то мы рискуем стать жертвой кражи личных данных. Проблема усугубляется в случае, если один и тот же пароль используется в разных учетных записях онлайн – в этом случае при взломе одного аккаунта под угрозой оказываются все остальные. По этой причине многие сервис-провайдеры, в том числе Apple, Google и Microsoft, теперь предлагают двухфакторную аутентификацию – для доступа на сайт или для внесения изменений в настойки учетной записи от пользователя требуется ввести код, сгенерированный аппаратным ключом или присланный на мобильное устройство. Двухфакторная аутентификация действительно усиливает безопасность, но только в том случае, если она требуется в обязательном порядке, а не предлагается в виде опции.

Всегда необходим компромисс между уровнем безопасности и удобством использования. Twitter, стремясь достичь этого баланса, недавно запустил сервис Digits. Пользователям более не нужно создавать соче-

тание «имя пользователя + пароль», чтобы авторизоваться в приложении. Вместо этого они просто вводят номер телефона. Каждый раз при совершении транзакции пользователь получает одноразовый секретный код для ее подтверждения – этот код автоматически считывается приложением. Twitter фактически делает себя посредником, идентифицируя пользователя для провайдера приложения. Такая схема имеет сразу несколько преимуществ. Пользователям не нужно беспокоиться о создании комбинации «логин – пароль», чтобы создать учетную запись у провайдера приложения; им также не нужно иметь адрес электронной почты. Разработчикам приложений не нужно создавать собственную инфраструктуру для аутентификации пользователей; они также не теряют потенциальных клиентов, не использующих электронную почту.

Twitter получает больше информации о том, что интересует его пользователей. Дополнительным плюсом является то, что пароли не хранятся на сервере провайдера приложения: взлом его сервера не приведет к потере личных данных пользователей. Однако в случае кражи или утери пользовательского устройства аутентификация по номеру будет по-прежнему работать, и любой человек, получивший доступ к устройству, сможет получить и доступ к приложению – тем же способом, что и законный владелец устройства.

При всем этом, такой подход не является шагом назад с точки зрения безопасности по сравнению с традиционной аутентификацией с помощью логина и пароля. В любом случае, мобильные приложения пока не требуют авторизации при каждом запуске, так что при краже устройства, владелец которого не использует PIN-код, секретный код или идентификацию по отпечаткам пальцев, похититель получает доступ ко всему: к электронной почте, социальным сетям и приложениям. Другими словами, безопасность зависит от самого слабого звена – PIN-кода, секретного кода или отпечатков пальцев, используемых для получения физического доступа к устройству.

Реагируя на растущую озабоченность конфиденциальностью личных данных, разработчики веб-сайта pwnedlist.com создали простой в использовании интерфейс, позволяющий пользователям проверить, не были ли их почтовые адреса и пароли украдены и опубликованы в сети. В этом году эта услуга была преобразована в платный сервис.

В свою очередь, Apple и Google теперь предлагают шифрование данных по умолчанию на iOS и Android-устройствах. Некоторые представители правоохранительных органов утверждают, что такая практика играет на руку киберпреступникам, затрудняя их обнаружение.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПРИНОСИТ ПЛОДЫ

Киберпреступления являются оборотной стороной постоянно растущей активности пользователей в Сети и давно уже стали частью нашей повседневной жизни. Может показаться, что деятельность киберпреступников зачастую остается безнаказанной, однако на самом деле действия правоохранительных органов значительно осложняют им жизнь. Учитывая глобальную природу киберпреступности, в борьбе с ней особенно важно международное сотрудничество. В этом году было несколько случаев, когда правоохранительные органы достигли значимого успеха в противодействии киберпреступникам.

В июне 2014 г. прошла операция с участием правоохранительных органов нескольких стран, в т.ч. британского Национального Агентства по борьбе с киберпреступностью (National Crime Agency) и ФБР, в результате которой удалось прекратить деятельность глобальной сети компьютеров, управляющей ботнетом GameoverZeus. Операция правоохранительных органов («Операция Tovar») нарушила коммуникацию между ботами и командными серверами ботнета, лишив кибепреступников контроля над ним. GameoverZeus был одним из крупнейших действующих ботнетов, использующих код банковского троянца Zeus. Кроме заражения компьютеров троянцем Zeus и кражи учетных данных от почтовых ящиков, соцсетей, онлайн-банкинга и других финансовых онлайн-сервисов, ботнет также распространял программу-вымогатель Cryptolocker. Благодаря операции правоохранительных органов, пострадавшие пользователи получили шанс передохнуть и почистить свои компьютеры от зловредов.

В этом году «Лаборатория Касперского» внесла свой вклад в совместную операцию правоохранительных органов и представителей индустрии кибербезопасности, координируемую британским Национальным Агентством по борьбе с киберпреступностью (NCA), в ходе которой была прекращена работа инфраструктуры троянца Shylock. Банковский троянец Shylock был обнаружен в 2011 г. и получил свое название из-за того, что его код содержит фрагменты из «Венецианского купца» Шекспира. Подобно другим известным банковским троянцам, Shylock представляет собой образец атаки типа Man-in-the-Browser (MITB) и создан для кражи учетных данных для банкинга с компьютеров клиентов банков. Троянец использует заранее заданный список банков-мишеней из разных стран.

В результате операции Onymous, проведенной в ноябре, были ликвидированы черные рынки, действовавшие в сети Tor.

APT-УГРОЗЫ: ВЗГЛЯД В МАГИЧЕСКИЙ КРИСТАЛЛ

В последние годы Центр глобальных исследований и анализа угроз «Лаборатории Касперского» (GReAT) пролил свет на некоторые из крупнейших кампаний APT-класса, в том числе RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/Mask и др. В процессе их изучения мы обнаружили несколько эксплойтов нулевого дня, включая последний по времени – CVE-2014-0546. Мы также были среди первых, кто сообщил о новых тенденциях в области APT-угроз, таких как появление кибернаемников, готовых оказывать услуги по проведению «молниеносных» атак, или, относительно недавно, использование необычных векторов атаки, таких как Wi-Fi сети в отелях. В последние годы Центр глобальных исследований и анализа угроз «Лаборатории Касперского» отслеживал деятельность более 60 преступных групп, ответственных за кибератаки, проводимые по всему миру. Их участники говорят на разных языках: русском, китайском, немецком, испанском, арабском, персидском и других.

Скрупулезное наблюдение за деятельностью этих преступных групп позволило нам составить список, отражающий, как мы считаем, нарождающиеся угрозы APT-класса. По нашему мнению, эти угрозы будут играть важную роль в 2015 году и заслуживают особого внимания – как в плане изучения, так и с целью создания технологий для их нейтрализации.

Костин Раю

СЛИЯНИЕ КИБЕРПРЕСТУПНОСТИ И APT-УГРОЗ

В течение многих лет усилия киберпреступных групп были направлены только на кражу денег у конечных пользователей. Взрывной рост активности, связанной с кражей кредитных карт, взломом учетных записей в системах электронных платежей и перехватом соединений с системами онлайн-банкинга, привел к потере пользователями сотен миллионов долларов. Возможно, этот рынок стал менее прибыльным, или киберпреступников на нем стало слишком много, но нынешняя обстановка очень похожа на борьбу за «выживание». Как всегда, подобная борьба приводит к развитию.

Чего ожидать: в ходе инцидента, который мы недавно расследовали, злоумышленники взломали компьютер бухгалтера и запустили с этого компьютера крупный денежный перевод в свой банк. Несмотря на то, что, на первый взгляд, тут нет ничего особенного или необычного, мы считаем это проявлением новой интересной тенденции к **проведению целевых атак против самих банков, а не их клиентов**.

В нескольких инцидентах, которые расследовали эксперты Центра глобальных исследований и анализа угроз «Лаборатории Касперского», IT-системы банков были взломаны с помощью методов, как будто бы взятых из учебника по проведению атак APT-класса. Получив доступ к сети банка, злоумышленники собирали достаточно информации для того, чтобы красть средства непосредственно у банка, используя при этом несколько методов:

- Давая банкоматам удаленные команды на выдачу наличных
- Выполняя переводы через систему SWIFT со счетов клиентов банков
- Манипулируя системами онлайн-банкинга для выполнения денежных переводов без ведома пользователей.

Эти атаки свидетельствуют о появлении новой тенденции – использовании киберпреступниками методов, характерных для атак APT-класса. Как обычно, злоумышленники стремятся все упростить: теперь они напрямую атакуют банки, потому что деньги есть именно у них. Мы считаем, что на эту тенденцию следует обратить внимание, потому что она получит значительное развитие в 2015 году.

2

ФРАГМЕНТАЦИЯ КРУПНЫХ APT-ГРУППИРОВОК

В 2014 году несколько источников опубликовали информацию об APT-группировках. Вероятно, самое нашумевшее дело – это предъявление Федеральным бюро расследований США обвинений в различных компьютерных преступлениях пяти хакерам:

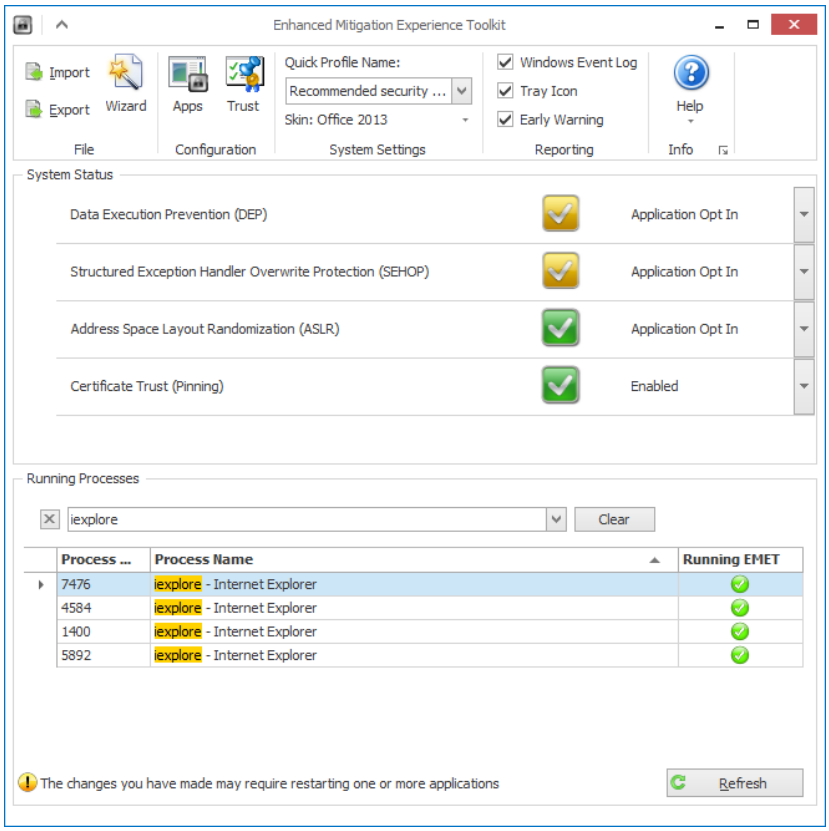
Мы ожидаем, что в результате такой публичности некоторые из наиболее крупных и известных APT-группировок распадутся на более мелкие группы, действующие независимо друг от друга.

Чего ожидать: результатом станут атаки по более широкому фронту. Соответственно, пострадает большее число компаний, поскольку атаки более мелких групп будут более диверсифицированными. В то же время большие компании, взломом сетей которых до сих пор занимались две-три крупные APT-группировки (например, Comments Crew и Wekby), теперь будут вынуждены защищаться от атак, исходящих из гораздо более широкого круга источников.

3

РАЗВИТИЕ ВРЕДОНОСНЫХ МЕТОДОВ И ПРИЕМОВ

По мере роста сложности и мощности современных компьютеров операционные системы также усложняются. Корпорации Apple и Microsoft потратили много времени и усилий на повышение безопасности своих операционных систем. Кроме того, теперь есть специальные средства, такие как EMET от Microsoft, помогающие защититься от целевых атак, направленных на уязвимости в ПО.



Мы ожидаем, что с ростом популярности Windows x64 и Apple Yosemite APT-группировки обновят свой инструментарий, включив в него более мощные бэкдоры и технологии, созданные для обхода защитных решений.

Чего ожидать: уже сейчас APT-группировки постоянно применяют вредоносное ПО для 64-разрядных систем, в том числе 64-разрядные руткиты. В 2015 году мы ожидаем появления более сложных внедряемых вредоносных модулей, усовершенствованных методов обхода защиты и более активного использования виртуальных файловых систем (в качестве примеров можно привести кампании Turla и Regin) для сокрытия ценного инструментария и украденных данных.

Одновременно с наблюдаемой нами тенденцией к широкому применению сложных приемов и методов, некоторые злоумышленники движутся в противоположном направлении. Они стараются свести к минимуму общее число эксплойтов и количество скомпилированного кода, загружаемого во взломанные сети. Однако при взломе инфраструктуры предприятий им тоже необходим сложный код или эксплойты, разнообразные скрипты и инструменты для повышения привилегий в системе, а также украденные у представителей организации логины и пароли доступа.

Как мы видели в случае BlackEnergy 2 (BE2), в случае обнаружения злоумышленники активно защищают свое присутствие во взломанных сетях, а также данные, по которым их можно было бы идентифицировать. Методы, применяемые киберпреступниками для закрепления в инфраструктуре жертв, становятся все более изощренными и агрессивными. APT-группировки, о которых мы писали выше, наращивают объем и активность деструктивных компонентов, применяемых в попытке замести следы. Кроме того, все чаще встречается поддержка Unix-подобных операционных систем, сетевого оборудования и встроенных ОС. Мы уже столкнулись с подобным «широким» подходом со стороны киберпреступников, стоящих за такими угрозами, как BE2, Yeti и Winnti.

НОВЫЕ МЕТОДЫ ПЕРЕДАЧИ КРАДЕНЫХ ДАННЫХ

Давно прошли те времена, когда злоумышленники могли просто установить бэкдор в корпоративной сети и начать загружать терабайты данных на разбросанные по всему миру FTP-серверы. Сегодня продвинутые группировки регулярно используют SSL, а также нестандартные протоколы передачи данных.

Некоторые из наиболее изощренных в технологическом плане групп предпочитают устанавливать бэкдоры в сетевые устройства и перехватывать трафик с них, отправляя данные непосредственно на командные серверы. Кроме того, мы сталкивались с передачей данных в облачные сервисы – например, с использованием протокола WebDAV (применяемого для упрощения совместной работы пользователей, связанной с редактированием и управлением документами, размещенными на веб-серверах).

В результате многие крупные компании запретили доступ к публичным облачным сервисам, таким как Dropbox, из своих сетей. Тем не менее, это остается эффективным способом обхода систем обнаружения вторжений и фильтров DNSBL.

Чего ожидать: в 2015 году еще ряд группировок включат в свой арсенал использование облачных сервисов, что позволит им более эффективно скрывать отправку данных, украденных у жертв.

5

НОВЫЕ APT-КАМПАНИИ ИЗ НЕОЖИДАННЫХ ИСТОЧНИКОВ: К ГОНКЕ КИБЕРВООРУЖЕНИЙ ПРИСОЕДИНЯЮТСЯ НОВЫЕ СТРАНЫ

В феврале 2014 года мы опубликовали отчет об исследовании Careto/«Маски» – чрезвычайно сложной кампании. Ее организаторы, по-видимому, хорошо владеют испанским языком, который редко встречается в целевых атаках. В августе мы также опубликовали результаты анализа Machete – еще одной кампании, в которой использовался испанский язык.

До этого момента мы, как правило, сталкивались с APT-кампаниями и киберпреступниками, владевшими относительно немногими языками. Кроме того, многие профессиональные киберпреступники не пишут на родном языке, а предпочитают изъясняться на прекрасном английском.

В 2014 году мы столкнулись с тем, что несколько стран публично выразили заинтересованность в обладании возможностями по проведению атак APT-класса:


SDA
SECURITY & DEFENCE AGENDA
A NEUTRAL PLATFORM FOR DISCUSSING DEFENCE AND SECURITY POLICIES
HOME POLICY AREAS ACTIVITIES LIBRARY PARTNERS MEMBERSHIP SECURITY JAM CYBER INITIATIVE
SWEDES WANT OFFENSIVE CYBER CAPABILITIES
18/10/2013
The Swedish armed forces want to attack other countries' computer networks, if need be. In a recent report, the armed forces stress the need to go on the offensive as part of its cyber defences.
The report notes that several countries already have or are currently developing a cyber defence that can also to launch cyber strikes. The conclusion of the report is that if Sweden does not keep up with this development, it risks becoming more vulnerable and exposed. In addition, the Swedish Armed forces want to develop capabilities in space and unmanned systems.
The opposing voices to the proposal argue that the armed forces do not have the budget to even carry out their current obligations and that investment should go to making the current system work properly.

Чего ожидать: несмотря на то, что мы пока не видели APT-атак, в которых был бы использован шведский язык, мы прогнозируем, что в «гонку кибервооружений» вступят новые страны, которые обзаведутся инструментами для кибершпионажа.

АТАКИ «ПОД ЧУЖИМ ФЛАГОМ»

Иногда киберпреступники совершают ошибки. В абсолютном большинстве анализируемых нами атак мы находим признаки, указывающие на язык, на котором говорят злоумышленники. Например, в случае RedOctober и Epic Turla мы пришли к выводу, что злоумышленники, вероятнее всего, хорошо говорят по-русски. В случае NetTraveler мы заключили, что организаторы атак хорошо говорят по-китайски.

В некоторых случаях эксперты обнаруживают другие метаданные, указывающие на национальную принадлежность атакующих. Например, по результатам анализа временных меток файлов, использованных в ходе атаки, иногда можно сделать вывод о том, в какой части света скомпилирована большая часть вредоносных образцов.

Однако, злоумышленники начинают реагировать на эту ситуацию. В 2014 году мы обнаружили несколько атак «под чужим флагом», в ходе которых атакующие применяли «неактивное» вредоносное ПО, обычно используемое другими APT-группировками. Представьте себе, что западная APT-группировка в ходе атаки загружает на компьютеры жертв вредоносное ПО, которое, как правило, использует Comment Crew – известная группировка из Китая. Всем знакомы вредоносные модули Comment Crew; при этом немногие из жертв способны выполнить квалифицированный анализ сложных новых модулей. В результате может быть сделан ошибочный вывод, что атаку провела вышеупомянутая китайская группировка.

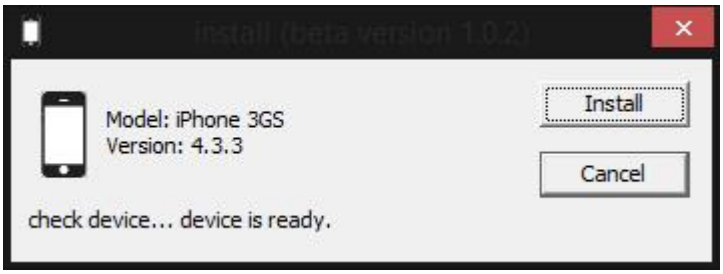
Чего ожидать: учитывая растущее стремление государственных органов публично обличать злоумышленников, мы считаем, что в 2015 году APT-группировки внесут соответствующие изменения в организацию своей деятельности и будут чаще проводить вредоносные кампании «под чужим флагом».

7

ДОБАВЛЕНИЕ АТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА В АРСЕНАЛ APT-ГРУППИРОВОК

Несмотря на то, что известны случаи, когда APT-группировки заражали мобильные устройства, это пока не стало серьезной тенденцией. Возможно, злоумышленников интересуют данные, которые, как правило, не хранятся на мобильных устройствах, а может быть, не все злоумышленники располагают технологиями, позволяющими заражать устройства под управлением Android и iOS.

В 2014 году мы столкнулись с несколькими новыми средствами, применяемыми в ходе атак APT-класса для заражения мобильных устройств – например, с мобильными модулями программы Remote Control System, производимой компанией HackingTeam.



Кроме того, в ходе протестов в Гонконге в октябре 2014 года были выявлены атаки на пользователей Android и iOS. По-видимому, эти атаки имеют отношение к APT-кампаниям.

Даже если на мобильном телефоне не хранятся ценные документы, схемы или планы геополитического развития на ближайшие 10 лет, он может быть использован как источник контактной информации, а также для подслушивания. Мы видели подобный функционал, разработанный группировкой RedOctober, которая заражала смартфоны и превращала их в «закладки» – мобильные подслушивающие устройства.

Чего ожидать: в 2015 году мы ожидаем активного применения вредоносного ПО для мобильных устройств, прежде всего для устройств под управлением Android и прошедшей джейлбрейк iOS.

APT+БОТНЕТ: ТОЧНО РАССЧИТАННАЯ АТАКА + МАССОВАЯ СЛЕЖКА

В целом, APT-группировки стараются не привлекать к своей деятельности излишнего внимания. Именно поэтому вредоносное ПО, применяемое в атаках APT-класса, значительно менее широко распространено, чем такие зловреды, как ZeuS, SpyEye и Cryptolocker.

В 2014 году мы столкнулись с использованием двумя APT-группировками (Animal Farm и Darkhotel) ботнетов в дополнение к обычным целевым атакам. Несомненно, ботнеты могут стать важным средством ведения кибервойны. Их можно применять для проведения DDoS-атак против враждебных стран, и такие случаи имели место. Становится понятно, почему некоторые APT-группировки в дополнение к проведению целевых атак организуют ботнеты.

Помимо проведения DDoS-атак, ботнеты дают еще одну возможность – они могут применяться как аппарат массовой слежки. Например, Flame и Gauss, обнаруженные в 2012 году, могли использоваться как инструменты массовой слежки, автоматически собирая информацию с компьютеров десятков тысяч жертв. Затем эту информацию должен был бы проанализировать суперкомпьютер – проиндексировать, сгруппировать по ключевым словам и темам. Вероятно, большая часть этой информации оказалась бы бесполезной. Но среди сотен тысяч украденных документов мог быть один, содержащий важные для злоумышленников сведения – в сложной ситуации такая находка способна сыграть решающую роль.

Чего ожидать: в 2015 году к тенденции использования точечных атак в сочетании с привлекающими к себе внимание кампаниями и организацией собственных ботнетов присоединятся новые APT-группировки.

9

АТАКИ НА ГОСТИНИЧНЫЕ СЕТИ

Группировка Darkhotel – одна из APT-групп, проводящих атаки на конкретных посетителей отелей в некоторых странах. В действительности, гостиницы дают прекрасные возможности для атак на определенные категории людей – например, на высшее руководство крупных компаний. Атаковать отели также чрезвычайно выгодно, поскольку это позволяет получать сведения о перемещениях высокопоставленных лиц по миру.

Взлом системы бронирования отелей – простой путь разведать планы конкретного лица, интересующего киберпреступников. Это также обеспечивает злоумышленников информацией о том, в каком номере остановилась жертва, что позволяет организовать на нее физическое нападение, а не просто кибератаку.

Организовать атаку на отель не так уж просто. Именно поэтому лишь немногие группировки – можно сказать, APT-элита – осуществляли подобные атаки в прошлом и продолжат использовать их как часть своего инструментария в будущем.

Чего ожидать: возможно, в 2015 году еще несколько группировок возьмут на вооружение подобные приемы, однако для большинства организаторов кампаний APT-класса подобные атаки останутся за пределами возможностей.

КОММЕРЦИАЛИЗАЦИЯ APT-КАМПАНИЙ И ЧАСТНЫЙ СЕКТОР

За последние годы мы опубликовали много материалов о вредоносных программах, созданных такими компаниями, как HackingTeam и Gamma International – наиболее известными производителями «легального» шпионского ПО. Несмотря на заверения этих компаний, что они продают свое ПО только «заслуживающим доверия государственным органам», в опубликованных отчетах различных организаций, в том числе Citizen Lab, неоднократно продемонстрировано, что продажи шпионского ПО невозможно контролировать. В результате эти опасные программные продукты оказываются в руках лиц и государств, заслуживающих доверия в значительно меньшей степени. Те, в свою очередь, применяют их для кибершпионажа против других стран или против собственного народа.

Тем не менее, подобная деятельность очень выгодна компаниям, производящим ПО для кибершпионажа. К тому же она сопряжена с минимальным риском, поскольку на данный момент не зафиксировано ни одного случая успешного уголовного преследования этих компаний за кибершпионаж. Правоохранительные органы, как правило, неспособны добраться до разработчиков подобного инструментария, поскольку ответственность ложится на тех, кто применял эти инструменты на практике, а не на компанию, разработавшую средства слежки.

Чего ожидать: это высокодоходный бизнес с низким уровнем риска. Поэтому можно ожидать появления новых игроков на рынке «легальных» средств слежки. Эти средства будут применяться для кибершпионских операций против других государств, слежки за собственными гражданами и, возможно, даже для подрывной деятельности.

ВЫВОДЫ

В целом, 2014 год ознаменовался достаточно сложными и разнообразными APT-атаками. Мы обнаружили несколько эксплойтов нулевого дня, например, CVE-2014-0515 – он применялся группировкой, известной как Animal Farm. Еще один обнаруженный нами эксплойт нулевого дня – CVE-2014-0487 – использовался группировкой, получившей название DarkHotel. Кроме новых, ранее неизвестных эксплойтов, мы столкнулись с несколькими новыми приемами закрепления в зараженной системе и сокрытия активности вредоносного ПО. Результатом этих открытий стала разработка и внедрение нескольких новых защитных механизмов для обеспечения безопасности наших пользователей.

Если 2014 году подходит определение «сложный», то 2015 год можно будет охарактеризовать словом «неуловимый». По нашему мнению, все больше APT-группировок будут стараться избежать обнаружения, применяя для этого все более сложные технические приемы.

Наконец, некоторые из подобных группировок будут действовать «под чужим флагом». Вот те изменения, которых мы ожидаем в следующем году и детали которых будем, как обычно, освещать в своих отчетах.

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