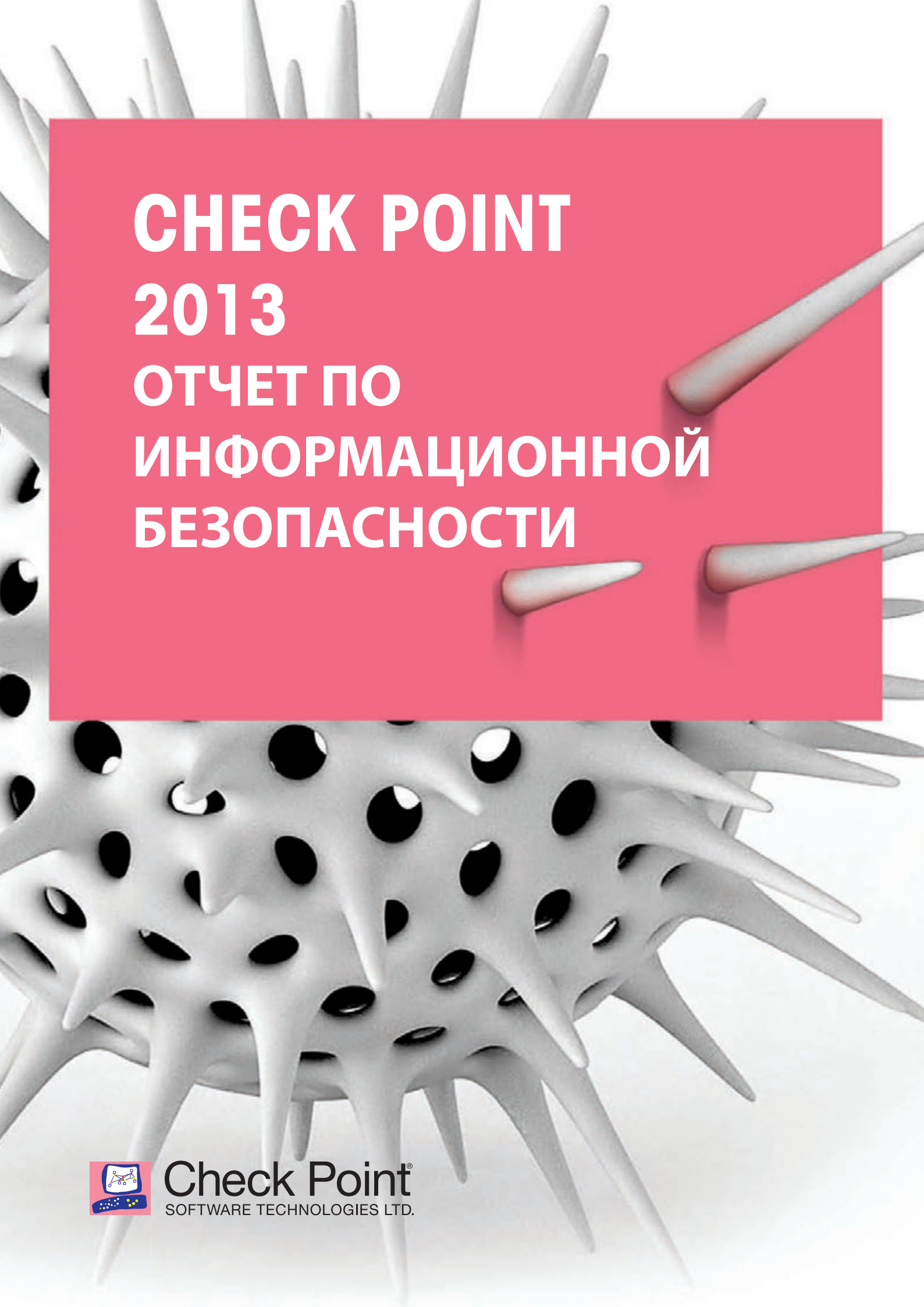


CHECK POINT 2013 ОТЧЕТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Check Point®
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT 2013 ОТЧЕТ ПО БЕЗОПАСНОСТИ

01 ВВЕДЕНИЕ И МЕТОДОЛОГИЯ

«ПОДОБНО ВОДЕ, КОТОРАЯ НИКОГДА НЕ СОХРАНЯЕТ СВОЕЙ ФОРМЫ, В БОЕВЫХ ДЕЙСТВИЯХ НИКОГДА НЕ СУЩЕСТВУЕТ ПОСТОЯННЫХ УСЛОВИЙ»[1]

ХОТЯ ЭТОЙ ФРАЗЕ УЖЕ 2600 ЛЕТ, ОНА УДИВИТЕЛЬНО ТОЧНО ОПИСЫВАЕТ СОВРЕМЕННЫЙ ВИД БОЕВЫХ ДЕЙСТВИЙ — КИБЕРВОЙНУ

Технологии, используемые хакерами, постоянно изменяются, вводя в оборот все более передовые и изощренные методы реализации атак, поднимая планку вызовов информационной безопасности на новый уровень. Центры обработки данных (ЦОД), пользовательские компьютеры и мобильные телефоны стали главными целями для хакеров, размещающих гигантское количество разнообразного вредоносного программного обеспечения (ПО), такого как боты, трояны и загрузчики «drive-by». Хакеры используют ухищрения и методы социальной инженерии для манипулирования ничего не подозревающими пользователями в целях получения доступа к корпоративной информации (такой как документы для внутреннего пользования, финансовые записи, кредитные карты и идентификаторы пользователей) или для вывода из строя сервисов с помощью атак класса «отказ в обслуживании». Здесь идет современная война с использованием передовых средств реализации угроз и изощренных атак. Корпоративная информация, хранящаяся в ЦОДах, ПК и мобильных телефонах увеличивается со скоростью света, и рост объемов данных и количества устройств несет в себе новые риски. Наконец, список угроз ИБ не сокращается — наоборот, с каждым разом новые атаки открывают все более глубокие уровни сложности.

С какими главными рисками ИБ сталкивалась Ваша сеть за последний год? Каким рискам она будет открыта в следующем году? Над этими ключевыми вопросами последние пять месяцев работала группа исследователей компании Check Point. Собирая ответы на них, компания Check Point провела интенсивный анализ состояния ИБ.

Предлагаемый отчет представляет собой выборку событий сетевой безопасности за 2012 год, которые произошли в различных организациях по всему миру. В отчете отражены события ИБ, происшедшие в организациях, с примерами инцидентов на основе общедоступной информации, объяснения методов реализации некоторых атак, а также рекомендации по защите от таких угроз ИБ. Отчет состоит из трех частей. Первая часть сфокусирована на таких угрозах ИБ как боты, вирусы, бреши в ИБ и атаки. Вторая часть посвящена обсуждению рисков веб-приложений, которые угрожают сетевой безопасности организации. Заключительная часть рассматривает вопросы потерь данных, связанных с ненамеренными действиями пользователей.

Методология

Отчет по ИБ компании Check Point 2013 базируется на совместном исследовании и анализе событий ИБ, полученных из четырех основных источников: аналитических отчетов Check Point Security Gateway[2], Check Point ThreatCloud™[3], отчетов по сетевой безопасности Check Point SensorNetTM и безопасности конечных устройств Check Point Endpoint Security.

Мета-анализ событий сетевой безопасности 888 компаний проводился на основании данных, полученных со шлюзов безопасности Check Point, которые сканировали входящий и исходящий трафик компаний в режиме реального времени. Для обнаружения таких угроз ИБ как приложения повышенного риска, попытки вторжения, вирусы и боты, потеря значимых данных и т. п., трафик инспектировался с использованием технологии multi-tier Software Blades компании Check Point. Мониторинг трафика в режиме реального времени обеспечивался благодаря использованию шлюзов безопасности Check

Point Security Gateway включенных в режиме inline, либо подключаемых к порту мониторинга (tap).

В среднем, сетевой трафик каждой организации просматривался в течение 134 часов. В рамках исследования изучались компании, представляющие широкий спектр индустрий, расположенные в различных географических регионах (Табл. 1-A и 1-B).

Кроме того, свыше 111.7 миллиона событий от 1494 шлюзов безопасности были проанализированы с использованием данных, полученных с помощью системы Check Point ThreatCloud™. ThreatCloud представляет собой массивную базу данных по ИБ, обновляемую в реальном времени, в которую попадают данные обширной сети глобальных сенсоров, размещенных по всему земному шару и собирающих информацию об угрозах и вредоносном ПО. ThreatCloud позволяет идентифицировать новые глобальные тенденции и угрозы ИБ, создавая коллаборативную среду для борьбы с киберпреступностью. В нашем отчете мы использовали данные полученные от системы ThreatCloud за трехмесячный срок с августа по октябрь 2012 года.

Данные по угрозам были собраны при помощи сети сенсоров Check Point SensorNet™ в период с 1 июля по 30 сентября 2012 года. Check Point SensorNet — это распределенная сеть сенсоров, собирающая для центральной системы анализа информацию о ИБ и статистику трафика. Эти данные используются для выявления тенденций и аномалий, а также построения картины состояния ИБ по всему миру в реальном времени.

И, наконец, мета-анализ 628 отчетов по ИБ конечных устройств в различных организациях. Анализ ИБ включал в себя данные по сканированию каждого хоста для проверки рисков потери данных, рисков вторжения и рисков вредоносного ПО. Анализ проводился с помощью утилиты Check Point Endpoint Security report tool, осуществляющей проверку на наличие на хосте активного процесса антивирусного ПО, является ли версия антивирусного ПО текущей, используются ли последние версии прикладного ПО и т. п. Утилита является бесплатной и общедоступной, и может быть загружена с общедоступного вебсайта Check Point[4].

Основываясь на данных вышеуказанных источников и был составлен данный отчет.

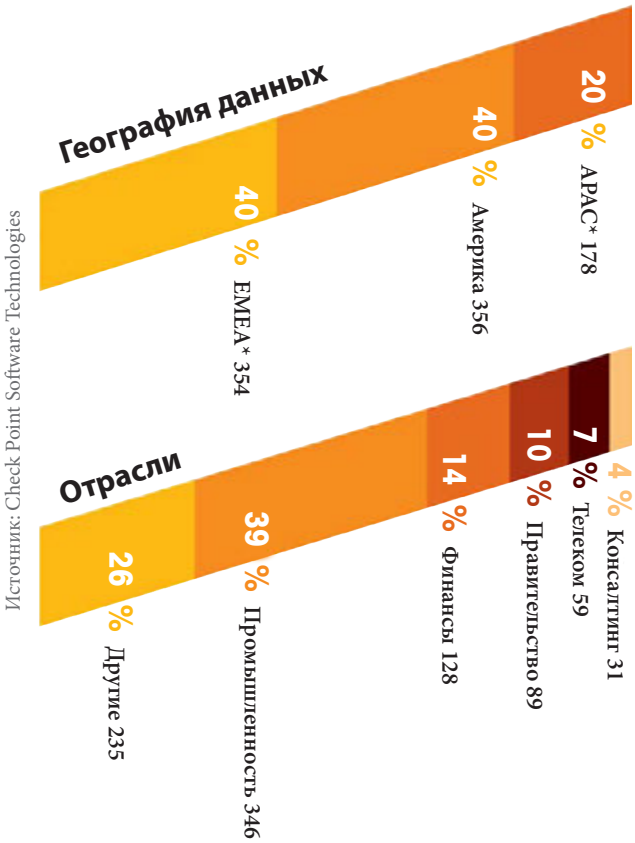


Таблица 1-A

*APAC - Азиатско-Тихоокеанский регион, EMEA - Европа, Ближний Восток и Африка

Определения отраслей

Промышленность — Химическая/нефтеперегонная промышленность, здравоохранение, фармацевтическая промышленность, информационные технологии, производство, транспорт, инфраструктура, энергетика.
Финансы — Финансовый сектор, бухгалтерия, банки, инвестиционные компании.
Правительство — Правительственные организации, военные структуры.
Телеком — Телефонные компании, сервис провайдеры, ISP, MSP.
Консалтинг — Консультационные услуги.
Другие — Реклама/СМИ, дистрибуторы, образование, юридические компании, развлечения и отдых, розничная и оптовая торговля, безопасность, другое.

02 УГРОЗЫ ДЛЯ ВАШЕЙ ОРГАНИЗАЦИИ

Горячая новость: обнаружена новая кибератака

В 2012 году кибератаки продолжили свое распространение и все чаще становились новостным поводом. Почти ежедневно угрозы вредоносного ПО, атаки и ботнеты занимали первые страницы новостных изданий, демонстрируя очередные успехи хакеров в деле кражи данных, нарушения нормальной работы и шпионажа в корпорациях и государственных структурах. Примеры, представленные ниже, являют собой лишь верхушку айсберга кибератак, случившихся в 2012 году: хакеры атаковали сеть Белого Дома[6], активисты хакерской группы Anonymous обрушили вебсайты торговых групп US Telecom Assotiation н TechAmerica[7], кибератаки обрушились на такие корпорации как Capital One Financial Corp., BB&T Corp., HSBC, Bank USA[8] и многие другие.

Угрозы класса Advanced Persistent Threats

Киберпреступники более не представляют из себя отдельных любителей. Во многих случаях они принадлежат к хорошо структурированным организациям, сходными с террористическими ячейками — они хорошо финансированы, имеют мотивации и цели. Киберпреступники, по всей видимости, уделяют существенное время и ресурсы на сбор разведывательной информации. Их криминальные действия наносят организациям серьезный ущерб, такой как утрата конфиденциальных данных, перерывы в работе бизнеса, репутационный ущерб и, безусловно, финансовые потери. Наиболее изощренные и долгосрочные атаки, разработанные для узких, заранее определенных целей мы будем называть Advanced Persistent Threats — APT. Такие атаки практически невозможно обнаружить с помощью традиционных систем ИБ, что представляет собой существенный риск для сетей правительственных организаций, предприятий, малого бизнеса и даже домашних пользователей.

«СУЩЕСТВУЮТ ТОЛЬКО ДВА ВИДА КОМПАНИЙ – ТЕ, КОТОРЫЕ БЫЛИ ВЗЛОМАНЫ, И ТЕ, **КОТОРЫЕ БУДУТ**»

Роберт Мюллер, директор ФБР, март 2012 года[5].

BLACKHOLE
НАБОР ЭКСПЛОЙТОВ ДЛЯ ШИРОКОГО КРУГА ПОЛЬЗОВАТЕЛЕЙ

Большой вклад в увеличение вредоносной активности за последний год был сделан за счет распространения среди хакеров предварительно собранных и легких в использовании утилит и пакетов ПО. С помощью одного клика мыши любой пользователь может загрузить готовый к использованию пакет ПО для проведения сложной атаки. Одним из таких наборов является BlackHole exploit kit — широко используемый пакет ПО на основе веб-технологий. BlackHole включает в себя инструментарий, позволяющий использовать дыры в безопасности веб-браузеров для загрузки вирусов, ботов, троянов и других видов вредоносного ПО на компьютеры ничего не подозревающих жертв. Цены на такие наборы колеблются от $50 за один день использования до $1500 за годовую подписку[9].

ИНЦИДЕНТЫ ПО ВЗЛОМУ ДАННЫХ В 2012 ГОДУ

В этом году имели место многочисленные инциденты по взлому данных, приведшие к открытию информации, хранящейся на корпоративных серверах, и относящейся к платежным картам, а также персональным данным клиентов, студентов и пациентов. Вся эта вредоносная активность имела своей общей целью добычу конфиденциальной информации. Приведем некоторые примеры:

Global Payments Inc.
Международная платежная компания была взломана в июне 2012 года. Была похищена информация о более чем 1.5 миллионов платежных карт.

Кларксвиль, Теннесси, США
В мае 2012 г. Хакеры осуществили взлом системы школы графства Кларксвиль-Монтгомери (Clarksville-Montgomery County School) и похитили имена, номера социального страхования и другие персональные данные более чем 110000 людей. Хакеры использовали информацию, размещённую онлайн сотрудниками и учащимися, для получения доступа к системе[10].

Serco Thrift Savings Plan
В мае 2012 года компьютерная атаке, направленная на Serco в США, привела ко взлому информации об 123000 федеральных служащих.

Университет Небраски пострадал от взлома, повлекшего кражу свыше 650000 файлов, содержащих персональную информацию студентов, выпускников, родителей и служащих университета из базы данных Информационной Системы Студентов Небраски (Nebraska Student Information System).

Департамент Технических Служб, Юта, США
В марте 2012 года, 780000 файлов пациентов, относящихся к системе медицинского страхования Medicaid, были объявлены похищенными хакерами, действовавшими, предположительно, из Восточной Европы.

Национальная Служба Здравоохранения Соединенного Королевства
В период июля 2011 и июня 2012 года, Национальная Служба Здравоохранения Соединенного Королевства пострадала от нескольких взломов, вскрывших около 1.8 миллионов записей о пациентах[11].

При реализации APT атак первым этапом обычно является сбор разведывательной информации о цели. После этого атакующие осуществляют первичное проникновение в сеть цели для того, чтобы открыть «заднюю деверь» (back-door) и постоянно присутствовать в этой сети. Обычно это достигается с помощью установки на хост бота, дающего возможность атакующему незаметно связываться с зараженным хостом. Затем атакующий пытается получить дальнейший доступ к сети и скомпрометировать большее количество узлов. После этого атакующий достигает своей цели. Он может эксплуатировать зараженный хост для сбора данных или проведения деструктивных действий удаленно, продолжая присутствовать в системе незамеченным долгое время.

НАБОРЫ БОТОВ ПРОДАЮТСЯ ОНЛАЙН ЗА $500. УЩЕРБ ОТ ИХ ПРИМЕНЕНИЯ МОЖЕТ СТОИТЬ БИЗНЕСУ **МИЛЛИОНЫ ДОЛЛАРОВ**

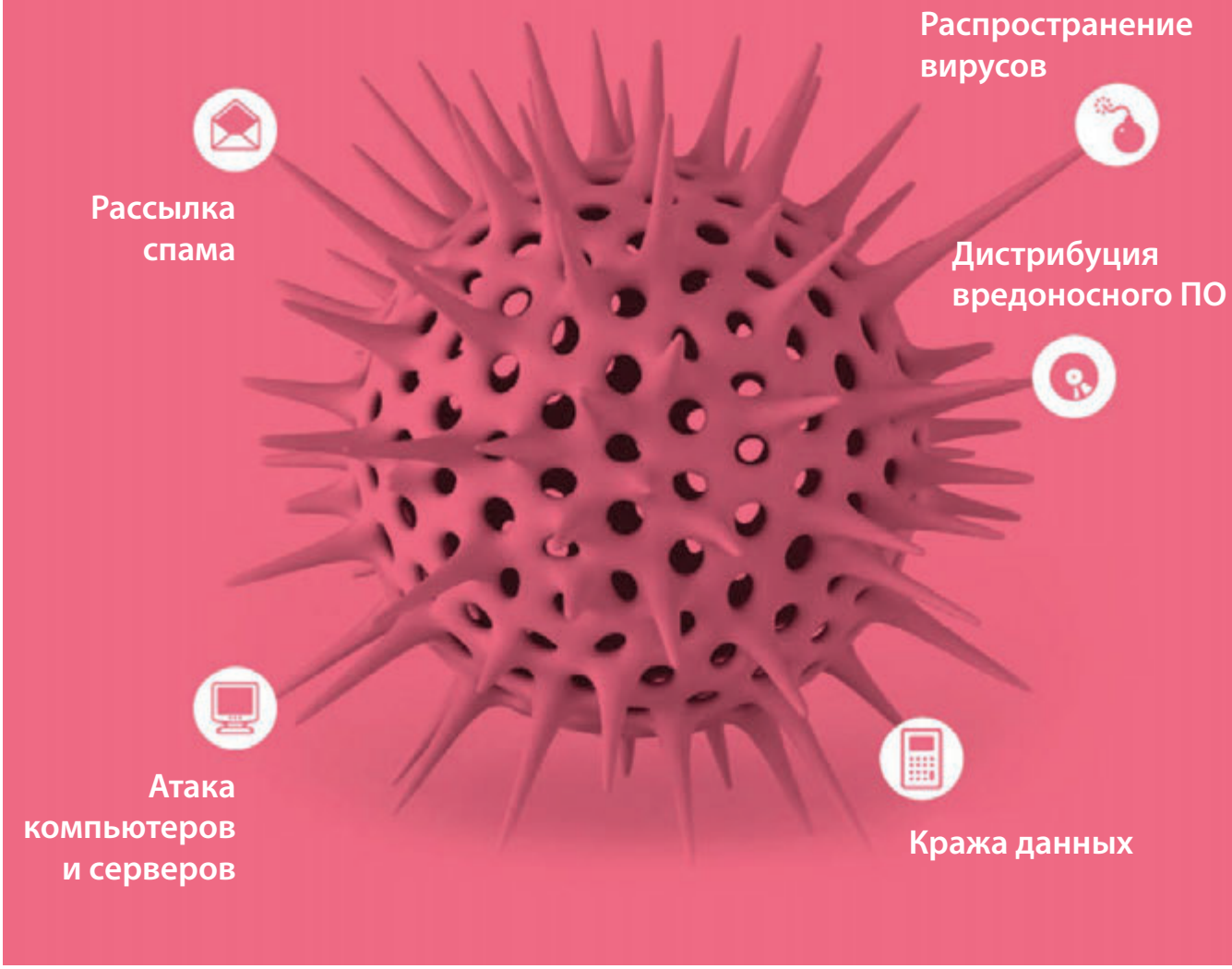
Ботнеты приходят, чтобы остаться

Ботнеты представляют собой одну из наиболее значимых угроз сетевой безопасности, с которыми приходится сегодня сталкиваться организациям. Бот — это вредоносное ПО, предназначенное для вторжения и заражения компьютера в целях предоставления удаленного управления злоумышленникам. Инфицированный компьютер может, таким образом, производить несанкционированные действия, такие как: кража данных, рассылка спама, распространение вредоносного ПО и участия в атаках класса «отказ в обслуживании» (Denial of Service, DoS). Владелец зараженного компьютера может совершенно не подозревать об активности такого рода. Боты также играют ключевую роль в целенаправленных APT атаках.
В настоящее время можно выделить две основных тенденции присущие угрозам, ориентированным

на атаки с использованием ботов. Первая тенденция — это растущая индустрия киберпреступлений, направленных на получение прибыли,— эта индустрия включает в себя киберпреступников, операторов вредоносного ПО, поставщиков инструментария, кодировщиков и сопутствующие программы. Их «продукты» могут быть легко приобретены онлайн на многочисленных сайтах (например, наборы «сделай сам» для вредоносного ПО, рассылка спама, кража данных и DoS атаки) и поэтому организациям достаточно сложно противостоять таким атакам. Вторая тенденция связана с атаками, вызванными идеологическими мотивами или инициированными государствами, и направленными на определенных людей или организации для продвижения политических требований или ведения кибервойны.

Ботнеты приходят, чтобы остаться. В противоположность вирусам или другим традиционным видам вредоносного ПО (чей код и форма остаются постоянными), ботнеты являются по своей природе динамическими и быстро меняют свою форму и характер трафика. Наборы ботов продаются онлайн за менее чем $500, и могут стоить бизнесу потерь миллионов долларов. Проблема ботов приобрела гигантское значение.

АКТИВНОСТЬ БОТНЕТОВ



63%

ОРГАНИЗАЦИЙ, РАССМОТРЕННЫХ В НАШЕМ ИССЛЕДОВАНИИ, ИНФИЦИРОВАНЫ БОТАМИ

Ботнеты есть везде, но насколько критична ситуация?

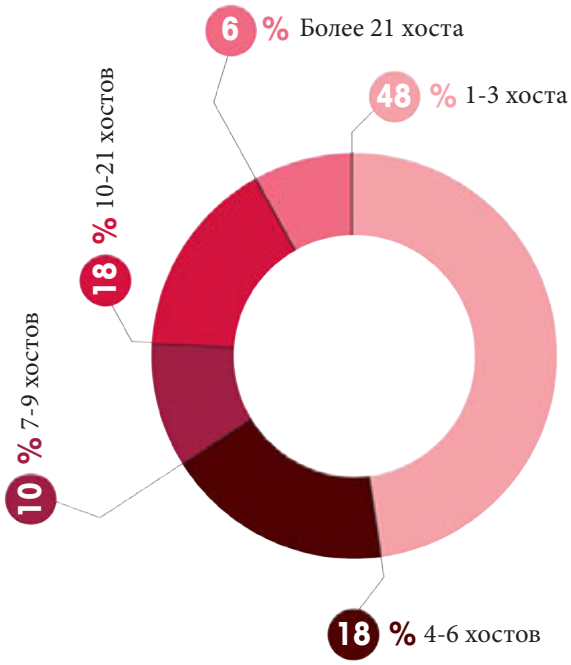
Согласно оценкам, около четверти всех персональных компьютеров, подключенных к Интернету, могут быть частью ботнета. Наше исследование показывает, что в 63% организаций был обнаружен как минимум один бот. Большинство организаций заражены несколькими ботами.

Как работает ботнет

Обычно ботнет включает в себя некоторое число компьютеров, зараженных вредоносным ПО, которое устанавливает связь с системой или системами управления, называемыми Командными и Управляющими (Command & Control, C&C) серверами. Когда бот инфицирует компьютер, он берет его под свой контроль и нейтрализует антивирусную защиту. Так как боты пытаются скрыть свое присутствие в компьютере и изменяют свои признаки, по которым их может опознать антивирусное ПО, их бывает достаточно трудно обнаружить. Затем бот соединяется с C&C центром для получения инструкций от киберпреступников. Для таких

Количество зараженных ботами хостов

(в % от общего числа организаций)

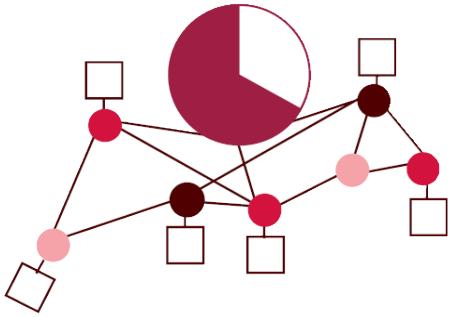


Источник: Check Point Software Technologies

Таблица 2-А

соединений используются разнообразные протоколы, включая Internet Relay Chat (IRC), HTTP, ICMP, DNS, SMTP, SSL, и в отдельных случаях протоколы, специально созданные разработчиками ботов.

КАЖДЫЕ 21 МИНУТУ БОТ СВЯЗЫВАЕТСЯ СО СВОИМ КОМАНДНЫМ И УПРАВЛЯЮЩИМ ЦЕНТРОМ

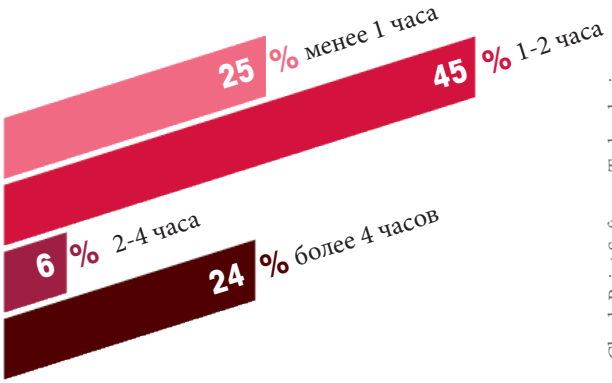


Управляющие действия

Боты представлены во множестве различных форм и могут совершать различные действия. Во многих случаях один бот может нести в себе несколько различных видов угроз. Под управлением C&C центра ботнет может направляться «бот-пастухом» для проведения нелегальных действий скрытно от пользователя. К таким действиям относятся: заражение других компьютеров для присоединения их к ботнету, массовые рассылки спама, DDoS атаки и кража персональной, финансовой и конфиденциальной информации предприятия с помощью ботов. Часто боты используются как инструменты атак APT, когда киберпреступники определяют частных лиц либо организации как объект для атаки. Таблица 2-B показывает, насколько часто бот осуществляет связь со своим центром управления. В рамках исследования обнаружено, что в 70% случаев боты осуществляют связь со своим C&C центром как минимум каждые 2 часа. В большинстве случаев (см Таблицу 2-C) такие центры управления находятся в США, за которыми следуют Германия, Нидерланды и Франция.

Отдельные типы связи бота со своим C&C центром включают в себя: сообщения от новых компьютеров о заражении, сообщения, подтверждающие активность, а также данные, собранные о системе с компьютера. Наше исследование показывает, что в среднем бот связывается со своим C&C центром каждые 21 минуту.

Частота связи ботов со своими управляющими центрами



Источник: Check Point Software Technologies

Таблица 2-B

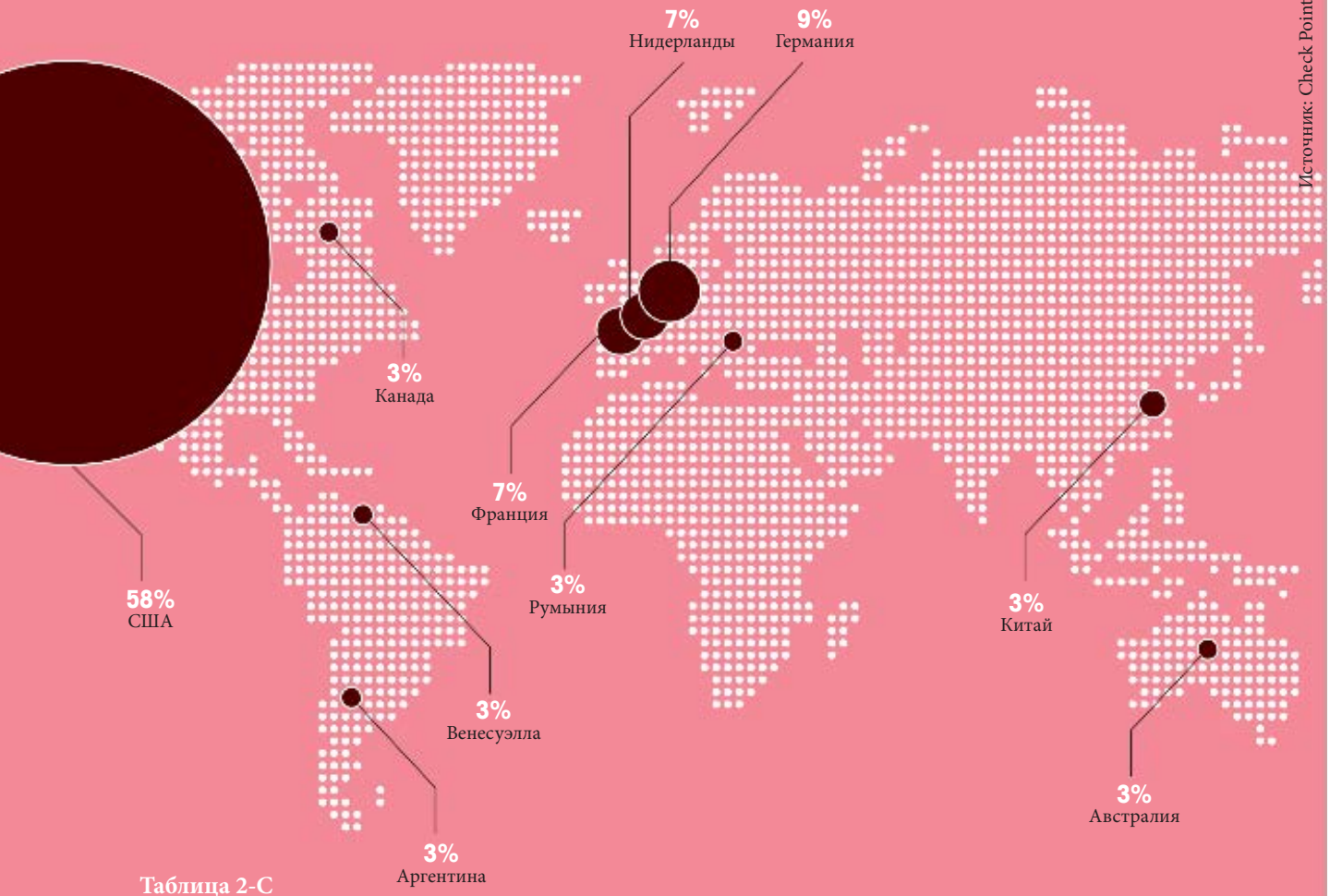
За какими ботнетами мы должны наблюдать?

В настоящее время существует большое число ботнетов. В следующей таблице приведены наиболее известные из них, обнаруженные в рамках нашего исследования. Для более глубокого понимания этих скрытых угроз, мы разместили по каждой из них дополнительную информацию в Приложении A.

Семейство ботнетов	Вредоносная активность
Zeus	Кража идентификационной информации для онлайн банкинга
Zwangi	Показ пользователю нежелательных рекламных сообщений
Sality	Самораспространяющийся вирус
Kuluoz	Удаленное исполнение вредоносных файлов
Juasek	Удаленные вредоносные действия: открытие командной оболочки (command shell), поиск/создание/удаление файлов и т.п.
Papras	Кража финансовой информации и получение удаленного доступа.

Дополнительная информация приведена в Приложении A.

СТРАНЫ, ГДЕ РАСПОЛОЖЕНО НАИБОЛЬШЕЕ ЧИСЛО ЦЕНТРОВ УПРАВЛЕНИЯ БОТАМИ



Источник: Check Point Software Technologies

Таблица 2-C

В 75%

ОРГАНИЗАЦИЙ ХОСТЫ ОСУЩЕСТВЛЯЮТ ДОСТУП К ВРЕДОНОСНЫМ САЙТАМ

КАЖДЫЕ 23 МИНУТЫ ХОСТ ОСУЩЕСТВЛЯЕТ ДОСТУП К ВРЕДОНОСНОМУ САЙТУ

Как Ваша организация может быть заражена вредоносным ПО

Существуют различные пути преодоления защиты организации: использование уязвимостей в веб-браузерах, мобильных телефонах, вредоносные аттачменты в сообщениях электронной почты, съемные носители информации,— это всего лишь несколько примеров из обширного списка. Кроме того, эксплуатация приложений Web 2.0 и социальных сетей, используемых в качестве инструментов ведения бизнеса, предоставляют хакерам прекрасную возможность склонить пользователя кликнуть на вредоносную ссылку или «вредообъявление» — вредоносный рекламный баннер, исполняемый на добропорядочных вебсайтах.

Хотя ботнеты рассматриваются на сегодняшний день как наиболее опасная угроза, организации в то же время сталкиваются с другими угрозами из мира вредоносного ПО: вирусами, червями, вредоносным рекламным ПО (adware), троянами и т.п. Наше исследование показало, что в 75% организаций хосты осуществляют контакт с вредоносными вебсайтами.

Следующая диаграмма показывает количество хостов, контактировавших с вредоносным вебсайтом, в процентах от общего числа организаций. В более чем 50% организаций как минимум пять хостов контактировали с вредоносным вебсайтом.

Количество хостов, контактировавших с вредоносными сайтами

(в % от общего числа организаций)

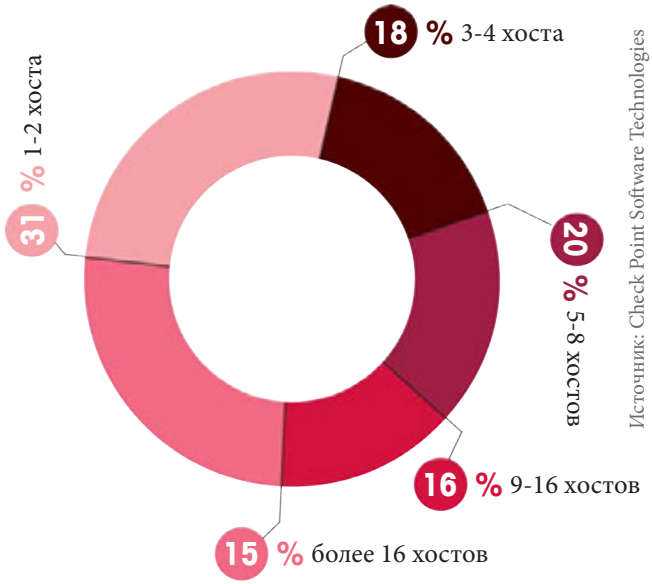


Таблица 2-D

Вредоносное ПО может быть загружено как пользователем, так и ботом, которым уже заражен компьютер. Исследование показывает, что в 53% организаций вредоносное ПО было загружено из корпоративной сети. В более чем 50% организаций были найдены четыре или более хоста, загрузивших вредоносное ПО.

Следующая диаграмма показывает среднюю частоту загрузок вредоносного ПО в организациях, наблюдаемых во время нашего исследования.

Частота загрузки вредоносного ПО

(в % от общего числа организаций)

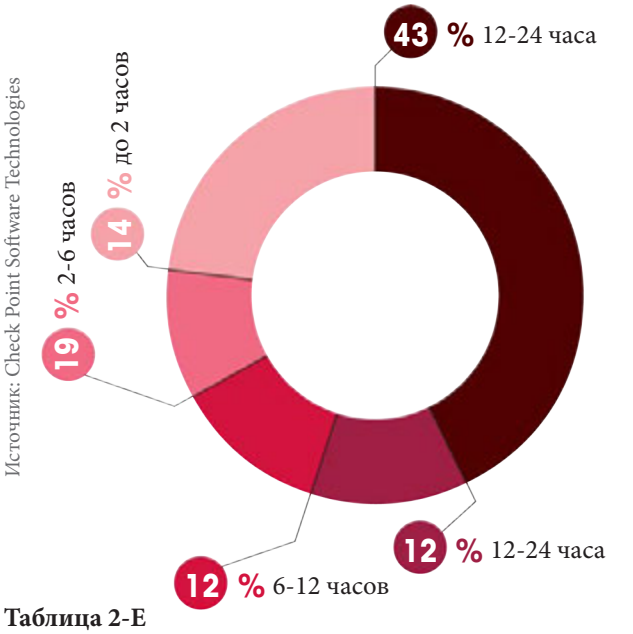


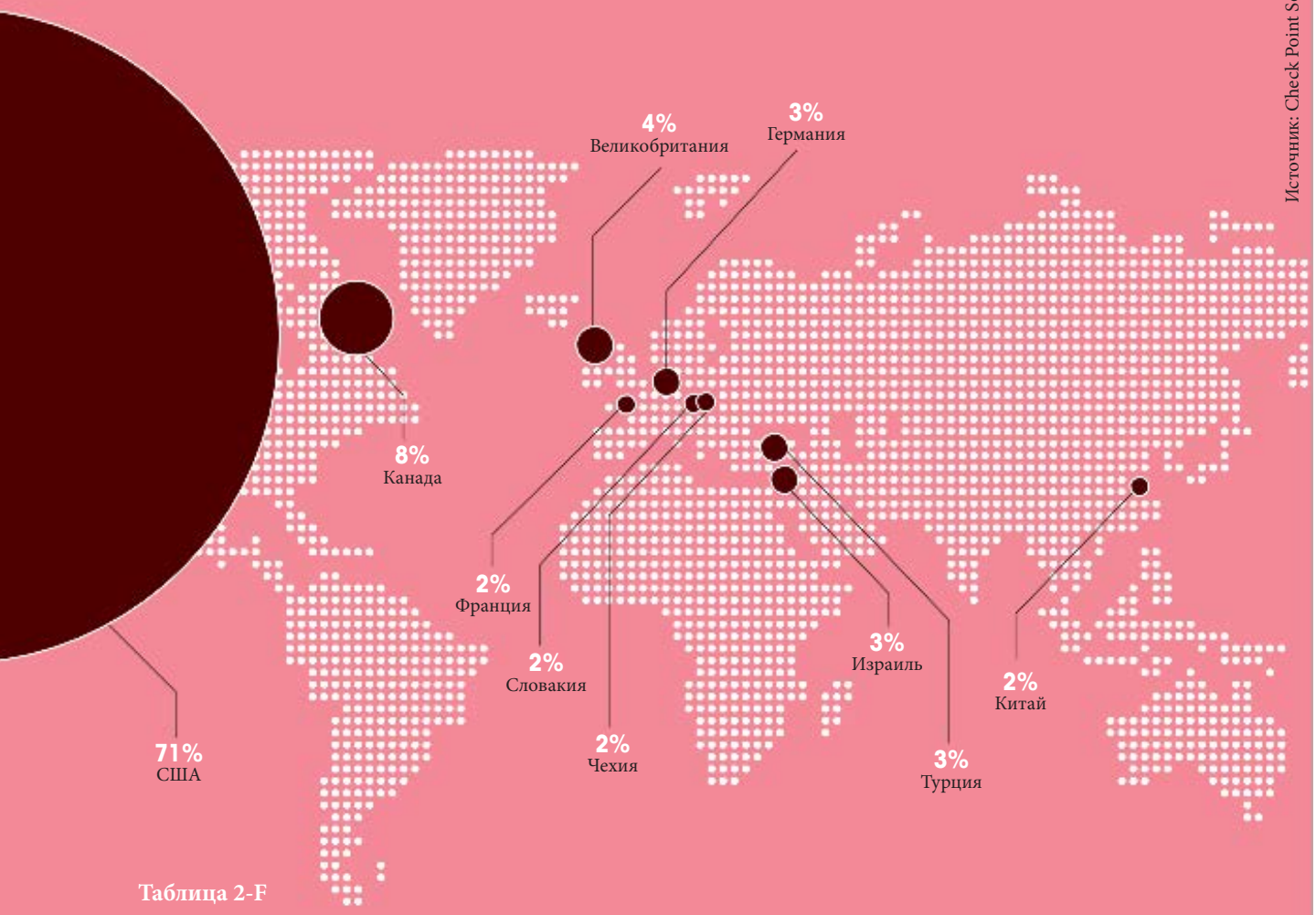
Таблица 2-E

В таблице 2-G представлено количество хостов, загрузивших вредоносное ПО. В более чем 50% организаций как минимум пять хостов загрузили вредоносное ПО.

В рамках нашего исследования, наибольшее количество вредоносного ПО было найдено в США, за которыми следуют Канада и Соединенное Королевство, как это представлено в Таблице 2-F.

Антивирусная защита является одним из методов противодействия заражению вредоносным ПО, однако наше исследование показало, что 23% хостов в организациях не обновляли ежедневно свои антивирусные базы. Хост, на которым установлен необновленный антивирус, открыт для заражения новыми вирусами. Мы также обнаружили что 14%

СТРАНЫ, ГДЕ РАСПОЛОЖЕНО НАИБОЛЬШЕЕ ЧИСЛО ЦЕНТРОВ УПРАВЛЕНИЯ БОТАМИ

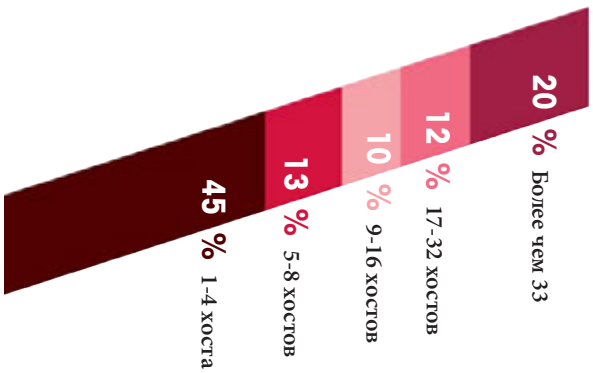


Источник: Check Point Software Technologies

Таблица 2-F

Количество хостов, загрузивших вредоносное ПО

(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица 2-G

хостов в организациях вообще не имеют антивирусного ПО. Такие хосты с высокой вероятностью могут быть заражены вредоносным ПО.

Познакомьтесь: вирус «miniFlame» — младший, но более опасный брат вируса Flame

Как видится сейчас, вредоносное ПО Flame, обнаруженное ранее в этом году, было только началом. Позже была открыта сходная программа, названная «miniFlame», и использованная для направленных атак на цели на Ближнем Востоке. miniFlame имеет «черный ход» (backdoor), позволяющий осуществлять удаленное управление, кражу данных и возможность снимать копии экрана.

АТАКА EUROGRABBER
У БОЛЕЕ, ЧЕМ 30000 КЛИЕНТОВ БАНКОВ ПОХИЩЕНО СВЫШЕ 36 МИЛЛИОНОВ ЕВРО

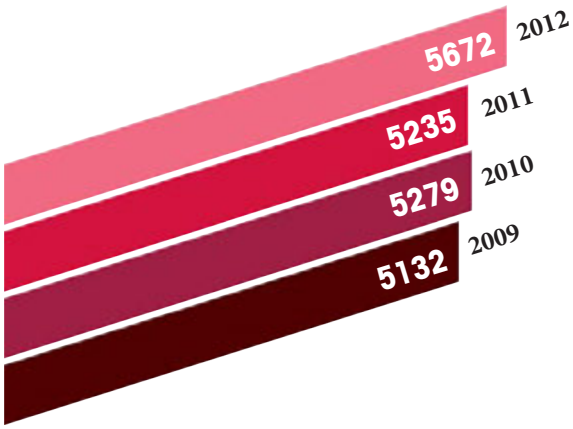
В течение 2012 года произошла сложная многоуровневая атака, завершившаяся похищением свыше 36 миллионов евро у более, чем 30000 клиентов различных банков Европы. Все было проведено полностью незаметно: клиенты банков даже не подозревали о том, что они были заражены троянами, что их сессии онлайн банкинга были скомпрометированы или что денежные средства были похищены прямо с их счетов. Эта серия атак, названная Eurograbber, была обнаружена компаниями Versafe и Check Point Software Technologies. Атака Eurograbber использовала новые и очень успешные варианты троянов ZITMO или Zus-In-The-Mobile. На сегодняшний день, эксплойт был зафиксирован только в странах еврозоны, но варианты этой атаки потенциально могут затронуть также и страны за пределами Евросоюза. В ходе многоэтапной атаки были заражены компьютеры и мобильные устройства клиентов онлайн банков и, как только троян Eurograbber был установлен на обоих устройствах, все сессии онлайн банкинга полностью мониторились и подвергались манипуляциям со стороны атакующих. Была обойдена даже система двухфакторной аутентификации, используемая банками для подтверждения онлайн транзакций, — фактически злоумышленники использовали ее для аутентификации своих незаконных денежных переводов. Кроме того, трояны, используемые для мобильных устройств были разработаны в версиях как для Blackberry, так и для Android, для охвата более широкого «целевого рынка» и, тем самым делалось возможным заражение как корпоративных, так и частных клиентов банков и последующий незаконный перевод средств в размерах от 500 до 250000 евро с каждого счета. Дополнительная информация об атаке Eurograbber, включая детальный разбор атаки, можно найти в отчете Eurograbber attack case study[12] на вебсайте компании Check Point.

Больше уязвимостей — больше эксплойтов

Известные уязвимости являются ключевыми целями для атак хакеров, просто полагающихся на то, что большинство организаций не обновляют свое ПО на еженедельной основе. Чем больше организация, тем труднее администраторам ИБ поддерживать системы полностью обновленными. Таким образом, во многих случаях, уязвимости, патчи к которым выпущены уже год назад, могут быть успешно использованы для проникновения в системы больших и малых организаций, которые не применяют последние патчи ПО к своим системам.

Число уязвимостей, открываемых ежегодно, производит сильное впечатление — в 2012 году для хакеров появилось более чем 5000[13] новых способов получить доступ и нанести урон системам. И, кроме того, существуют также многочисленные скрытые уязвимости, используемые киберпреступниками в своих целях.

Общее число основных уязвимостей



Источник: Common Vulnerabilities and Exposures (CVE)

Таблица 2-H

В таблице 2-I приведены данные по наиболее распространенным продуктам, используемым в различных организациях по всему миру, являющихся наиболее уязвимыми — Oracle, Apple и Microsoft являются среди них наиболее уязвимыми производителями.

Распределение количества уязвимостей обнаруженных в 2012 году по компаниям-производителям

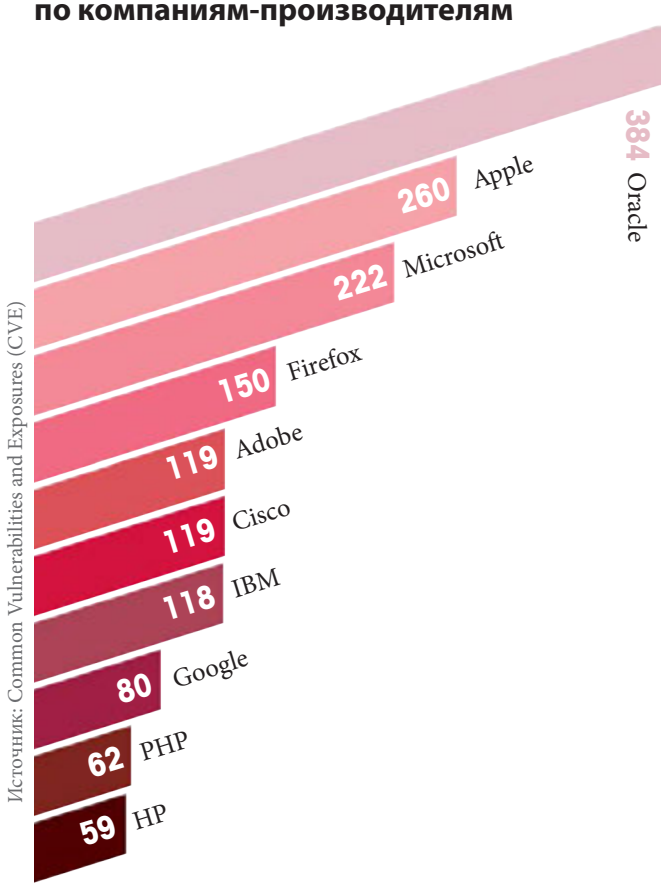


Таблица 2-I

Наше исследование показало, что 75% хостов в организациях не используют последние версии ПО (например: Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment и т. п.). Это означает, что такие хосты имеют большое число открытых уязвимостей, которые могут быть использованы хакерами. Наше исследование показало, что у 44% хостов в организациях не используются последние Microsoft Windows Service Pack. Service Pack обычно включают в себя обновления безопасности для операционной системы. Не использовать последний Service Pack означает подвергать систему риску ИБ.

Кроме того, мы обнаружили, что инциденты ИБ, связанные с продуктами компании Microsoft имеются в 68% организаций. События ИБ, относящиеся к другим производителям, таким как Adobe и Apple, мы обнаружили в существенно меньшем числе организаций. Интересно отметить, что хотя Apple является вторым производителем по числу найденных уязвимостей, в действительности лишь малый процент организаций имел инциденты ИБ, связанные с продуктами Apple.

Количество инцидентов ИБ по компаниям-производителям ПО

(в % от общего числа организаций)

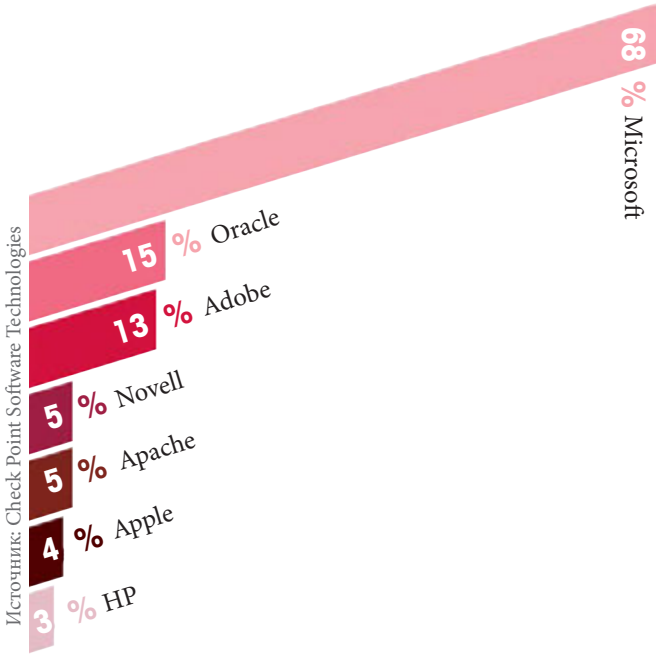


Таблица 2-J

Хакеры используют различные техники, обычно называемые «векторами атак». В Таблице 2-K представлены некоторые векторы атак согласно доле организаций, от них пострадавших. В рамках нашего исследования наиболее популярными векторами атак были: повреждение памяти, переполнение буфера и отказ в обслуживании.

Наиболее популярные векторы атак

Источник: Check Point Software Technologies

Таблица 2-K

Что представляет собой атака SQL Injection? Хроника событий SQL Injection

Этот пример показывает нам реальный случай серии атак класса SQL Injection, происшедший в период между июлем и октябрем 2012 года у одного из заказчиков компании Check Point. Атака была обнаружена и блокирована шлюзом безопасности Check Point Security Gateway. Рассматриваемый случай вошел в отчет группы Check Point ThreadCloud Managed Security Service.

SQL Injection представляет собой эксплойт безопасности (CVE-2005–0537), при котором атакующий добавляет код SQL (Structured Query Language) ко входным данным для вебформы с целью получения доступа или изменения хранящихся в базе данных. Таблица 2-M показывает, как выглядит такая атака. Выделенный текст отмечает данные, которые хакер пытается раскрыть с помощью SQL Injection (в данном примере — имена пользователей и пароли). Команды SQL здесь следующие: select, concat и from. Атака производилась с 99 различных IP адресов. И хотя цель находилась в Европе, атаки производились из различных частей земного шара, как это показано в Таблице 2-M.

SQL Injection может выполняться вручную (хакер использует клавиатуру для ввода), или автоматически (с помощью скрипта). В данном примере, как показано в Таблице 2-L, пик атаки имел всплеск в 4184 попытки (скорее всего автоматические) которые были запущены в течение двух дней, используя одинаковый шаблон и имея одинаковый IP адрес источника.

Частота событий SQL Injection

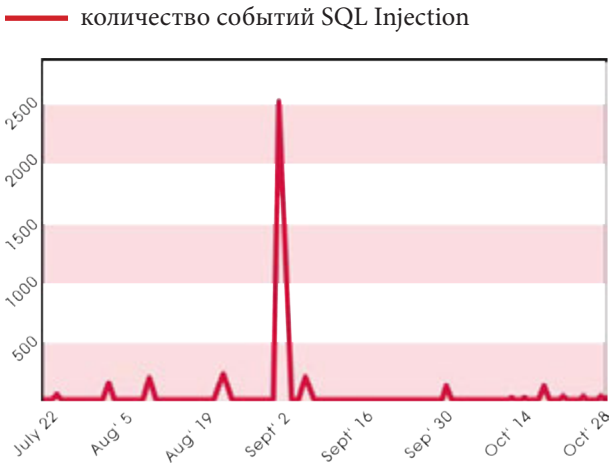
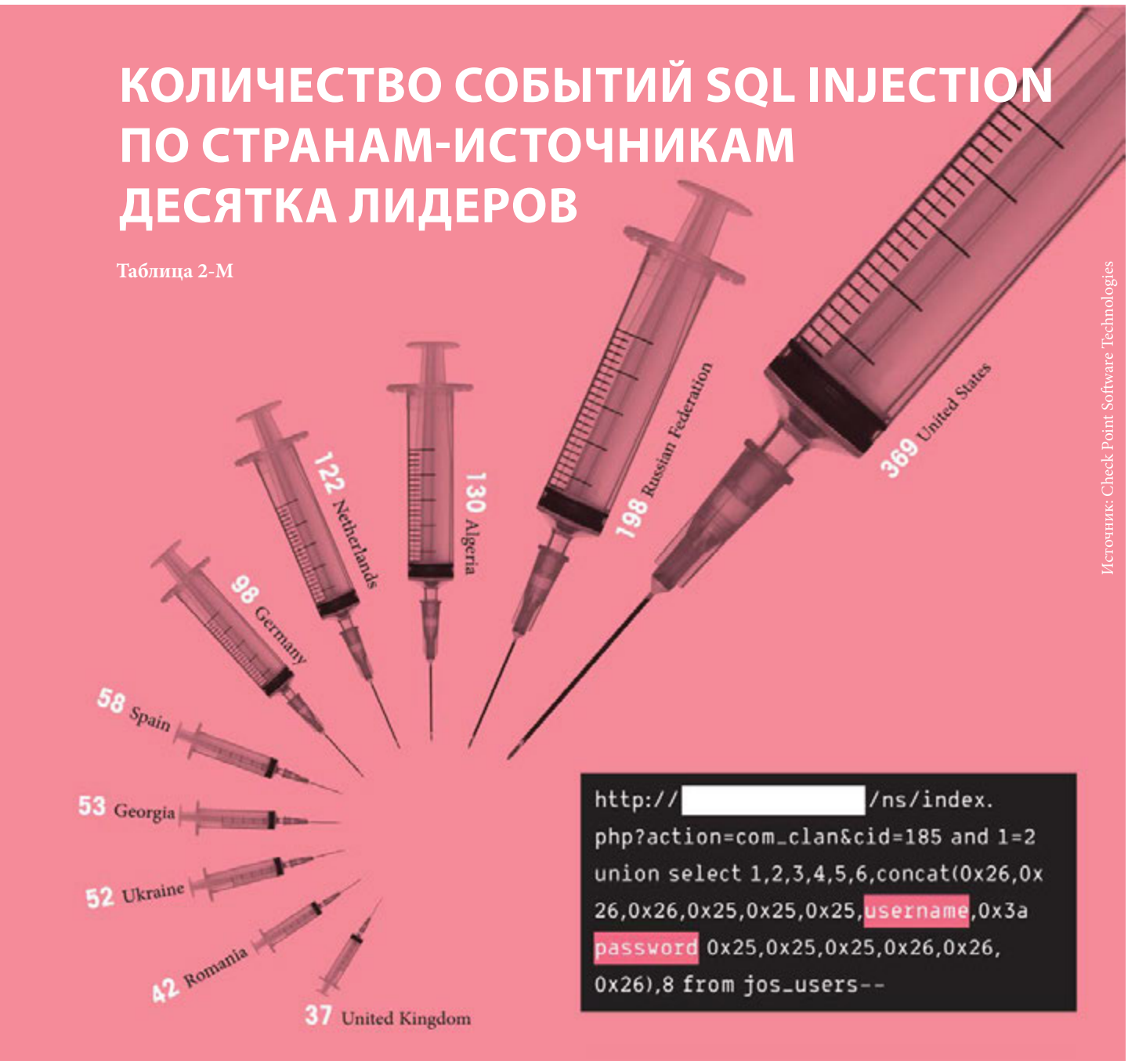


Таблица 2-L

КОЛИЧЕСТВО СОБЫТИЙ SQL INJECTION ПО СТРАНАМ-ИСТОЧНИКАМ ДЕСЯТКА ЛИДЕРОВ

Таблица 2-М



Источник: Check Point Software Technologies

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ МНОГОСЛОЙНАЯ БЕЗОПАСНОСТЬ

Угрозы становятся все более и более изощренными и вызовы ИБ продолжают расти. Для улучшения ИБ организации необходимо применять многоузловой защитный механизм для обороны от различных векторов сетевых угроз и взломов:

- Антивирус для выявления и блокировки вредоносного ПО;
- Анти-бот для обнаружения и предотвращения ущерба, наносимого ботами;
- Система предотвращения вторжения (IPS) для проактивного предотвращения вторжений;
- Контроль веб — фильтрация URL и контроль приложений для предотвращения доступа к сайтам с размещенным/распространяемым вредоносным ПО;
- Анализ состояния ИБ в реальном времени и глобальное сотрудничество;
- Интеллектуальный мониторинг и проактивный анализ данных.

Остановить входящие вредоносные файлы

Организации необходимо решение против вредоносного ПО, способное сканировать входящие файлы в сети и в реальном времени определять,

2012, ГОД ХАКТИВИЗМА

В 2012 году нестабильность мировой политической ситуации, начавшаяся в 2010 году с восстаний в арабском мире, продолжилась в виде различных гражданских протестов в других странах. Не удивительно, что одновременно мы наблюдаем и рост кибератак по политическим причинам.

Базирующаяся на Тайване компания Foxconn, являющаяся поставщиком компании Apple, подверглась хакерским атакам со стороны группы, именующей себя Swagg Security. Эта группа протестовала, по сообщениям СМИ, против плохих условий работы на фабриках по производству электроники в Китае[14].

Группа хактивистов Anonymous заявила о взломе веб-сервера Бюро по юридической статистике Министерства Юстиции США и опубликовала 1.7 Гб украденных данных. Группа выпустила заявление по поводу публикации этих данных: «Мы обнародовали эти данные для того, чтобы положить конец существующей коррупции и действительно освободить тех, кто угнетаем».[15]

Ватикан также обнаружил, что его веб-сервера и внутренние почтовые сервера подвергались более чем недельной атаки со стороны группы Anonymous. Группа заявила, что эта акция была вызвана тем, что Радио Ватикана имеет мощные передатчики в сельских районах за чертой Рима, которые представляют угрозу для здоровья. Группа заявила, что передатчики предположительно вызывают «лейкемию и рак» у людей, проживающих поблизости. Также группа оправдывала свои действия тем, что Ватикан, якобы, помогал нацистам, уничтожал книги, представляющие историческую ценность, а также тем, что некоторые клирики замешаны в сексуальных домогательствах к малолетним[16].

В ходе еще одной своей атаки группа Anonymous вывела из строя веб-сервера торговых групп U.S. telecom Association и TechAmerica. Эти атаки были проведены потому, что данные компании поддерживали Билль о кибербезопасности, предложенный республиканцем Майком Роджерсом (Mike Rogers). Этот законопроект позволял бы частным компаниям и государству делиться любой информацией «напрямую имеющей отношение к уязвимостям или угрозам» компьютерным сетям[17].

заражены ли они вредоносным ПО. Такое решение должно препятствовать вредоносным файлам заражать внутреннюю сеть, а также предотвращать доступ к вебсайтам, зараженным вредоносным ПО, который может привести к выполнению загрузки «drive-by».

Многоуровневая защита от ботов

Защита от ботов состоит из двух фаз: обнаружения и блокирования.

Для увеличения вероятности обнаружения бота в сети необходим многоуровневый механизм обнаружения, покрывающий все аспекты поведения бота. Решение для обнаружения ботов должно включать репутационный механизм, обнаруживающий IP адреса, URL и DNS адреса, используемые удаленными операторами для соединения с ботами. Также чрезвычайно необходимо, чтобы защита включала в себя возможность обнаружения уникальных шаблонов и протоколов для каждого семейства ботнетов. Другой критичной функцией системы защиты от ботов является определение активности ботов. Решение должно иметь возможность идентифицировать такие активности ботов как рассылка спама, подделка кликов, и самораспространение.

Второй фазой защиты, после обнаружения зараженных машин, является блокирование исходящих соединений ботов с серверами управления. На этом этапе нейтрализуются угрозы и устанавливается, что агенты ботов не могут отослать важную информацию или получить дальнейшие инструкции для вредоносных действий. Таким образом, исключается ущерб, связанный с ботами. Этот подход позволяет организациям поддерживать непрерывность бизнеса — пользователи могут нормально работать, не вдаваясь в детали блокировки обмена информацией с ботами, и организация, таким образом, становится защищенной без снижения производительности.

Глобальное сотрудничество в реальном времени

Проблема кибератак слишком велика для решения в рамках одной организации. Организации имеют

лучшие шансы ответить на все возрастающие вызовы, используя сотрудничество и профессиональную помощь. Наряду с тем, что киберпреступники делают упор на использование вредоносного ПО, ботов и других форм современных угроз, они часто выбирают в качестве своих целей несколько точек и организаций, чтобы увеличить вероятность успешной атаки. Если организации борются с такими угрозами по одиночке, множество атак остается необнаруженными потому, что не существует эффективных путей обмена информацией об угрозах между корпорациями. Чтобы опередить современные угрозы, бизнесы должен сотрудничать между собой и обмениваться данными об угрозах. Только сообща они смогут сделать ИБ сильнее и эффективнее.

Предотвращение вторжений

Системы предотвращения вторжений (Intrusion Prevention Systems — IPS) являются обязательным элементом противодействия различным векторам атак. Решения IPS необходимо для проведения глубокой инспекции трафика в целях предотвращения враждебных попыток взлома системы безопасности и получения доступа к данным организации. Адекватное решение IPS должно обладать следующим функционалом:

- Проверка протоколов и обнаружение аномалий — для идентификации и предотвращения трафика, не соответствующего стандартам протоколов и могущего вызывать некорректную работу устройств или проблемы безопасности.
- Предотвращение пересылки неизвестного содержимого поля данных (payload), способного эксплуатировать специфические уязвимости.
- Предотвращение избыточного объема обмена информацией, который может быть признаком атаки «отказ в обслуживании» (DoS).

Видеть картину угроз и принимать ответные меры

Ясная картина событий и тенденций ИБ является еще одним важным компонентом борьбы с киберпреступниками. Администратор ИБ должен иметь постоянное и четкое знание текущего состояния ИБ сети для понимания угроз и атак, направленных против организации. Такое понимание требует решение ИБ, которое предоставляло бы высокоуровневый обзор ИБ и выделяло бы критичную информацию и потенциальные атаки. Решение также должно предоставлять возможность проведения расследований отдельных инцидентов. Возможность предпринимать немедленные действия на основании полученной информации — еще одно важное свойство, позволяющее предотвращать атаки в реальном времени или проактивно блокировать будущие угрозы. Решения ИБ должно иметь гибкое и интуитивное управление для упрощения анализа угроз и снижения операционной нагрузки и расходов.

Обновления безопасности и поддержка

В условиях постоянно меняющихся угроз меры защиты также должны изменяться в соответствии с угрозами, и даже опережать их. Продукты ИБ могут эффективно бороться с последним вредоносным ПО, уязвимостями и эксплойтами только в том случае, если производитель решений ИБ способен проводить комплексные исследования и предоставлять регулярные обновления средств ИБ.

Хороший сервис ИБ базируется на:

- Внутренних исследованиях производителя и использовании данных из нескольких источников;
- Регулярных обновлениях ИБ по всем соответствующим технологиям, включая системы предотвращения вторжений, антивирус и анти-бот;
- Простой и удобной системе поддержки, способной дать ответы на вопросы и запросы с учетом специфики заказчика.

03 ПРИЛОЖЕНИЯ В РАБОЧЕМ ПРОСТРАНСТВЕ ОРГАНИЗАЦИИ

Правила игры поменялись

Правила игры поменялись. Интернет приложения, которые когда-то рассматривались как способ времяпровождения или средство посмотреть фотографии из недавнего путешествия Вашего друга, с приходом Web 2.0 превратились в мощный инструмент ведения бизнеса современного предприятия. Мы общаемся с коллегами, заказчиками и партнерами, мы делимся информацией с другими людьми, мы получаем новости, мнения и точки зрений. Интернет ресурсы такие как, например, Facebook, Twitter, WebEx, LinkedIn, YouTube становятся все более и более распространенными на предприятиях и признаются ими как средства ведения бизнеса.

В этой части нашего исследования мы обсудим общие риски, привнесенные приложениями Web 2.0 и их инфраструктурой, ставя фокус на специфических приложениях, обнаруженных в организациях во время нашего исследования. Наши находки мы проиллюстрируем на примере реальных инцидентов.

Веб-приложения — это не игра.

Изменения технологии бросают новые вызовы ИБ. Интернет приложения также добавляют новые ИБ риски. Большое количество Интернет приложений используются как инструменты атак против организаций или приводят к взлому сетевой безопасности. Такие приложения, как анонимайзеры, хранилища данных и общий доступ, обмен файлами в пиринговых (P2P) сетях, инструменты удаленного администрирования и социальные средства коммуникации — все это используется для проникновения в организации.

Существует великое множество платформ и приложений, которые могут использоваться в личных целях или для бизнеса. Каждая организация должна знать, какие приложения используют ее сотрудники и для каких целей, и на основании этого определять свою политику использования Интернета.

Были получены данные, что в 91% организаций пользователи используют приложения, способные обходить механизмы защиты, скрывать идентификационные параметры, что может привести к утечке данных или даже к заражению вредоносным ПО без ведома самих пользователей.

ВАЖНАЯ ИНФОРМАЦИЯ РАСПРОСТРАНЯЛАСЬ В ФАЙЛООБМЕННЫХ P2P СЕТЯХ – ПРИЛОЖЕНИЯ ДЛЯ ОБМЕНА ДАННЫХ В США

В июне 2012 года Федеральная комиссия по торговле США (Federal Trade Commission, FTC) предъявила обвинение двум организациям за размещение конфиденциальной информации в файлообменных пиринговых сетях, что ставило под угрозу тысячи потребителей. FTC установила, что одна из организаций, ERN, Inc., занимающаяся сбором задолженностей, выложила на компьютер, подключенный к пиринговой сети конфиденциальную информацию, включавшую номера социального страхования, номера полисов медицинского страхования и коды медицинских диагнозов более чем 3800 пациентов больницы. Также FTC заявила, что другая организация — автодилер Franklin's Budget Car Sales, Inc., выложила в пиринговую сеть информацию о 95000 клиентах. Информация содержала имена, адреса, номера социального страхования, даты рождений и номера водительских удостоверений[18].

В 2010 году FTC оповестила около 100 организаций о том, что персональная информация, включая конфиденциальные данные о клиентах и/или сотрудниках, была выложена из их информационных систем через пиринговые (P2P) файлообменные сети. Любой пользователь таких сетей мог использовать эти данные для совершения кражи идентификационной информации и подлога[19].

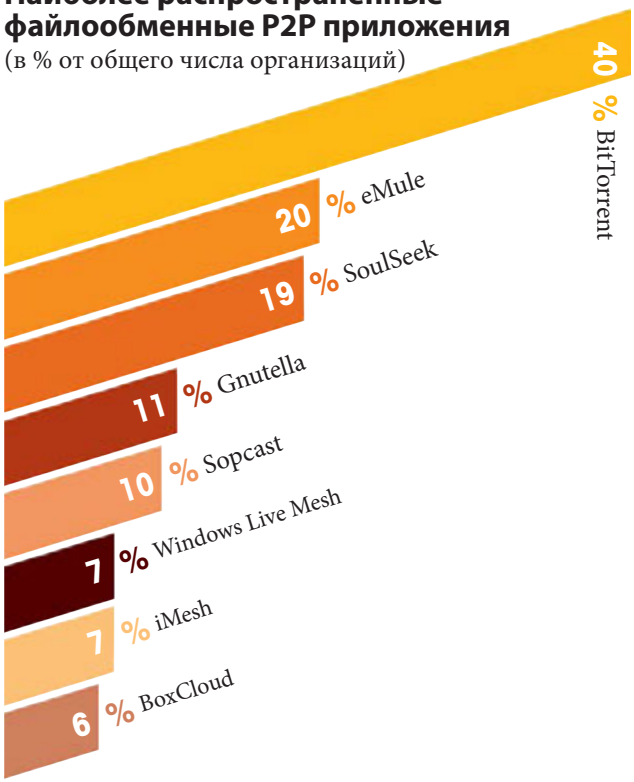
В 61 % ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТСЯ ПРИЛОЖЕНИЯ ДЛЯ ПИРИНГОВОГО ФАЙЛООБМЕНА

P2P приложения — открытая дверь в Вашу сеть

Пиринговые (Peer-to-Peer, P2P) приложения используются для обмена файлами между пользователями. P2P приобретают все большую популярность у атакующих, как средство распространения вредоносного ПО среди обмениваемых файлов. P2P приложения по сути являются открытым «черным ходом» в сеть. Они позволяют пользователем разделять доступ к папкам, что может привести к утечке конфиденциальной информации, они также могут сделать организации ответственными за нелегальное приобретение пользователями фильмов, музыки или ПО через сети P2P. Мы наблюдаем высокую популярность использования P2P сетей, — в нашем исследовании свыше половины (61%) организаций использовали P2P приложения. Наиболее распространенным ПО для P2P обмена файлами были клиенты BitTorrent. С точки зрения местонахождения, нижеприведенная диаграмма показывает, что в Азиатско-Тихоокеанском регионе P2P сеть пользуются большей популярностью, чем в других частях земного шара.

Наиболее распространенные файлообменные P2P приложения

(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица 3-A

Дополнительную информацию по P2P приложениям – см. Приложение B.

Использование файлообменных P2P приложений по регионам

(в % от общего числа организаций)

Источник: Check Point Software Technologies

Таблица 3-B

Приложения анонимайзеров обходят политики безопасности организаций

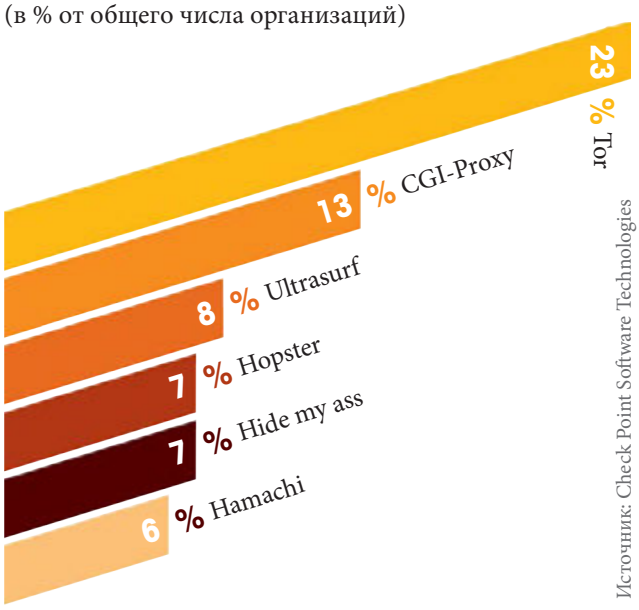
Анонимайзер (или анонимный прокси) — это инструмент, с помощью которого пользовательская активность в Интернете может быть сделана неотслеживаемой. Приложение-анонимайзер использует прокси-сервер, действующий как маска приватности между клиентским компьютером и Интернетом. Оно осуществляет доступ в Интернет от лица пользователя, скрывая персональную

информацию путем скрытия идентификационных данных компьютера клиента и конечной точки, которую пользователь пытается достичь. Приложения-анонимайзеры могут использоваться для обхода политик безопасности, особенно построенных на использовании идентификаторов пользователей и конечных URL/сайтов. Используя анонимайзеры, пользователь представляется кем-то, использующим другой IP адрес и запрашивающим доступ к другому ресурсу, так что политика не может быть применена в случае измененного IP адреса пользователя и измененного конечного адреса назначения. В отдельных случаях анонимайзеры могут использоваться для сокрытия преступных действий.

В ходе нашего исследования было выявлено, что в 43% организаций работник использовал хотя бы один анонимайзер, из которых наиболее распространенным был Tor. В 86% организаций, в которых декларировалась недопустимость использования анонимайзеров, таковые использовались вопреки инструкциям и политикам безопасности. Если мы посмотрим на использования приложений-анонимайзеров по регионам, мы увидим, что наиболее популярными они являются в Америке и немного менее — в Азиатско-Тихоокеанском регионе.

Наиболее распространенные анонимайзеры

(в % от общего числа организаций)



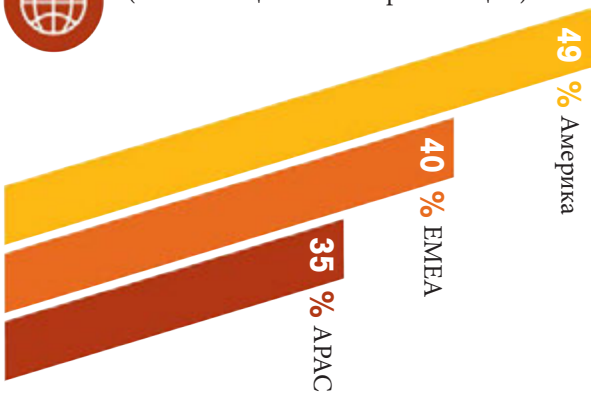
Источник: Check Point Software Technologies

Таблица 3-C

Дополнительную информацию по анонимайзерам – см. Приложение B.

Использование анонимайзеров по регионам

(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица 3-D

Как работает анонимайзер Ultrasurf?

Ultrasurf представлет собой технически очень совершенный анонимайзер, работающий как прокси-клиент, создающий зашифрованный HTTP туннель междукомпьютеромпользователяицентральнымпулом прокси-серверов, позволяя пользователям обходить межсетевые экраны (МСЭ) и цензуру. Ultrasurf имеет очень надежный механизм по поиску прокси серверов, включая кэш-файл IP адресов прокси-серверов, DNS запросов, которые возвращают закодированные IP адреса прокси-серверов, зашифрованные документы в среде Google Docs и встроенный в программу жестко-запрограммированный список IP адресов прокси-серверов. Эти технологии делают анонимайзер трудным для обнаружения устройствами безопасности.

В 43% ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТСЯ АНОНИМАЙЗЕРЫ

АНОНИМАЙЗЕР TOR ПОДРЫВАЕТ БЕЗОПАСНОСТЬ

Недавно проведенные исследования выявили ботнет, управление которым осуществлялось атакующими с использованием IRC сервера, запущенного как скрытый сервис внутри анонимизирующей сети Tor. Соединения между пользователями Tor узлов многослойно зашифрованы, что делает задачу слежения за конечным адресом запроса пользователя[20] чрезвычайно трудной как на уровне локальной сети, так и на уровне ISP. Основной целью сети Tor (также известной под именем Onion Router) является обеспечение анонимности при просмотре Интернета. Несмотря на высокую популярность и хороший уровень поддержки, при использовании в корпоративных средах Tor создает определенные проблемы в безопасности. Он может быть легко использован для обхода политик безопасности предприятия, так как специально спроектирован для создания анонимности своим пользователям. При использовании Tor для просмотра ресурсов сети Интернет, запросы, посылаемые с пользовательского компьютера, случайным образом маршрутизируются через цепочку узлов, добровольно поддерживаемых другими пользователями сети Tor.

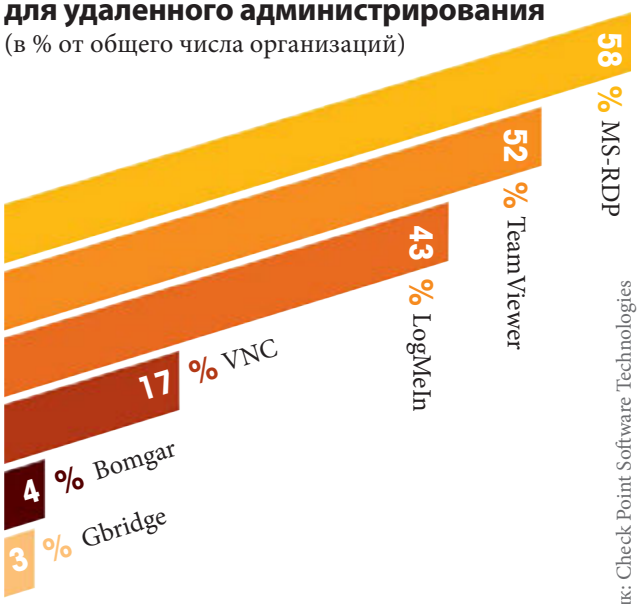
81% ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Средства удаленного администрирования используются для вредоносных атак

Средства удаленного администрирования (Remote Administration Tools, RAT) могут являться разрешенным ПО, когда они используются администраторами или сотрудниками технической поддержки. Однако, некоторые атаки в последние годы использовали RAT для управления зараженными машинами, для дальнейшего проникновения в сеть, журналирования нажатий клавиш или для кражи конфиденциальной информации. Так как утилиты удаленного управления представляют собой весьма необходимый элемент бизнес-процесса, они не должны блокироваться на периметре; однако их использование должно мониториться и находиться под контролем для предотвращения потенциального нелегитимного использования.

При рассмотрении организаций в нашем исследовании мы нашли, что 81% из них использует как минимум один тип ПО удаленного администрирования, из которых самым распространенным является Microsoft RDP.

Наиболее распространенные приложения для удаленного администрирования
(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица 3-F

Дополнительную информацию по приложениям для удаленного администрирования – см. Приложение В.

ВЗЛОМАН С ПОМОЩЬЮ СРЕДСТВ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

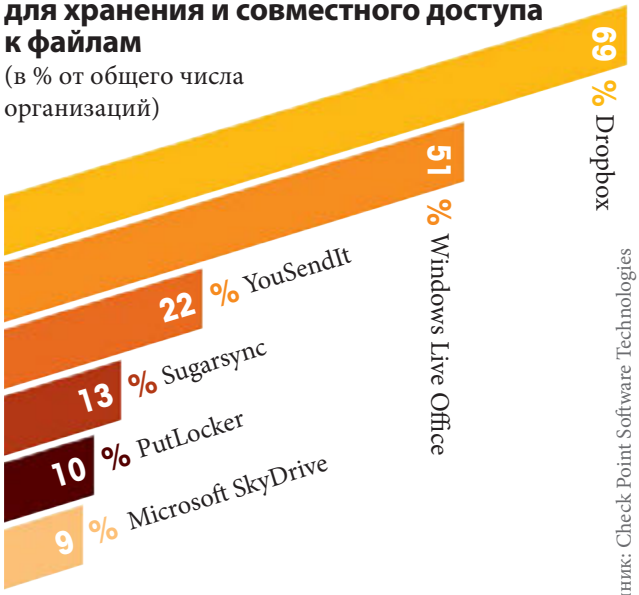
С июля по сентябрь 2011 года была проведена серия атак под названием: «Nitro». Атакующие использовали готовую утилиту удаленного доступа Poison Ivy для вынюхивания секретов около 50 компаний, в основном химической или оборонной сферы. Poison Ivy было внедрено на ПК с ОС Windows, чьи владельцы стали жертвами рассылки вредоносных спам-сообщений электронной почты. В этих сообщениях содержались запросы на встречи от уважаемых бизнес-партнеров или, в некоторых случаях, обновления антивирусного ПО или Adobe Flash Player. Когда пользователи открывали приложение к письму, незаметно для самих себя они устанавливали на свои машины Poison Ivy. После этого атакующие могли выдавать зараженным компьютерам команды, искать высокоуровневые пароли для получения доступа к серверам, содержащим конфиденциальную информацию, и, в конце концов, пересылать информацию на системы, контролируемые хакерами. 29 из 48 успешно атакованных фирм были химическими компаниями и компаниями по продаже передовых материалов, применяемых на военных транспортных средствах, а другие 19 — представляли различные сектора экономики, включая оборонный. Нитро не является единственным в своем роде случаем нецелевого использования средств удаленного администрирования. Другими примерами могут служить взлом RSA, SandyRAT и Operation Aurora. Во всех указанных случаях использовалась утилита Poison Ivy.

«Поделиться» — не всегда значит «позаботиться»

Когда мы делимся чем-либо с другим человеком, это означает, что мы проявляем о нем заботу. Однако, это не всегда означает то же самое, когда кто-то пользуется приложениями по хранения и совместному доступу к файлам. Одной из отличительных черт Web 2.0 является возможность генерации контента и его совместное использование. Однако это несет в себе определенный риск. При совместном использовании файлов конфиденциальная информация может попасть в чужие и нежелательные руки. Наше исследование включало в себя приложения по хранению и совместному использованию файлов высокого риска, использование которых могло бы привести к утечке данных или заражению вредоносным ПО без ведома пользователя. Наше исследование показало, что 80% организаций имеют хотя бы одно хранилище файлов или приложение по совместному использованию файлов в своих сетях. Было найдено, что 69% инцидентов было результатом использованием сервиса Dropbox. На втором месте — Windows Live Office с 51%.

Наиболее распространенные приложения для хранения и совместного доступа к файлам

(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица 3-D

Дополнительную информацию по анонимайзерам – см. Приложение B.

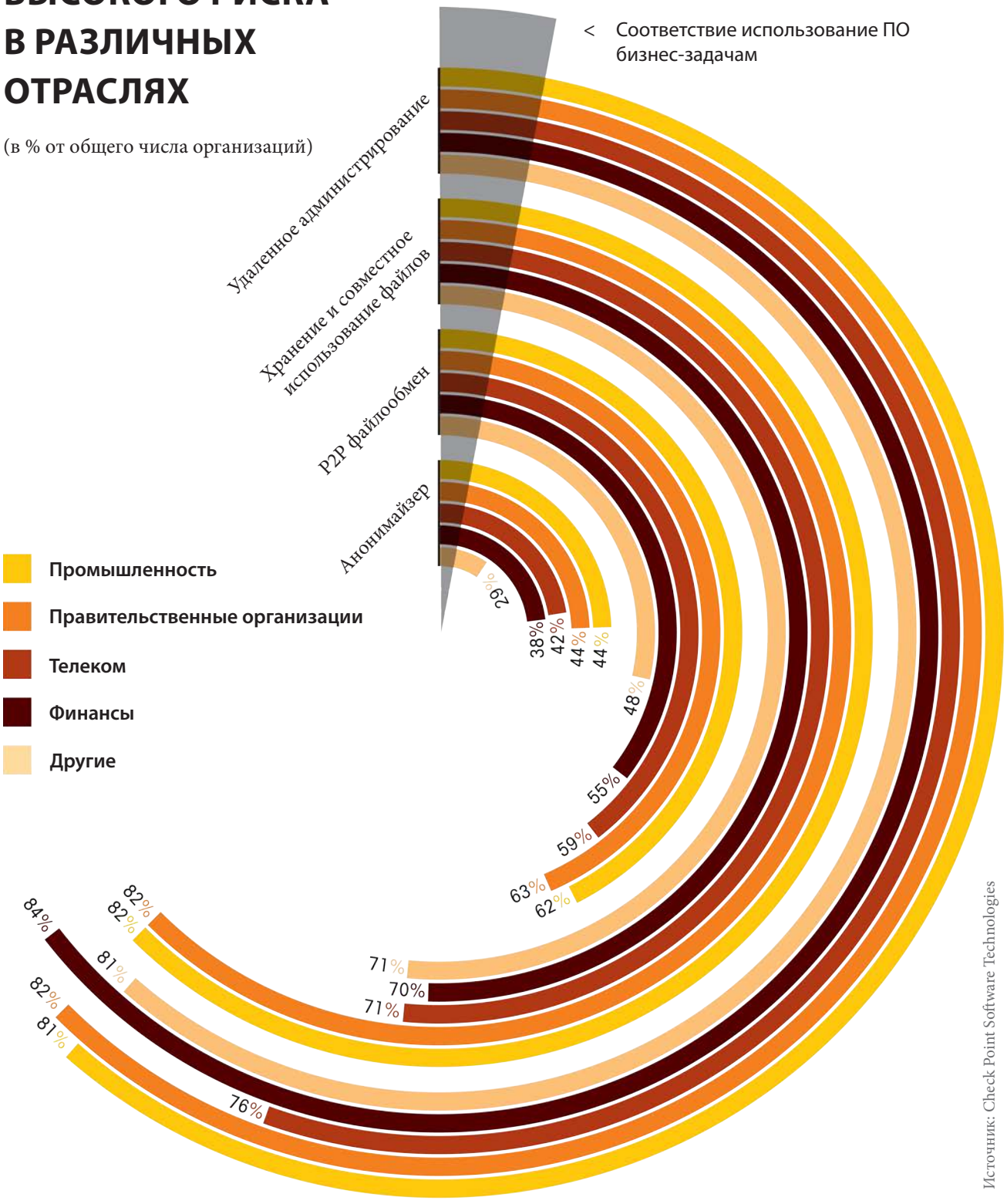
81% ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ **СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ**

Приложения высокого риска: их использование в различных отраслях

Check Point проанализировала использование приложений высокого риска с точки зрения применения их в различных отраслях экономики. В Таблице 3-E показано, что организации Промышленного сектора и Правительственные организации наиболее широко используют такие приложения. Существуют случаи, когда использование таких приложений может быть легитимным в такой организации, например, использование утилит удаленного администрирования в службе технической поддержки, в этом случае горизонтальный столбик диаграммы показывает вероятность того, что данное ПО используется в бизнес среде легитимно.

ПРОЦЕНТ ИСПОЛЬЗОВАНИЯ ПРИЛОЖЕНИЙ ВЫСОКОГО РИСКА В РАЗЛИЧНЫХ ОТРАСЛЯХ

(в % от общего числа организаций)



Источник: Check Point Software Technologies

DROPBOX: ДВА СЕРЬЕЗНЫХ ИНЦИДЕНТА БЕЗОПАСНОСТИ ЗА 2 ГОДА

В июле 2012 года на пользователей сервиса Dropbox была совершена атака. Имена пользователей Dropbox и их пароли были раскрыты в результате взлома другого веб-сайта, который тестировался на учетных записях Dropbox. Хакеры использовали украденные пароли для подключения к учетной записи сотрудника в сервисе Dropbox, который содержал файл с адресами электронной почты пользователей. Затем злоумышленники использовали эти адреса для рассылки спама[22].

Этот инцидент иллюстрирует тактику, наиболее часто используемую хакерами. Довольно часто хакеры крадут имена пользователей и пароли к сайтам, которые, на первый взгляд, не содержат значимой финансовой или персональной информации. Затем они проверяют эти учетные записи на различных веб-сайтах финансовых организаций, брокерских аккаунтах или, например, аккаунтах Dropbox, то есть там, где потенциально может содержаться ценная информация.

В 2011 году ошибка в обновлении ПО Dropbox сделала возможным ситуацию, когда любой пользователь мог войти в любой аккаунт Dropbox, если он знал адрес электронной почты владельца аккаунта. Этот дефект ПО открыл путь к документам и информации пользователей, пользующихся системой совместного доступа. Проблема была решена за несколько часов после получения оповещения от пользователей и компаний, чьи сотрудники использовали системы совместного хранения и доступа к файлам, такие как Dropbox и Google Docs, для хранения важной корпоративной информации[23].

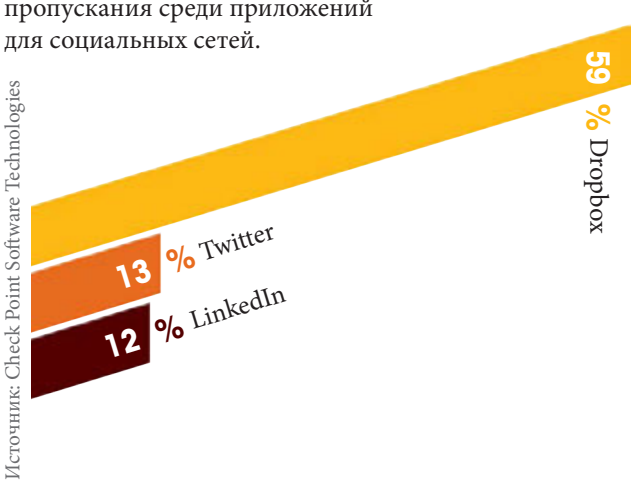
Легитимная запись Facebook или вирус?

С постоянным ростом популярности социальных сетей организации сталкиваются с новыми вызовами ИБ. Нечаянно размещенная в социальной сети важная проектная информация может нанести ущерб репутации организации, привести к утрате конкурентных преимуществ или финансовым потерям. Хакеры широко применяют новые технологии социальной инженерии для развития активности ботнетов. Вложенные видео или ссылки на страницы социальных сетей становятся популярными местами, куда хакеры встраивают вредоносное ПО. Помимо рисков ИБ, приложения социальных сетей создают серьезную проблему при использовании полосы пропускания. Facebook, несомненно, является наиболее посещаемой социальной сетью. Другие социальные сети, посещаемые сотрудниками в течение рабочего времени (но в гораздо более скромных масштабах, чем Facebook) — Twitter и LinkedIn.

Ссылка в Facebook, ведущая на вредоносный сайт:

Потребление полосы пропускания приложениями социальных сетей

Средние значения используемой полосы пропускания среди приложений для социальных сетей.



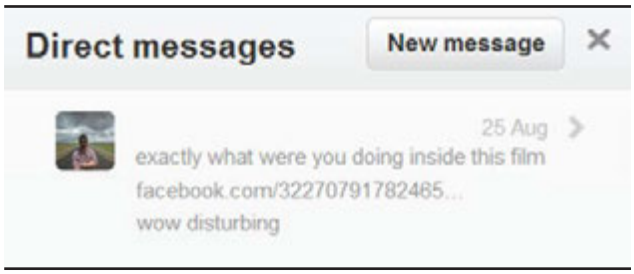
Источник: Check Point Software Technologies

Таблица 3-H

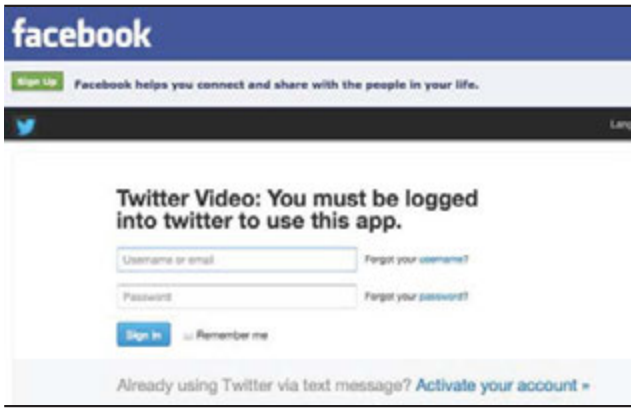
Примеры атак социальной инженерии.

Недавние атаки показали, что хакеры, при формировании каналов распространения вредоносного ПО, сместили акцент с электронной почты на социальные сети. Нижеприведенный пример основан на реальной атаке, проведенной в августе 2012 года. Хакеры использовали приемы социальной инженерии в Twitter и Facebook для распространения вредоносного контента. Используя

взломанную учетную запись Twitter, хакер послал личные сообщения всем последователям (followers) ее владельца. В сообщении значилось: «точно то, что ты делал в этом фильме [Facebook URL]… вау, волнующе».



URL ссылался на приложение в Facebook, которое запрашивало ввода учетных данных Twitter. Страница запроса этих данных располагалась на сервере, которым владел хакер и использовал его для сбора «урожая» учетных записей Twitter получателей этого сообщения.



Используя эти учетные записи Twitter, хакер мог повторить те же действия с другим взломанным аккаунтом, чтобы собрать еще больше паролей. Злоумышленник, затем, мог использовать украденные учетные данные для доступа к другим сервисам, таким как Gmail, Facebook и т. п., или, что хуже, использовать их для доступа к банковским счетам или даже бизнес-приложениям, таким как SalesForce или другим.

После того, как вредоносное сообщения было вторично распространено (в этот раз уже последователями того пользователя взломанного аккаунта), единственной эффективной мерой противодействия оставалось размещения объявления с извинениями.

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ВЕБ-ПРИЛОЖЕНИЙ В ВАШЕЙ СЕТИ

Как установить эффективную защиту приложений Web 2.0?

Первым шагом в обеспечении безопасности веб-приложений в организации должно стать использование решения, предоставляющего контроль и управление всеми аспектами использования веб-ресурсов. Необходима полная прозрачность всех приложений, использующихся в среде, наряду с возможностью ограничения их использования. Такой контроль должен быть установлен как над клиентскими приложениями (как, например, Skype), так и над более традиционным способом использования ресурсов веб — URL. Так как многие сайты (такие как Facebook) используют многочисленные приложения, основанные на URL, представляется необходимым иметь детальный контроль на уровне URL — например, выделять Facebook chat или игровые приложения. После этого организация сможет легко блокировать приложения, угрожающие ее безопасности.

Использование социальных сетей для бизнеса

Отдельные организации предпочитают полностью блокировать Facebook, однако для многих других эта социальная сеть является важных инструментом их бизнеса. Компании часто публикуют там информацию о будущих мероприятиях, вебинарах, информацию о последних версиях и продуктах, ссылки на интересные статьи и видео.

Каким образом можно разрешить использование социальных сетей в организации, не нанося ущерб безопасности? Этого можно достичь, внедряя контроль за функционалом и виджетами в приложениях и платформах и имея возможность разрешить использование Facebook, в то же время блокируя те его части, которые не относятся к данному бизнесу. Таким образом, можно сделать использование социальных сетей приемлемым с точки зрения рисков ИБ.

Разные пользователи имеют разные потребности

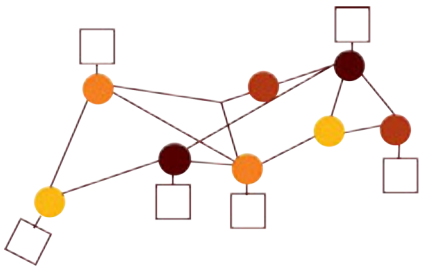
Разные пользователи в организации имеют различные потребности, поэтому политики безопасности должны поддерживать требования бизнеса, а не вступать с ними в конфликт. Например, менеджер по продажам может использовать Facebook, в то время как работник отдела IT должен пользоваться Facebook для получения свежих новостей индустрии. Каким образом мы можем быть уверенны в том, что пользователи получают доступ к необходимым ресурсам? Реально ли ожидать, что менеджер ИБ будет знать для каждого пользователя или группы пользователей список необходимых или запрещенных ресурсов?

Практическое решение должно включать механизмы гранулярного контроля по пользователям, группам и машинам для упрощения различения сотрудников от других пользователей (например, гостей и контрактных работников).

Другим важным аспектом является возможность обучать конечных пользователей и привлекать их внимание во время использования приложений. Когда пользователь посещает сомнительный сайт или запускает сомнительное приложение, во всплывающем окне можно выводить запрос на объяснение бизнес-необходимости этого действия, введенный ответ может журналироваться и мониториться, в то же время само сообщение проинформирует пользователя о политике использования приложений в бизнес-процессе и обратит его внимание на то, что использование таких приложений подвергается аудиту.

«Понимание» — это критический компонент веб-контроля

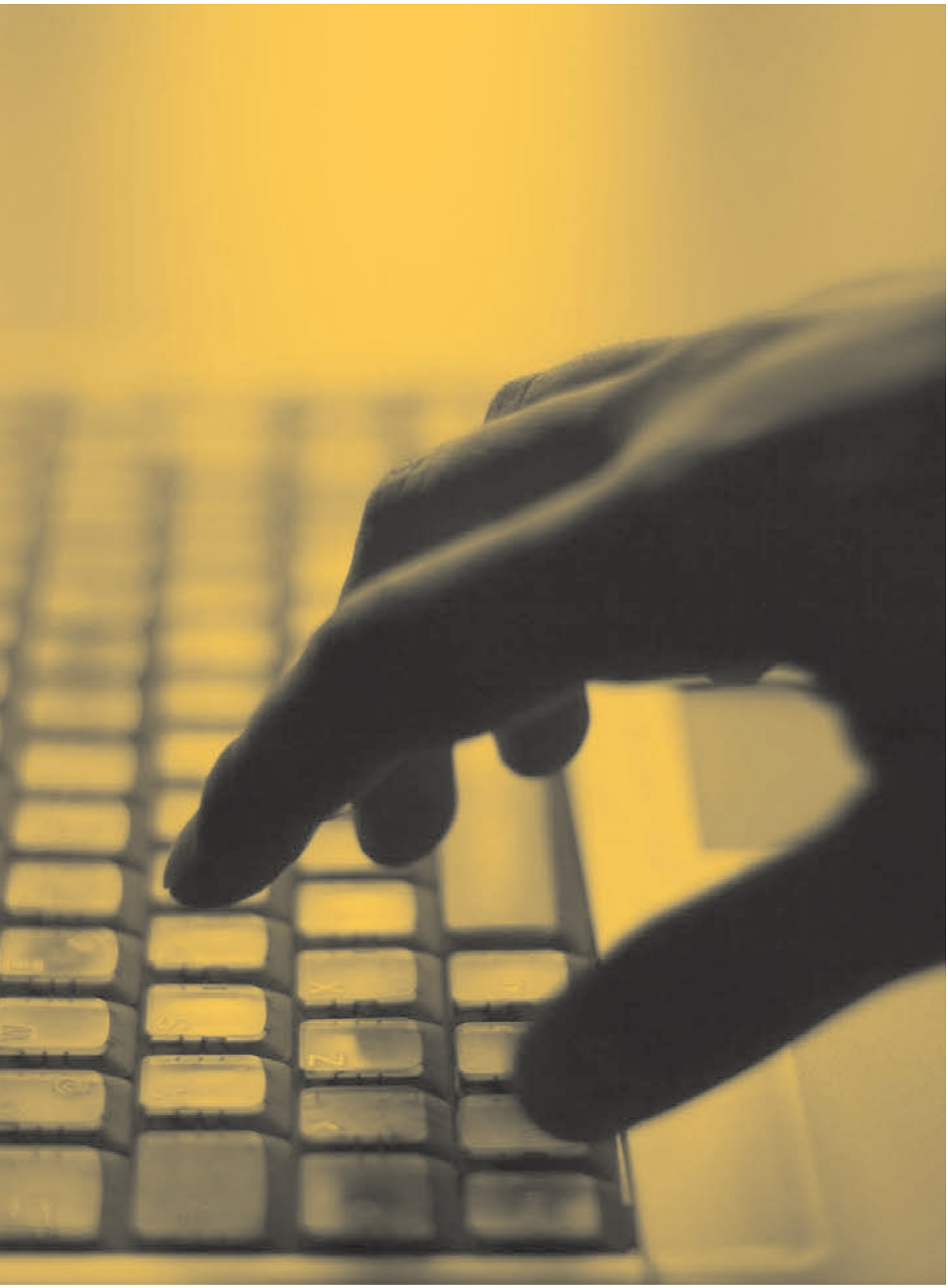
Администраторы должны располагать общей картиной событий веб-безопасности для обеспечения веб-контроля. Решение ИБ должно обеспечивать широкий обзор и четкую видимость всех событий веб-безопасности. Решение должно обеспечивать прозрачность и мониторинг с выполнением таких функций, как построение временной шкалы событий, фильтрации полного списка событий с их группировкой по пользователям, приложениям, категориям, уровням риска, используемой полосе пропускания, времени и т. д. Необходима также возможность создания отчетов в режиме оффлайн для выделения наиболее востребованных категорий, приложений, сайтов и пользователей, для выяснения тенденций использования и планирования мощностей.



ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WEB 2.0 ТРЕБУЕТ ИНТЕГРАЛЬНОГО ПОДХОДА С ФИЛЬТРАЦИЕЙ URL, КОНТРОЛЕМ ПРИЛОЖЕНИЙ, ОПОВЕЩЕНИЕМ И ОБУЧЕНИЕМ ПОЛЬЗОВАТЕЛЕЙ, А ТАКЖЕ ПОДДЕРЖАНИЕМ ВСЕГО ВЕБ-КОНТРОЛЯ ПРОЗРАЧНЫМ ДЛЯ АДМИНИСТРАТОРА

Заключение

Правила игры поменялись. Обеспечение безопасности Web 2.0 более не сводится к простой блокировке нежелательных URL. Это не просто предотвращение запуска приложения. Обеспечение безопасности Web 2.0 требует интегрального подхода многоуровневой зашиты: фильтрации URL, контроля приложений, защиты от вредоносного ПО, обучения пользователей, сложных инструментов мониторинга и анализа для постоянного поддержания контроля в руках администраторов.



04 ИНЦИДЕНТЫ ПОТЕРИ ДАННЫХ В ВАШЕЙ СЕТИ

Корпоративные данные: самый ценный актив организации

Корпоративные данные сегодня более доступны и перемещаемы нежели когда либо раньше, и большая часть из них представляет собой важную информацию различного уровня. Часть из них является конфиденциальной информацией только лишь потому, что включает в себя внутренние данные корпораций и не предназначена для публичного использования. Данные других типов могут быть важны в силу корпоративных требований, государственных законов или международных соглашений. Но в большинстве случаев значимость данных зависит от степени их конфиденциальности — мы имеем ввиду интеллектуальную собственность и конкурентную информацию.

На самом деле ситуация сложнее — наряду с серьезностью проблемы утечки данных, сегодня мы сталкиваемся с множеством методов и практик, делающих необратимую ошибку еще более вероятной: облачные сервера, система Google docs, и просто ненамеренные нарушения корпоративных процедур — например, в случае, если сотрудник взял работу на дом. Фактически, большинство инцидентов утечки данных представляют собой непредумышленные утечки.

Утечка данных может случиться с любым из нас

Утечка данных может произойти не только при вмешательстве киберпреступника, но также и непреднамеренно, по вине сотрудника. Конфиденциальный документ может быть по ошибке отослан не тому человеку, документ с важной информацией может быть выложен на общедоступный сайт, или рабочий файл может быть отослан на неавторизованный домашний адрес электронной почты. Все эти сценарии могут неожиданно случиться с каждым из нас и повлечь за собой разрушительные последствия. Потеря важных данных может привести к потере репутации, нарушению соответствия регулирующим документам, потере прибыли или даже серьезным штрафам.

Наше исследование

Когда организации необходимо определить, какие данные можно посылать вовне, в расчет должны приниматься многие параметры. Каков тип этих данных? Кто их владелец? Кто посылает их? Кто их

54%

ОРГАНИЗАЦИЙ В РАМКАХ НАШЕГО ИССЛЕДОВАНИЯ ИМЕЛИ ХОТЯ БЫ ОДИН ИНЦИДЕНТ, СВЯЗАННЫЙ С ПОТЕНЦИАЛЬНОЙ ПОТЕРЕЙ ДАННЫХ

ООПС… Я ПОСЛАЛ ПОЧТУ ПО ОШИБОЧНОМУ АДРЕСУ

Приведем некоторые примеры происшедших в 2012 году инцидентов, связанных с потерей данных из-за ненамеренных действий сотрудников:

В октябре 2012 года **Городской совет г. Сток-он-Трент** (Stoke-on-Trent City Council) в Соединенном Королевстве был оштрафован на 120000 фунтов стерлингов после того, как сотрудник юридического отдела отправил сообщения электронной почты, содержащие важную информацию, на неправильный адрес. Одиннадцать сообщений предназначались адвокату, работающему над одним делом, и в результате опечатки при наборе были отосланы по другому адресу.

Японская газета **Йомиури Симбун** (Yomiuri Shimbun) в октябре 2012 года уволила одного из своих репортеров за то, что он случайно отослал по неверному адресу важные материалы расследования. Репортер намеревался отослать по электронной почте своим коллегам некоторые обнаруженные данные, но вместо этого письма ушли некоторым новостным агентствам, что привело к раскрытию источников информации[24].

В апреле 2012 года, **Военный Институт в Вирджинии** (Virginia Military Institute) в Лексингтоне неосторожно отослал средние оценки своих студентов как приложения к сообщениям электронной почты. Письмо было послано президенту выпускного класса и содержало таблицу со средними оценками каждого старшекурсника. Не заметив приложения, президент затем переслал сообщение другим 258 студентам. Первоначальным его замыслом было просто отослать таблицу с именами и адресами студентов, чтобы они подтвердили свой почтовый адрес[25].

Техасский Университет A&M (Texas A&M University) случайно послал сообщение электронной почты с приложением, содержащим номера социального страхования, имена и адреса 4000 бывших студентов человеку, который сообщил, затем, об этом в университет. Инцидент имел место в апреле 2012 года[26].

предполагаемый получатель? Когда они посылаются? Каковы потери в случае, если бизнес-процесс будет прерван из-за чрезмерно строгих правил безопасности? В рамках нашего исследования мы проанализировали трафик, посылаемый изнутри организации вовне. Был рассмотрен как SMTP, так и HTTP трафик. Например, в случае, если сообщения электронной почты посылались внешним получателям, устройство Check Point инспектировало тело сообщения, электронные адреса получателей и приложения к сообщению (в том числе и сжатые). Мы также просматривали активность браузеров на предмет веб-постов или веб-электронной почты. В качестве политик безопасности на этих устройствах мы сконфигурировали стандартные предопределенные типы данных для обнаружения важной информации, формы и шаблоны (такие как номера кредитных карт, исходный код, финансовые данные и т. д.), которые могли бы обозначить потенциальную утечку данных, при попадании в чужие руки. Детальный список таких данных приведен в Приложении D.

Потенциальные потери данных в Вашей организации

В ходе нашего исследования мы обнаружили, что 54% организаций имели хотя бы один инцидент, который

Наиболее распространенные приложения для хранения и совместного доступа к файлам

(в % от общего числа организаций)

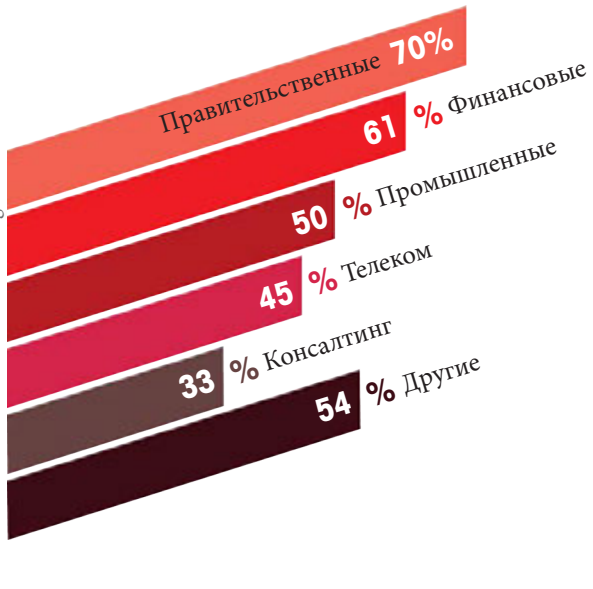
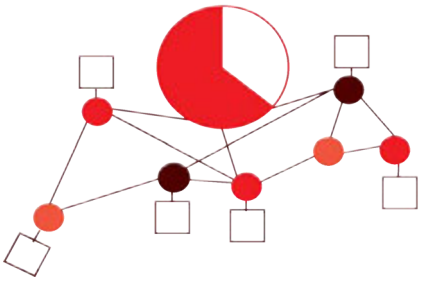


Таблица 4-A

мог бы означать потенциальную потерю данных за период, в среднем, 6 дней. Мы принимали во внимание события, влючавшие в себя внутреннюю информацию (полный список — см. Приложение D), посланную на внешний ресурс, было ли это отсылкой на внешний адрес электронной почты или онлайн-постинг.
Наше исследование показало, что государственные и финансовые организации имеют больший риск потенциальной потери данных (см. Таблицу 4-A).

В 28% ОРГАНИЗАЦИЙ ОБНАРУЖЕНО, ЧТО ВНУТРЕННЯЯ ЭЛЕКТРОННАЯ ПОЧТА БЫЛА ОТОСЛАНА ВНЕШНЕМУ ПОЛУЧАТЕЛЮ



Внутренняя почта, посланная за пределы организации

Во многих случаях потеря данных случается непреднамеренно, из-за того, что сотрудник посылает почту по ошибочному адресу. В нашем исследовании мы рассматривали два типа таких случаев с электронной почтой. Первый тип состоит из почтовых сообщений, посланных внутренним получателям в видимых полях (To и CC) и внешним получателям в скрытом поле BCC. Такие сообщения электронной почты в подавляющем большинстве случаев, смотрелись как внутренние, но, на самом деле, ушли за пределы компании. Ко второму типу относятся сообщения, посланные нескольким внутренним получателям и одному внешнему. Такие сообщения чаще всего посылались в адрес внешнего получателя ненамеренно. Один или оба типа событий, описанных выше, были обнаружены в 28% организаций.

Какие типы данных сотрудники посылают внешним получателям или постят онлайн?

Таблица 4-C показывает наиболее часто встречающиеся типы данных, отсылаемые внешним по отношению к организации адресатам. Информация о кредитных картах лидирует в списке, за ней следуют исходный код и файлы, защищенные паролем.

Соответствует ли Ваша организация требованиям PCI?

Сотрудники пересылают номера кредитных карт через Интернет. Номера своих карт и карт клиентов. Они пересылают во вложениях к сообщениям электронной почты квитанции платежей, содержащие номера кредитных карт. Они отвечают, используя «Reply» на письма клиентов, содержащие их номера кредитных карт в теле письма. Иногда сотрудники даже пересылают таблицы с данными клиентов на личные адреса электронной почты или адреса партнеров. Часто инциденты, связанные с номерами кредитных карт, являются результатом нарушенного бизнес-процесса или недостаточной осведомленности и подготовки персонала. Такого рода инциденты могут свидетельствовать о том, что корпоративная политика безопасности не соответствует цели поддержание безопасного и осторожного использования корпоративных ресурсов.
Более того, пересылка номеров кредитных карт через Интернет является нарушением требования 4 стандарта PCI DSS, которое говорит о том, что данные держателя карт должны быть зашифрованы при пересылке через сети общего доступа. Нарушение требований стандарта PCI DSS может привести к ущербу репутации, судебным искам, страховым выплатам, закрытию счетов, проблемам с платежами по пластиковым картам и штрафам со стороны государства.
В рамках нашего исследования мы просматривали исходящий трафик организаций и сканировали содержимое всех частей сообщения, включая приложения и архивы, в поисках сообщений, содержащих номера кредитных карт

Наиболее распространенные приложения для хранения и совместного доступа к файлам

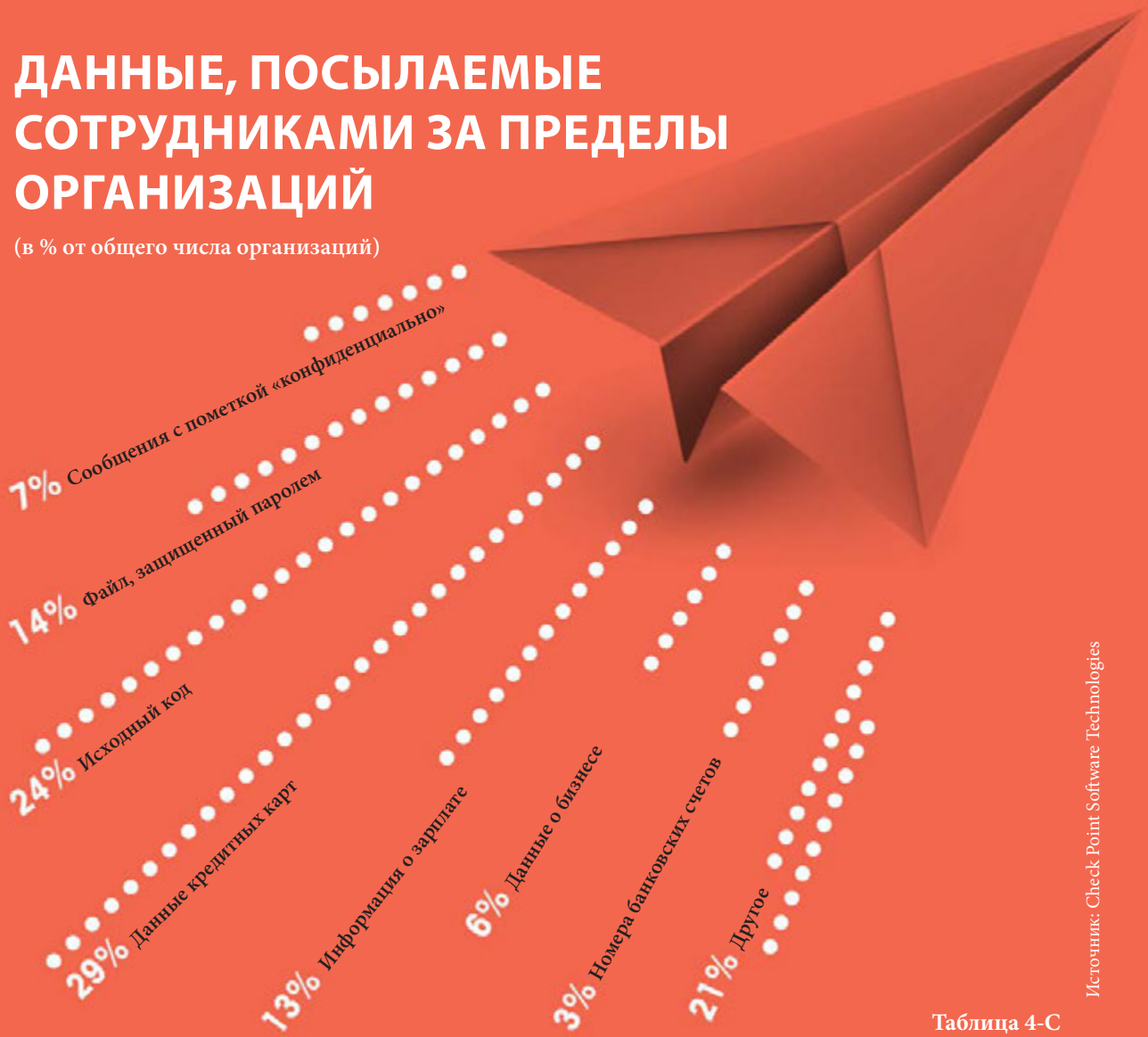
(в % от общего числа организаций)

Таблица 4-B

В 36%
ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ДАННЫЕ КРЕДИТНЫХ КАРТ БЫЛИ ПОСЛАНЫ ЗА ПРЕДЕЛЫ ОРГАНИЗАЦИИ

ДАННЫЕ, ПОСЫЛАЕМЫЕ СОТРУДНИКАМИ ЗА ПРЕДЕЛЫ ОРГАНИЗАЦИЙ

(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица 4-С

или информацию о держателе карты. Инспектирование базировалось на аппарате регулярных выражений, проверке контрольных цифр и требований стандарта PCI DSS.

Наше исследование показало, что в 29% организаций за анализируемый период было найдено как минимум одно событие, связанное с пересылкой вне организации информации, связанной с требованиями PCI. Мы также установили, что в 36% финансовых организаций, которые обычно должны соблюдать стандарт PCI DSS, произошло как минимум одно событие, связанное с требованиями PCI.

HIPAA

Правило персональной информации HIPAA (HIPAA Privacy Rule) обеспечивает защиту персональных данных о состоянии здоровья и предоставляет пациентам правовой комплекс относительно такой информации. В то же время HIPAA Privacy Rule позволяет раскрыть такую информацию, если того требует лечение пациента или при других определенных условиях.

HIPAA Privacy Rule позволяет организациям, оказывающим медицинскую помощь, использовать электронную почту для обсуждения проблем здоровья со своими пациентами, если при этом используются соответствующие методы защиты. Шифрование не является обязательным; однако, другие методы защиты должны быть применены для защиты частного характера информации. Как же возможно поддерживать связи с пациентами, используя открытые каналы электронной почты и одновременно соблюдать требования HIPAA?

В ходе нашего исследования мы просматривали исходящий трафик организаций и сканировали все части сообщений и приложения на предмет наличия в сообщениях электронной почты частной информации пациентов посредством поиска идентификационной информации (такой как номер социального страхования) и специфических медицинских терминов (CPT, ICD-9, LOINC, DME, NDC и т. п.). Мы обнаружили, что в 16% медицинских и страховых организаций, информация, подлежащая защите согласно HIPAA, была послана за пределы организаций — на адреса электронной почты внешних получателей или был выполнен пост онлайн.

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

В современном мире, где потери данных растут день ото дня, организациям ничего не остается, как предпринимать попытки защитить важные данные. Лучшим решением по защите от непреднамеренных утечек данных является внедрение автоматизированной корпоративной политики, которая могла бы обеспечить перехват данных до того, как они покинут организацию. Такие решения называют решениями по Предотвращению Потери Данных (DLP — Data Loss Prevention). Контент-ориентированные продукты DLP обладают широким спектром возможностей и организации имеют различные варианты их размещения. Перед внедрением решения DLP организация должна разработать четкие DLP стратегии с конкретными требованиями относительно того, что считать конфиденциальной информацией, кто может ее пересылать и т. д.

Механизм классификации данных

Высокая точность определения важной информации является критичной компонентой решения DLP, которое должно быть способно обнаруживать персональную идентификационную информацию (PII), данные, связанные с регулирующими стандартами (HIPAA, SOX, PCI и т. п.) и конфиденциальные данные бизнеса. Оно должно просматривать потоки данных и обеспечивать соблюдение политик в наиболее распространенных протоколах TCP, включая SMTP, FTP, HTTP, HTTPS и веб-приложения электронной почты. Решение DLP должно также иметь возможность классификации

54%

ОРГАНИЗАЦИЙ В РАМКАХ НАШЕГО ИССЛЕДОВАНИЯ ИМЕЛИ ХОТЯ БЫ ОДИН ИНЦИДЕНТ, СВЯЗАННЫЙ С ПОТЕНЦИАЛЬНОЙ ПОТЕРЕЙ ДАННЫХ

инспектируемых файлов на основании шаблонов данных для того, чтобы идентифицировать их содержимое вне зависимости от расширения или компрессии.
Дополнительно решение DLP должно распознавать и обеспечивать защиту важной информации на основании предопределенных шаблонов и сопоставления файлов/форм. Важной функцией решения DLP является максимальная гибкость по созданию пользовательских типов данных, наряду с предустановленными производителем.

Дать пользователю возможность предотвратить инцидент

Традиционные решения DLP могут обнаруживать, классифицировать и даже распознавать специфические документы и различные типы файлов, но они не могут определить намерение пользователя, стоящее за попыткой распространения важной информации. Для этого недостаточно одной лишь технологи, так как она не может определить намерение и ответить на него. Таким образом, хорошее решение DLP должно для получения оптимальных результатов подключать к решению этих задач пользователей. Один из путей решения этой проблемы — дать пользователю возможность предотвратить инцидент в реальном времени — решение DLP должно информировать пользователя о том, что его действие может нести потенциальный риск утечки данных, и предоставить ему возможность принять решение: уничтожить сообщение или все равно отослать его. Это повышает уровень безопасности за счет повышения осведомленности о существующих политиках использования данных путем предупреждения пользователя о потенциальных ошибках и предоставления возможности мгновенно исправить их, а также быстро авторизовать легитимное действие. Кроме того, это позволяет облегчить управление. В то время как администратор может отслеживать события DLP для анализа, нет необходимости его персонального присутствия в режиме реального времени при каждой попытке пересылки данных за пределы компании.

Защита от внутренних взломов данных

Другой важной функцией решения DLP является способность не только контролировать попытки утечки важной информации за пределы компании, но также инспектировать и контролировать важные сообщения электронной почты, пересылаемые между отделами внутри организации. Для того чтобы предотвратить утечку конфиденциальной информации в отделы, не имеющие к ней доступа, необходимо определить политики. Примерами таких ситуаций, где есть необходимость защиты от случайной утечки в другой департамент, могут служить данные о компенсационных планах, конфиденциальные документы отдела кадров, документы по слиянию и поглощению или медицинские формы.

Защита данных на жестких дисках конечных устройств

Компании должны защищать данных на своих ноутбуках. Это необходимый элемент эффективной политики ИБ. Без защиты таких данных, внешние люди могут получить ценную информацию из потерянных или украденных ноутбуков, что может привести к негативным правовым или финансовым последствиям. Адекватным решением проблемы должно стать предотвращения доступа к данным неавторизованных пользователей путем шифрования данных на всех жестких дисках конечных устройств, включая пользовательские данные, файлы операционной системы и стертые файлы.

Защита данных на съемных дисках

Для предотвращения инцидентов, в результате которых корпоративная информация на USB устройствах или других съемных носителях может попасть в чужие руки, необходимо применения шифрования и защиты от неавторизованного доступа к этим устройствам. Сотрудники часто смешивают персональные файлы, такие как музыка, картинки с файлами, содержащими бизнес-документы, такими как финансовые или кадровые данные на переносных устройствах, что делает контроль за корпоративными данными существенно более сложной задачей. При использовании шифрования данных на съемных накопителях, в случае компрометации таких устройств, взлом безопасности будет менее вероятным.

Защита документов

Документы бизнеса загружаются на веб с помощью приложений хранения файлов, посылаются на персональные смартфоны, копируются на съемные носители информации и выставляются для совместного доступа бизнес-партнерам на регулярной основе. Каждая из этих операций несет в себе риск потери важных данных, нецелевого использования или доступа к ним неавторизованных пользователей. Для сохранения корпоративных документов в безопасности решение по их защите должно обеспечивать контроль за политикой криптозащиты документов и предоставлять доступ только авторизованным пользователям.

Управление событиями

Для соответствия политикам организации в области пользования данными определение правил DLP должно комбинироваться с хорошими средствами мониторинга и создания отчетов. Для минимизации потенциальных утечек данных в организации решение безопасности должно включать в себя мониторинг и анализ в реальном времени, а также анализ исторических событий DLP. Это даст администратору безопасности широкую и ясную картину информации, отсылаемой за пределы организации, ее источников, а также возможность реакции в реальном времени, когда это необходимо.

05 ЗАКЛЮЧЕНИЕ. СТРАТЕГИЯ БЕЗОПАСНОСТИ

МЫ ЗАВЕРШИМ НАШ ОТЧЕТ ЕЩЕ ОДНОЙ ЦИТАТОЙ СУН ЦЗЫ, ВЗЯТОЙ ИЗ «ИСКУССТВА ВОЙНЫ» — СОВЕТ ОДНОМУ ПОЛКОВОДЦУ:

«СОБИРАЯ ВОЙСКА И КОНЦЕНТРИРУЯ СВОИ СИЛЫ, ОН ДОЛЖЕН СОБРАТЬ И ПРИВЕСТИ В ГАРМОНИЮ РАЗЛИЧНЫЕ ЭЛЕМЕНТЫ ПЕРЕД ТЕМ, КАК РАЗБИВАТЬ СВОЙ ЛАГЕРЬ»

2600 лет спустя тот же самый подход прекрасно подходит к сегодняшней борьбе против киберпреступности — наилучшая сетевая защита может быть реализована, когда все уровни защиты гармонизированы между собой для борьбы с угрозами безопасности с различных направлений.

Настоящий отчет покрывает многочисленные аспекты рисков ИБ, обнаруженные компанией Check Point в различных организациях. Было продемонстрировано, что боты, вирусы, взломы и атаки являются постоянными и реальными угрозами для безопасности предприятий. Отчет показал, что некоторые веб-приложения, используемые пользователями, могут скомпрометировать сетевую безопасность. Наконец, в отчете продемонстрировано, что некоторые действия сотрудников могут привести к непреднамеренной утечке данных.

Ваша стратегия безопасности: здесь недостаточно одной лишь технологии

Подход компании Check Point гласит, что для достижения необходимого уровня безопасности предприятия недостаточно одной лишь технологии. Безопасность должна вырастать из простого собрания отдельных технологических решений и практик в эффективный бизнес-процесс. Компания Check Point рекомендует организациям при развертывании стратегии безопасности и соответствующих решений рассматривать три измерения: Политики, Люди и Обеспечение соблюдения требований.

Политики

Безопасность начинается с внятной и хорошо описанной политики — тесно связанной с бизнес-задачами, а не простым набором проверок системного уровня и технологий. Политики должны принимать во внимание, что приоритетом является бизнес и должны предлагать безопасные способы ведения бизнеса как часть корпоративной политики.

Например, в ходе нашего анализа мы обнаружили, что сотрудники используют веб-приложения как часть бизнес-процесса, но это может поставить под угрозу безопасность. Если мы развернем одни лишь технические средства для блокировки этих приложений, это может привести к тому, что администраторы безопасности будут завалены жалобами от сотрудников, или, что хуже, люди будут пытаться преодолеть политику и создать проблемы с безопасностью. Вместо этого компания Check Point рекомендует Вам создать такую политику, которая принимала бы во внимание случаи, в которых использование таких приложений необходимо и определяла процедуры обеспечения их применения безопасным способом. Пользователи должны автоматически оповещаться о такой политике, когда это необходимо.

Люди

Пользователи компьютерных систем — это критичная часть процесса безопасности. Часто пользователи делают ошибки, которые приводят к заражению вредоносным ПО и утечкам информации. Организации должны быть уверены, что пользователи вовлечены в процесс безопасности. Сотрудники должны быть информированы и обучены политикам безопасности и тому, что от них ожидают при просмотре Интернета или создании общего доступа к файлам. В то же время безопасность должна быть как можно более «бесшовной» и прозрачной, а также не должна вносить изменения в привычный способ работы пользователей.

Внедрение программы безопасности должно включать в себя:

- Программу обучения — для того, чтобы все пользователи были оповещены о том, что системы являются потенциально уязвимыми для атак и что их собственные действия могут допустить их или способствовать их предотвращению.
- Технология — информирование пользователей в реальном времени о том, почему определенные операции являются рискованными и о том, как их можно осуществить безопасным способом.

Обеспечение соблюдения требований

Развертывание технологических решений безопасности, таких как шлюзы безопасности и ПО, на конечных станциях является критически важным элементом защиты организаций от взломов безопасности и потери данных. Шлюзы безопасности должны устанавливаться на всех межсетевых соединениях для того, чтобы быть уверенными, что только соответствующий авторизованный трафик входит в сеть или покидает ее. Эта проверка должна осуществляться на всех уровнях безопасности и всех видах связи, протоколах, методах, запросах, ответах и полезных нагрузках с помощью межсетевых экранов, контроля приложений, фильтрации URL, DLP, систем предотвращения вторжений, антивирусных и анти-ботовых решениях информационной безопасности.

06 О КОМПАНИИ CHECK POINT SOFTWARE TECHNOLOGIES

Компания Check Point Software Technologies Ltd. (www.checkpoint.com) является мировым лидером по обеспечению безопасности в сети Интернет, предлагая своим клиентам надежную защиту против всех типов угроз, уменьшая сложность задачи по обеспечению безопасности и снижая совокупную стоимость владения. Check Point был первой компанией, представившей на рынок межсетевой экран FireWall-1 с патентованной технологией Stateful Inspection. Сегодня Check Point продолжает разрабатывать инновационные решения, основанные на Архитектуре «Программные блейды», предоставляя клиентам простые и гибкие решения, которые могут быть полностью адаптированы для соответствия требованиям безопасности любой организации. Check Point является единственным производителем, который не ограничивается только лишь технологией, но определяет безопасность как бизнес-процесс. Концепция Check Point 3D Security уникальным образом сочетает политики, человеческий фактор и обеспечение соблюдения требований для создания более эффективной защиты информационных активов и помогает организациям внедрить проект ИБ, соответствующий бизнес-требованиям. Клиентами компании являются десятки тысяч организаций, включая все компании из списков Fortune и Global 100. Знаменитое решение ZoneAlarm от Check Point защищает миллионы клиентов от хакеров, шпионского ПО и краж идентификационной информации.

Check Point 3D Security

Концепция Check Point 3D Security определяет безопасность как трехмерный бизнес-процесс, который является комбинацией политик, людей и обеспечения соблюдения требований для усиления защиты на всех уровнях безопасности — включая сеть, данные и конечные устройства. Для того, чтобы достигнуть того уровня защиты, который необходим в XXI веке, безопасность должна вырасти из набора отдельных технологий в эффективный бизнес-процесс. С концепцией 3D Security организации могут реализовывать свои проекты безопасности, далеко выходящие за рамки технологий, в целях обеспечения целостной ИБ.

Check Point 3D Security помогает организациям переопределить безопасность путем интеграции в бизнес-процесс ее трех измерений:

Политики, которые поддерживают бизнес-требования и трансформируют безопасность в бизнес-процесс

Безопасность должна вовлекать **Людей** в определение политик, образование и предотвращение инцидентов

Обеспечивать соблюдения требований, консолидировать и контролировать все уровни безопасности – сеть, данные, приложения, контент и пользователей

Check Point Архитектура «Программные блейды»

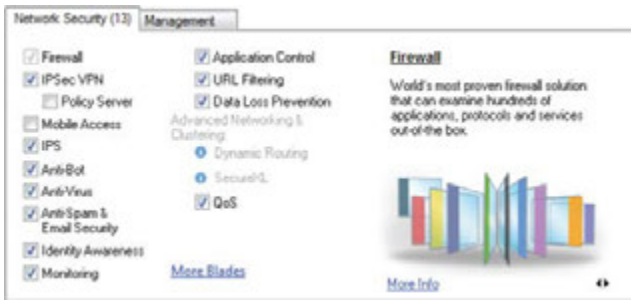
Являясь ключевым элементом 3D Security, Check Point Архитектура «Программные блейды» позволяет компаниям обеспечивать соблюдение политик безопасности, обучая им пользователей. Архитектура «Программные блейды» — первая и единственная в своем роде архитектура, предоставляющая всеобщую, гибкую и управляемую безопасность для компаний любой величины. Кроме того, Check Point Архитектура «Программные блейды» позволяет быстро и гибко расширять сервисы безопасности при появлении новых угроз или требований — без добавления нового оборудования или усложнения управления. Управление всеми решениями с единой консоли существенно снижает сложность и операционные расходы. Многоуровневость защиты на сегодняшний день является критически важной характеристикой для борьбы с такими угрозами как боты, трояны и угрозы класса Advanced Persistent Threat (APT). Межсетевые экраны сегодня представляют собой в большей степени многофункциональные шлюзы безопасности, однако не все компании хотят иметь одни и те же характеристики безопасности в разных

местах. Компаниям требуется гибкость и контроль над их ресурсами безопасности.

Программные блейды — это приложения или модули безопасности, такие как, например, Firewall, Virtual Private Network (VPN), Intrusion Prevention System (IPS), или Application Control, которые являются независимыми, модульными и находящимися под централизованным управлением. Они позволяют организациям создавать специфические настройки безопасности для достижения оптимальной комбинации защиты и инвестиций. Программные блейды могут быть легко активированы и настроены на любом шлюзе или системе управления с помощью простого клика «мыши» — без дополнительных обновлений аппаратной платформы, ПО или драйверов. При изменении нужд безопасности, дополнительные Программные блейды могут быть легко активированы для наращивания безопасности уже существующей конфигурации на той же аппаратной платформе безопасности.

Check Point предлагает централизованное управление событиями как для всех продуктов Check Point, так и для устройств других производителей. Наличие возможности просмотра событий безопасности

Панель управления SmartDashboard шлюза безопасности Check Point. Окно активации Программных блейдов



в реальном времени позволяет быстро вникнуть в текущую ситуацию безопасности и немедленно предпринять соответствующие действия через единую консоль. Просмотр временной шкалы делает возможным визуализацию тенденций и распространения атак. Просмотр графиков предоставляет статистику событий в виде круговых диаграмм или в виде диаграмм со столбцами. Просмотр карт предоставляет информацию о потенциальных угрозах по странам.

Система управления событиями безопасности Check Point SmartEvent. Просмотр в реальном времени

ThreatCloud™ — аналитическая информация по ИБ в реальном времени

ThreatCloud является коллаборативной сетью и облачной базой знаний, предоставляющей динамическую аналитику в реальном времени для шлюзов безопасности. Эта аналитика используется для идентификации возникающих вспышек угроз и их тенденций. ThreadCloud дает возможность Программному блейду Anti-Bot шлюза безопасности отслеживать постоянно изменяющиеся IP, URL и DNS адреса известных Центров управления ботами. Так как обработка информации происходит в облаке, миллионы сигнатур и защит от вредоносного ПО могут быть обработаны в реальном времени.

База знаний ThreatCloud динамически обновляется, питаясь информацией от глобальной сети сенсоров и информацией от шлюзов безопасности со всего мира, а также используя информацию лабораторий Check Point Security Labs и лучшие отраслевые источники информации. Коррелированная информация ИБ затем делается доступной для совместного использования всеми шлюзами.

Устройство Check Pont 61000

THREATCLOUD

Устройства безопасности Check Point

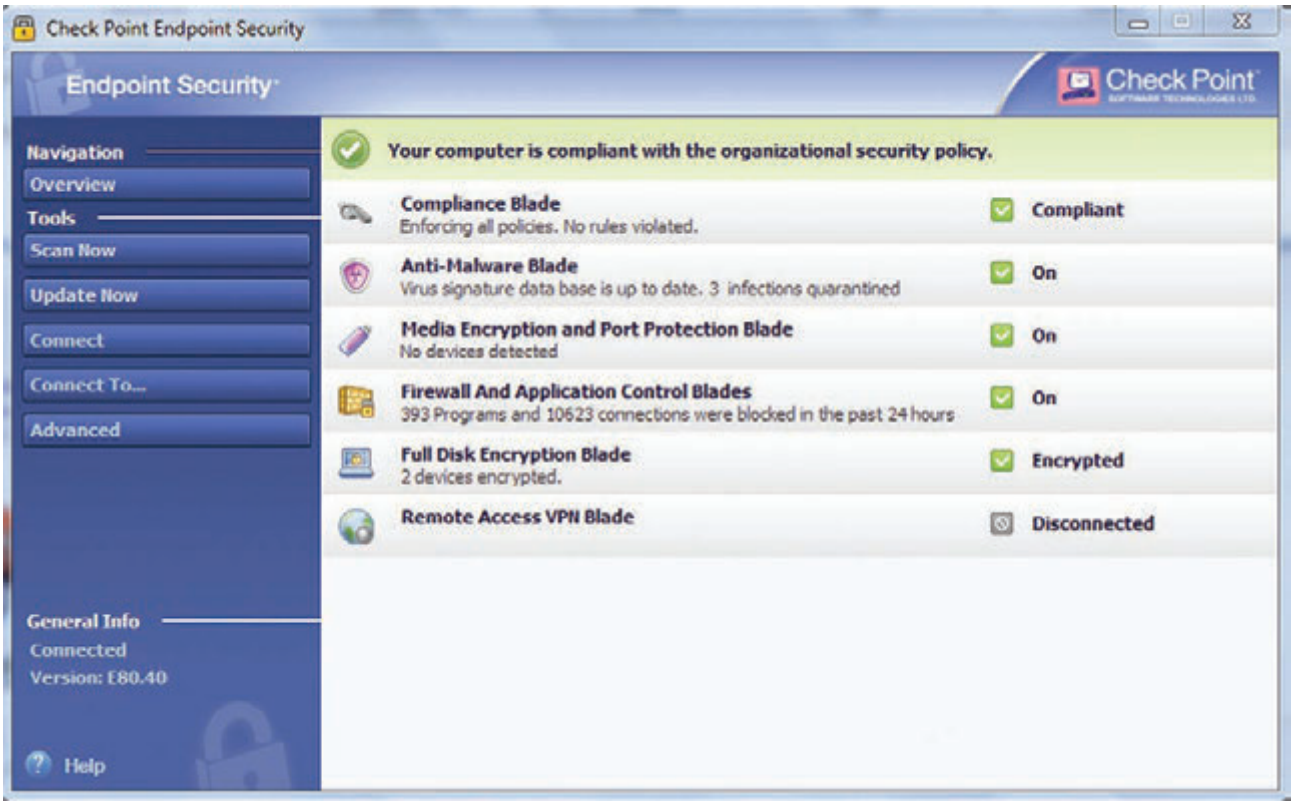
В сетях современных предприятий шлюзы безопасности являются не просто межсетевыми экранами — они представляют собой устройства, сталкивающиеся с постоянно увеличивающимся числом сложных угроз. Они должны использовать разные технологии для контроля сетевого доступа, обнаружения сложных атак и предоставления дополнительных сервисов обеспечения безопасности, таких как предотвращение потери данных, защита от угроз, связанных с веб, и защита постоянно растущего числа мобильных устройств, таких как IPhone и таблетов в корпоративных сетях. Эти постоянно растущие угрозы и задачи защиты требуют от устройств безопасности все большей производительности и расширенных возможностей.

Построенные на операционной системе нового поколения Check Point GAiA, устройства Check Point сочетают в себе высокую производительность многоядерной архитектуры со скоростными сетевыми технологиями, предоставляя высочайший уровень безопасности для данных, сети и сотрудников. Оптимизированное для использования Архитектуры «Программные блейды», каждое устройство способно использовать любое сочетание Программных блейдов, включая Firewall, IPSec VPN, IPS, Application Control, Mobile Access, DLP, URL Filtering, Anti-Bot, Anti-Virus, Anti-spam, Identity Control и Advanced Networking & Clustering — обеспечивая гибкость и точно выверенный уровень безопасности для любого бизнеса и любом месте сети. Консолидируя многие технологии безопасности в едином шлюзе безопасности, устройства были спроектированы для предоставления различных интегрированных решений, способных отвечать различным нуждам организаций в области безопасности бизнеса. Представленный в августе 2011 года, тест SecurityPower™ является метрикой, которая выражает способность устройства исполнять различные функции безопасности на указанном объеме трафика. С ним заказчики получили возможность выбрать устройство, соответствующее их специфическим требованиям, на основе революционной методики измерений. Рейтинги Security Power определены с использованием реального трафика пользователей, многих функций безопасности и типовой политики безопасности.

Check Point Endpoint Security — безопасность конечных устройств от компании Check Point

Модули Программных блейдов Check Point Endpoint Security предоставляют беспрецедентную гибкость, контроль и эффективность при управлении и развертывании безопасности конечных устройств. Менеджеры IT могут сделать свой выбор среди шести различных модулей Программных блейдов Endpoint для развертывания только необходимых механизмов защиты, с последующей возможностью в любое время нарастить решение безопасности. **Программный блейд Full Disk Encryption** прозрачно и в автоматическом режиме защищает всю информацию на жестких дисках конечного устройства. Многофакторная аутентификация перед загрузкой позволяет надежно идентифицировать пользователя. **Программный блейд Media Encryption** предоставляет централизованное управление шифрованием съемных носителей информации с возможностью избирательного шифрования только информации, относящейся к бизнесу, а также возможностью оповещать пользователя и вовлекать его в процесс защиты информации. **Программный блейд Remote Access VPN** дает пользователям возможность удаленного доступа к корпоративным сетям и ресурсам во время путешествий или работы из дома. **Программный блейд Anti-Malware and Program Control** эффективно обнаруживает и уничтожает вредоносное ПО с конечных устройств в рамках одного сканирования. Контроль Программ позволяет быть уверенным, что на конечных устройствах исполняются только легитимные и разрешенные программы. **Программный блейд Firewall and Security Compliance Verification** предоставляет проактивную защиту входящего и исходящего трафика для предотвращения заражения конечных устройств вредоносным ПО, блокирования целенаправленных атак и запрета нежелательного трафика. Верификация Соответствия Требованиям Безопасности позволяет убедиться, что Ваши конечные устройства будут всегда соответствовать требованиям политики безопасности организации. **Программный блейд WebCheck Secure Browsing** защищает от последних угроз, связанных с использованием веб, включая загрузку «при прохождении» (drive-by), фишинговые сайты и атаки «нулевого дня». Сессии браузера исполняются в безопасном виртуальном пространстве.

Клиент Check Point Endpoint Security



A ПРИЛОЖЕНИЕ A: НАИБОЛЕЕ РАСПРОСТРАНЕННОЕ ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Этот раздел содержит информацию, относящуюся к вредоносному ПО, наиболее распространенному в рамках нашего исследования. Полная база данных компании Check Point по вредоносному ПО доступна по адресу threatwiki.checkpoint.com.

Zeus представляет из себя бот-агент «черного хода», нацеленный на платформу Microsoft Windows. “Черный ход” является методом обхода процедур аутентификации. После того, как система была скомпрометирована, в нее могут быть установлены один или несколько «черных ходов» для организации легкого доступа в будущем. Наше исследование обнаружило ботов Zeus, созданных из набора Zeus toolkit версии 2.0.8.9. Zeus — это большое семейство банковских троянов с большим количеством версий и вариантов. Это вредоносное ПО предоставляет атакующему удаленный доступ к зараженным системам. Главной задачей в этом случае является хищение банковской идентификационной информации, которую вводят пользователи для доступа к своим счетам.

Zwangi — это рекламное ПО, нацеленное на Microsoft Windows. Оно регистрируется как helper object в браузере зараженной системы. Оно может создавать свою панель инструментов в Internet Explorer и демонстрировать пользователю нежелательные рекламные сообщения. Это вредоносное ПО заражает системы через наборы программного обеспечения.
Sality представляет собой вирус, распространяющий себя через заражение и модификацию исполняемых файлов и копирование себя на съемные диски и папки совместного доступа.

Kuluoz — бот, направленный на платформу Microsoft Windows. Этот бот, как сообщается, рассылает спам–сообщения, будто бы от имени почтовой службы США (US Postal Service). Он высылает вовне системную информацию и принимает инструкции от удаленного сервера на загрузку и исполнение вредоносных файлов на зараженном компьютере. Кроме того, он создает запись в регистре для того, чтобы запускаться после перезагрузки системы.

Juasek — это бот «черного хода», нацеленный на платформу Microsoft Windows. Это вредоносное ПО позволяет удаленному не аутентифицированному атакующему выполнять вредоносные действия, такие как открытие командной оболочки, загрузку и выгрузку файлов, создание новых процессов, вывод списков и уничтожение процессов, поиск/создание/удаление файлов и получение системной информации. Дополнительно он устанавливает сервис для того, чтобы выжить при перезагрузке.

Papras — это банковский троян, нацеленный на 32 битные и 64 битные платформы Microsoft Windows. Это вредоносное ПО отсылает вовне системную информацию и запрашивает конфигурационную информацию с удаленного хоста. Он перехватывает сетевые функции и просматривает Интернет–активность пользователя с целью хищения критичной финансовой информации. Дополнительно он обладает функционалом «черного хода» для предоставления удаленному атакующему неавторизованного доступа к зараженному компьютеру. Принимаемые команды управления включают в себя загрузку других вредоносных файлов, сбор информации о cookies и сертификатах, перезагрузку и выключение системы, отсылку информации системных журналов, получение снимков экрана, установку сокетных соединений к удаленному хосту для других задач и т. п. Более того, это вредоносное ПО вставляет себя в процессы и также может осуществлять вставку других вредоносных программ в указанные процессы.

B ПРИЛОЖЕНИЕ B: НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ ПРИЛОЖЕНИЯ ВЫСОКОГО РИСКА ИБ

Этот раздел содержит информацию, относящуюся к приложениям, наиболее распространенным в рамках нашего исследования. Полная база данных компании Check Point по приложениям доступна по адресу apptwiki.checkpoint.com.

Анонимайзеры

Tor — приложение для обеспечения онлайн анонимности. Клиент Tor направляет весь интернет-трафик через всемирную сеть серверов, созданную волонтерами, для того, чтобы скрыть местоположения пользователя или его запросы от любого, кто осуществляет наблюдение за сетью или анализ трафика. Использование Tor-а существенно затрудняет процесс соотнесения Интернет-активности, включая «посещение веб-сайтов, посты онлайн, мгновенные сообщения и другие формы коммуникации», с тем или иным пользователем.

CGI-Proxy является программным обеспечением Интерфейса Общего Шлюза (Common Gateway Interface) и выглядит для пользователя как веб-страница, позволяющая получить доступ к другому сайту. Поддерживаемые протоколы — HTTP, FTP и SSL.

Hopster — приложение для обхода МСЭ и прокси-серверов, позволяющее анонимно просматривать Интернет и обмениваться сообщениями в чатах.

Hide My Ass — весплатный сервис веб-прокси, маскирующий IP адрес и позволяющий пользователям анонимно подключаться к вебсайтам.

Hamachi — свободно распространяемое (shareware) ПО виртуальной частной сети (VPN). Используется для установления соединения поверх Интернета, которое эмулирует соединение локальной сети (LAN).

Ultrasurf — бесплатная утилита прокси, позволяющая пользователям обходить МСЭ и средства блокировки контента в Интернете.

OpenVPN — бесплатное, свободно распространяемое ПО с открытым исходным кодом (free open source software), использует технологии виртуальных частных сетей (VPN) для создания безопасных соединений “точка-точка” или “сайт-сайт” в маршрутизируемых или коммутируемых конфигурациях, а также для создания инфраструктуры удаленного доступа.

Приложения обмена файлами P2P

Bittorent — протокол P2P обмена файлами. Представляет собой метод широкого распространения больших объемов данных без наличия первичного центрального раздающего узла, требующего больших затрат на оборудование, хостинг и полосу пропускания. Вместо этого, когда данные распределены с использованием протокола BitTorrent, каждый получатель предоставляет части данных, в свою очередь, новым получателем, снижая затраты и нагрузку на каждый отдельно взятый источник, создавая избыточность относительно системных сбоев и снижая зависимость от центрального источника раздачи. Существует большое число клиентского ПО, совместимого с BitTorrent, написанного на разных языках программирования и исполняемого на различных вычислительных платформах.

eMule — P2P файлообменное приложение, соединяющееся с сетями eDonkey и Kad. Программа предоставляет прямую коммутацию источников между клиентскими узлами, восстановление поврежденных загрузок и использование системы кредитов для поощрения раздающих участников. eMule осуществляет передачу данных в zlib-сжатом виде для экономии полосы пропускания.

Soulseek –это приложение P2P обмена файлами. Используется в основном для обмена музыкой, хотя пользователи могут предоставлять совместный доступ к различным файлам.

Gnutella — популярная файлообменная сеть и один из наиболее популярных протоколов P2P. Используется такими приложениями, как BearShare, Shareaza, Morpheus и iMesh. Используется в основном для обмена музыкальными MP3 файлами, видео, приложениями и документами.

Sopcast — мультимедийное потоковое приложение, позволяющее потоковое вещание через P2Pсети. Sopcast дает пользователям возможность осуществлять широковещательные передачи или смотреть широковещательные передачи других пользователей.

Утилиты удаленного администрирования

Remote Desktop Protocol (RDP) — проприетарный протокол, разработанный компанией Microsoft, предоставляющий пользователю удаленный интерфейс к другому компьютеру.

Team Viewer — позволяет пользователям управлять удаленными компьютерами используя клиентское ПО или подключаясь к веб-сайту.

LogMeIn — собрание программных сервисов, предоставляющих удаленный доступ к компьютерам через Интернет. Различные версии продукта предназначены как для конечных пользователей, так и для профессиональных сервисов технической поддержки. Продукты удаленного доступа LogMeIn используют проприетарный протокол удаленного доступа к рабочему столу, передающийся посредством SSL. Пользователи получают доступ к удаленным рабочим столам, используя веб-портал в Интернете или, как вариант, через отдельное приложение LogMeIn Ignition.

VNC — ПО, состоящее из сервера и клиентского приложения, использующего протокол VNC (Virtual Network Computing) для удаленного управления другим компьютером. Существуют варианты ПО для Windows, Mac OS X, UNIX-подобных операционных систем. VNC часто запускается на платформе Java, а также на Apple iPhone, iPod touch и iPad.

Приложения хранения и совместного доступа к файлам

Dropbox — приложение, позволяющее пользователю организовывать совместный доступ к файлам. Dropbox является сервисом хостинга файлов, предоставляемого компанией Dropbox, Inc., предлагающей облачное хранилище файлов, синхронизацию файлов и клиентское ПО. Вкратце, Dropbox предоставляет пользователям возможность создать специальную папку на каждом из их компьютеров, которые затем Dropbox синхронизирует таким образом, что они будут представляться как одна и та же папка (с одинаковым содержимым), независимо от того, на каком из компьютеров она просматривается. Файлы, помещенные в эту папку, также доступны через веб-сайт и приложения для мобильных телефонов.

Windows Live Office — онлайн-утилита, созданная компанией Microsoft, позволяющая хранить, редактировать и организовывать совместный доступ к документам Microsoft Office. С помощью Office Web Apps пользователи могут создавать, просматривать, редактировать, обмениваться и совместно работать над документами, таблицами, презентациями и заметками в режиме онлайн, находясь в любой точке планеты, через Интернет.

Curl — утилита командной строки, позволяющая передавать данные в синтаксисе URL. Поддерживает FILE, FTP, HTTP, HTTPS, SSL сертификаты и другие протоколы передачи.

YouSendIt — цифровой сервис доставки файлов. Сервис позволяет пользователям посылать, получать и отслеживать файлы по запросу.

C ПРИЛОЖЕНИЕ C: ДОПОЛНИТЕЛЬНЫЕ ДАННЫЕ ПО ИСПОЛЬЗОВАНИЮ WEB-ПРИЛОЖЕНИЙ

Следующие данные представляют собой дальнейший анализ данных, представленных в разделе «Приложения в Корпоративной Среде».
Таблицы C-A и C-B представляют суммарную статистику использования приложений по категориям и по регионам.

Использование приложений по категориям

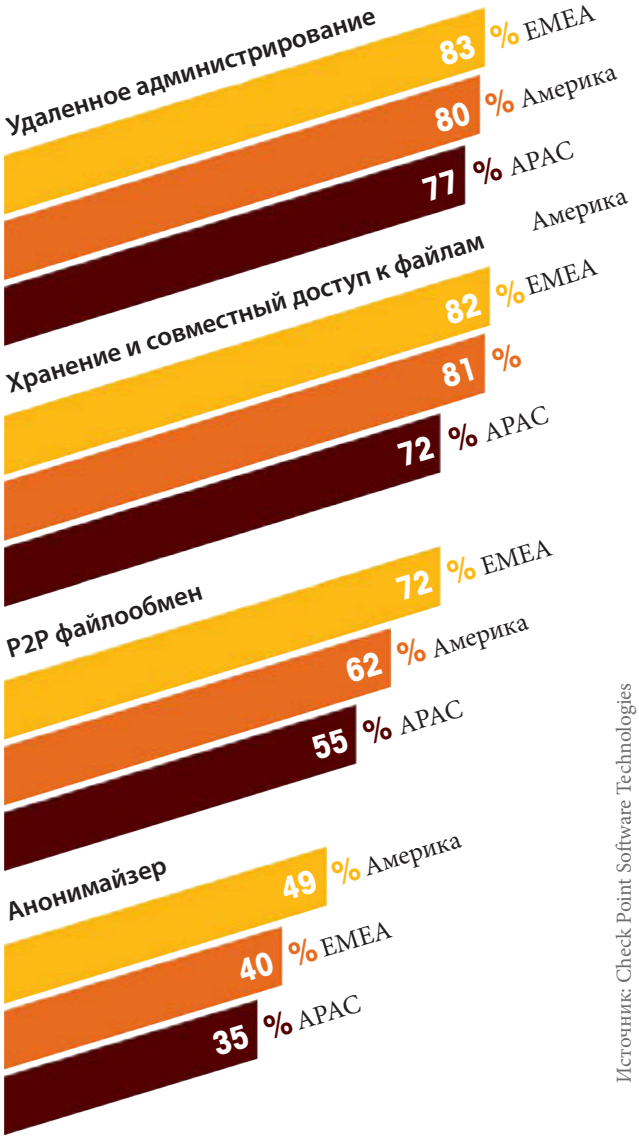
(в% от общего числа организаций)

Источник: Check Point Software Technologies

Таблица C-A

Использование приложений по регионам

(в % от общего числа организаций)



Источник: Check Point Software Technologies

Таблица C-B

Следующие таблицы детализируют данные по наиболее популярным клиентам BitTorrent и Gnutella

Наиболее популярные клиенты BitTorrent	Количество организаций
Vuze	108
Xunlei	74
uTorrent	55
BitComet	25
FlashGet	21
QQ Download	8
Pando	7
P2P Cache	7
Transmission	6
Other	242

Наиболее популярнуе клиенты Gnutella	Количество организаций
BearShare	52
LimeWire	23
FrostWire	16
Foxy	2
Other	31

В следующих таблицах приведена дополнительная информация о наиболее используемых приложениях по различным категориям в регионах

Категория приложений	Регион	Название приложения	% организаций
Анонимайзер	Америка	Tor	24%
		CGI-Proxy	16%
		Hamachi	8%
		Hopster	8%
		Ultrasurf	7%
	Европа, Ближний Восток и Африка	Tor	23%
		CGI-Proxy	12%
		Hamachi	4%
		Hopster	7%
		Hide My Ass	7%
	Азиатско-Тихоокеанский регион	Tor	20%
		Hopster	6%
		CGI-Proxy	6%
		Hamachi	6%
		Hide My Ass	7%

Категория приложений	Регион	Название приложения	% организаций
Файлообмен P2P	Америка	BitTorrent Clients	35%
		SoulSeek	23%
		eMule	21%
		Windows Live Mesh	8%
		Sopcast	8%
	Европа, Ближний Восток и Африка	BitTorrent Clients	33%
		SoulSeek	19%
		eMule	15%
		Sopcast	12%
		iMesh	10%
	Азиатско-Тихоокеанский регион	BitTorrent Clients	62%
		eMule	26%
		SoulSeek	11%
		Sopcast	10%
		BearShare	8%
Хранилище файлов и совместный доступ	Америка	Dropbox	73%
		Windows Live Office	52%
		Curl	28%
		YouSendIt	26%
		ZumoDrive	12%
	Европа, Ближний Восток и Африка	Dropbox	71%
		Windows Live Office	51%
		Curl	22%
		YouSendIt	21%
		ImageVenue	18%
	Азиатско-Тихоокеанский регион	Dropbox	57%
		Windows Live Office	50%
		Curl	26%
		YouSendIt	16%
		Hotfile	10%

Категория приложений	Регион	Название приложения	% организаций
Удаленное администрирование	Америка	MS-RDP	59%
		LogMeIn	51%
		TeamViewer	45%
		VNC	14%
		Bomgar	8%
	Европа, Ближний Восток и Африка	MS-RDP	60%
		TeamViewer	55%
		LogMeIn	44%
		VNC	20%
		pcAnywhere	3%
	Азиатско-Тихоокеанский регион	TeamViewer	58%
		MS-RDP	51%
		LogMeIn	26%
		VNC	16%
		Gbridge	3%

D ПРИЛОЖЕНИЕ D: ТИПЫ ДАННЫХ ДЛЯ DLP

Наше исследование включало в себя инспекцию нескольких десятков различных типов данных на предмет потенциальных утечек данных. Нижеприведенный список содержит основные данные, которые были инспектированы и обнаружены модулем Check Point Программный блейд DLP.

Исходный код — данные, содержащие строки на языках программирования, таких как C, C++, C#, JAVA и других; Указывает на утечку интеллектуальной собственности.

Информация кредитных карт — включает в себя два типа данных: номера кредитных карт и Важные Данные Аутентификации, по стандарту PCI (PCI-Sensitive Authentication Data).

- **Номера кредитных карт:**
  Критерии совпадения: имеют отношение к индустрии платежных карт (Payment Card Industry, PCI); данные, содержащие номера кредитных карт MasterCard, Visa, JCB, American Express, Discover и Diners Club; совпадение основано на шаблоне (регулярное выражение) и проверке корректности контрольных цифр по схеме, определенной в Annex B ISO/IEC 7812–1 и в JTC 1/SC 17 (алгоритм Luhn MOD-1); Указывает на утечку конфиденциальной информации.
  Пример: 4580–0000–0000–0000.
- **PCI-Sensitive Authentication Data:**
  Критерии совпадения: имеют отношение к индустрии платежных карт (Payment Card Industry, PCI); данные, содержащие информацию, классифицируемую как Важные Аутентификационные Данные (Sensitive Authentication Data) согласно стандарту PCI Data Security Standard (DSS). Данные, такие как информация о Держателе карты, крайне важна, и стандарт PCI DSS не допускает их хранения. Производится поиск совпадения данных магнитных дорожек карт (дорожки 1, 2 или 3), зашифрованного или расшифрованного блока PIN и Кода Безопасности Карты (CSC, Card Security Code).
  Примеры:%B4580000000000000^JAMES /L.^99011200000000000?, 2580.D0D6.B489.DD1B, 2827.

Файл, защищенный паролем — файлы, защищенные паролем, либо зашифрованные. Такие файлы могут содержать конфиденциальную информацию.

Файл зарплатной квитанции — файлы, содержащие расчетный листок (payslip), корешок от зарплатного чека (paycheck stub), уведомление о платеже (pay advice) или другие зарплатные документы; указывает на потерю персональных данных.

Конфиденциальное сообщение электронной почты — сообщения Microsoft Outlook, маркированные отправителем как <Confidential>; такие сообщения обычно содержат важную информацию. Примечание: Microsoft Outlook позволяет пользователь маркировать отосланные сообщения различными метками важности; данные этого типа были промаркированы как <Confidential>используя вышеуказанную функцию Outlook.

Информация о зарплате и компенсациях — документы, содержащие слова и фразы, связанные с компенсационным пакетом сотрудников: зарплата, бонус и т. п.

Другие типы данных, обнаруженные в ходе исследования — идентификационная карта Гон-Конга, термины финансовых отчетов, номера банковских счетов, номера IBAN Финляндии, канадские номера социального страхования, FERPA — конфиденциальные отчеты по образованию, почтовые Zip коды США, регистрационные номера НДС Великобритании, номера социального страхования Мексики, номера социального страхования США, уровни (грэйды) студентов — GPA, отчеты о продажах, персональный идентификационный код Финляндии, данные ITAR — International Traffic in Arms Regulations, важные персональные записи, файлы графических проектов CAD-CAM, конфиденциальную медицинскую информацию, защищаемую стандартом HIPAA, номера социального страхования Франции, имена сотрудников, New Zealand Inland, данные держателей карт, номера водительских удостоверений США, номера медицинских записей, номера социального страхования Канады, HIPAA — ICD-9, IBAN Дании, Номера НДС Финляндии, международные номера банковских счетов — IBAN и другие.

ССЫЛКИ

[1] Сун Цзы «Искусство войны», http://suntzusaid.com/artofwar.pdf
[2] http://www.checkpoint.com/campaigns/3d-analysis-tool/index.html
[3] http://www.checkpoint.com/products/threatcloud/index.html
[4] http://supportcontent.checkpoint.com/file_download?id=20602
[5] http://www.nytimes.com/2012/03/05/technology/the-bright-side-of-being-hacked.html?pagewanted=2&ref=global-home
[6] http://edition.cnn.com/video/#/video/bestoftv/2012/10/01/exp-erin-cyberattack-nuclear-networks-leighton.cnn?iref=allsearch
[7] http://www.networkworld.com/news/2012/071312-security-snafus-260874.html?page=4
[8] http://www.businessweek.com/news/2012-10-18/bank-cyber-attacks-enter-fifth-week-as-hackers-adapt-to-defenses
[9] http://arstechnica.com/security/2012/09/blackhole-2-0-gives-hackers-stealthier-ways-to-pwn/
[10] http://www.networkworld.com/slideshow/52525/#slide1
[11] http://www.ihealthbeat.org/articles/2012/10/30/breaches-at-uks-nhs-exposed-nearly-18m-patient-health-records.aspx
[12] http://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf
[13] http://cve.mitre.org/index.html
[14] http://www.networkworld.com/news/2012/020912-foxconn-said-to-have-been-255917.html
[15] http://news.cnet.com/8301-1009_3-57439718-83/anonymous-attacks-justice-dept-nabbing-1.7gb-of-data/
[16] http://news.cnet.com/8301-1009_3-57396114-83/vatican-anonymous-hacked-us-again/
[17] http://news.cnet.com/8301-1023_3-57411619-93/anonymous-hacks-into-tech-and-telecom-sites/
[18] http://www.ftc.gov/opa/2012/06/epn-franklin.shtm
[19] http://www.ftc.gov/opa/2010/02/p2palert.shtm
[20] http://www.networkworld.com/news/2012/091212-botnet-masters-hide-command-and-262402.html
[21] http://www.computerworld.com/s/article/9221335/_Nitro_hackers_use_stock_malware_to_steal_chemical_defense_secres
[22] http://bits.blogs.nytimes.com/2012/08/01/dropbox-spam-attack-tied-to-stolen-employee-password/
[23] http://news.cnet.com/8301-31921_3-20072755-281/dropbox-confirms-security-glitch-no-password-required/
[24] http://japandailypress.com/newspaper-reporter-fired-for-emailing-sensitive-info-to-wrong-people-159277
[25] http://www.roanoke.com/news/roanoke/wb/307564
[26] http://tamutimes.tamu.edu/2012/04/13/am-acting-on-email-message-that-inadvertently-included-some-alumni-ss-numbers/
[27] www.hhs.gov/ocr/privacy/hipaa/index.html
[28] Сун Цзы «Искусство войны», http://suntzusaid.com/artofwar.pdf
[29] http://en.wikipedia.org/wiki/Malware#Backdoors

Check Point®
SOFTWARE TECHNOLOGIES LTD.

www.checkpoint.com

CONTACT RRC

Россия
119331, г. Москва, проспект Вернадского, д.29, офис 903 | Тел.: +7 (495) 956 1717 | Факс: +7 (499) 133 5230
195112, г. Санкт-Петербург, Малоохтинский пр., д.68, офис 302 | Тел.: +7 (812) 333 1510 | Факс: +7 (812) 528 0225
По вопросам заказов E-mail: security@rrc.ru
По вопросам технической поддержки E-mail: cp_support@rrc.ru | www.security-rrc.ru

Украина
04073, г. Киев, проспект Московский, д.8, корп.1 | Тел.: +38 (044) 581 1118 | Факс: +38 (044) 581 1119 | E-mail: office@rrc.com.ua

Республика Казахстан
050010, г. Алматы, ул. Бегалина, д.72 | Тел.: +7 (727) 298 0257 | Факс: +7 (727) 293 0325 | E-mail: info@rrc.kz

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

Декабрь, 2012