М. В. Кузин

ИССЛЕДОВАНИЕ VERIZON BUSINESS: КОМПРОМЕТАЦИЯ ДАННЫХ В 2008 г.

1. Исследование компании Verizon Business

Компания Verizon Business ведет свою историю с конца 80-х годов прошлого века, в настоящее время специализируется на комплексных решениях в таких областях, как ИТ, безопасность, связь и сетевые решения. IP-сеть компании является самой связной из открытых магистральных интернет-сетей в мире. Verizon Business предоставляет коммуникационные сервисы тысячам компаний, ряду правительственных организаций и 98 % компаний из крупнейших в списке Fortune 500. Компания владеет более чем 4 тысячами сетей в 142 странах мира, обеспечивает работу свыше 200 центров обработки данных [1].

В течение 2008 г. Verizon Business участвовала в расследовании 150 инцидентов, связанных с компрометацией данных. По 90 инцидентам информация о компрометации оказалась подтвержденной, именно эти факты и статистика, собранная и обработанная ранее, с 2004 по 2007 г., легли в основу исследования "2009 Data Breach Investigations Report", проведенного подразделением Verizon Business Risk Team. Полный текст отчета на английском языке доступен на сайте компании [2].

Среди компаний, подвергшихся атакам, 31 % относится к предприятиям розничной торговли, 30 % — к сфере финансовых услуг, 14 % — пищевые компании, по 6 % — производство, бизнес-услуги и гостиницы. Всего в результате успешных атак ***оказались скомпрометированы 285 млн записей***, представляющих собой отдельные элементы данных, таких как номер банковской карты или данные по конкретному счету, персональные данные человека, учетная запись в некоторой системе АС и т. д. ***Подавляющее большинство — 93 % — скомпрометированных данных (с.д.) относится к финансовому сектору***.

2. Источники угроз

Источники угроз представлены в исследовании тремя категориями:

· *внутренние* — располагаются внутри организации: люди (управленцы, персонал, практиканты), информационные системы, технические средства;

· *внешние* — располагаются вне организации, например хакеры, организованные преступные группы, государственные структуры, природные явления;

· *со стороны партнеров* — любой третьей стороны, с которой осуществляется какое-либо взаимодействие: продавцы, поставщики, подрядчики, клиенты.

Анализ результатов пятилетних исследований, так же как и данные 2008 г. (всего около 600 инцидентов с 2004 г.), приводит к выводу, что *за большинством атак стоят внутренние нарушители*. Большинство инцидентов в 2008 г. происходили из-за внешних угроз — 74 % от общего числа, на внутренние угрозы и угрозы со стороны партнеров пришлись соответственно 20 % и 32 %. Очевидно, что суммарно приведенные величины превосходят 100 % — это связано с тем, что 39 % инцидентов возникли ввиду реализации нескольких угроз, из различных источников. Медианное значение числа скомпрометированных записей при реализации одной внутренней угрозы равно 100 000, однако в результате только внешних угроз суммарное число скомпрометированных данных составило 266,768 млн, а 15,796 млн пришлось на более чем одну реализованную угрозу.

Внешние атаки в основном (82 %) проводились из Восточной Европы, Восточной Азии и Северной Америки. При расследовании 43 инцидентов помимо IP-адреса не удалось выявить

никакой информации о его обладателе, в 19 случаях была установлена связь с организованными преступными группами, а в 6 — с конкретными людьми.

Внутренние нарушители действовали намеренно приблизительно в двух случаях из трех, остальные были связаны со случайными ошибками. В 9 случаях опасность исходила от конечных пользователей, в 8 была связана с администраторами или привилегированными пользователями.

Относительно действий партнеров можно сделать вывод о том, что в огромном числе инцидентов не были обеспечены достаточные меры и практики взаимодействия организаций с третьими сторонами, при этом партнеры осуществляли администрирование информационных активов или имели доступ на уровне пользователей.

3. Угрозы и атаки

Анализ инцидентов позволил выявить следующее распределение методов, использовавшихся злоумышленниками, по относительным величинам от числа инцидентов и числа с.д. соответственно:

- взлом (hacking) — 64 % и 94 %;
- вредоносное программное обеспечение (malware) — 38 % и 90 %;
- неправильное использование, злоупотребление (misuse) — 22 % и 2 %;
- обман (deceit) — 12 % и 6 %;
- физические методы (physical) — 9 % и 2 %;
- ошибки (error) — 1 % и 67 %.

Взлом и использование вредоносного программного обеспечения являются наиболее часто применяемыми методами злоумышленников с 2006 г., при этом взлом — самый популярный на протяжении всего времени проведения исследований с 2004 г. Наиболее популярным среди злоумышленников стало использование встроенных и общих учетных записей (17 успешных атак и 53 % с.д.), однако SQL-инъекции оказались первыми по объему данных (79 %) и вторыми по числу успешных атак (16). SQL-инъекции стали возможными ввиду отсутствия фильтрации данных, вводимых пользователям, а также из-за избыточных привилегий приложений, обращающихся к БД.

Третью позицию в списке применявшихся средств для атак занимают некорректно настроенные списки управления доступом (6 успешных атак, 66 % с.д.). Атаки полного перебора, «в лоб» (brute force), были выявлены лишь в 4 случаях и привели к компрометации 7 % данных. Иные типы атак (обход процедур аутентификации, повышение привилегий, использование переменных сессии, переполнение буфера, cross-site scripting) не набрали и по 1 % от числа с.д.

Взлом с применением удаленного доступа использовался в 22 атаках (27 % с.д.), посредством веб-приложений — в 21 атаке (79 % с.д.), других серверов и приложений — в 7 атаках (7 % с.д.), сетевых устройств — в 6 атаках (11 % с.д.), клиентских приложений — в 1 атаке (26 % с.д.).

С использованием вредоносного ПО была связана треть всех атак и 9 из 10 записей, оказавшихся скомпрометированными. Вредоносное ПО внедрялось нарушителями различными способами — непосредственная установка (18 случаев и 89 % с.д.), через посещение жертвой зараженного сайта (7 случаев), скачивание из Интернета и установка персоналом (3 случая). Лишь в 4 случаях злоумышленники использовали известные уязвимости прикладного и системного ПО, причем необходимые обновления разработчиками были выпущены ранее чем за год до осуществления атак.

Вредоносное ПО характеризовалось следующими функциями:

- перехват клавиатурного ввода (keyloggers) и шпионские функции (spyware) — 17 случаев;
- доступ к командной строке (command shell) и наличие «черного хода» (backdoor) — 16 случаев;

· перехват и хранение данных — 13 случаев;

· атаки на другие системы, отключение средств защиты и иные — по 2 случая.

Следует отметить, что компрометация хранимых данных осуществлялась не только с таких привычных мест хранения, как жесткие диски, CD-диски, магнитные ленты, но и непосредственно из ОЗУ.

Создание и адаптация вредоносного ПО для атак на конкретные, выбранные злоумышленниками системы также является характерной чертой исследованных в 2008 г. случаев. ***По сравнению с 2007 г. число специализированных вредоносных программ увеличилось более чем в 2 раза, причем 85 % с.д. из общего числа в 285 млн были скомпрометированы с использованием таких программ***. Это означает, что современные антивирусы на момент атак были неспособны обнаружить большинство из них — этот вывод подтвержден в исследовании.

Многие атаки стали успешными из-за ошибок различного типа: неправильная настройка (31 атака), бездействие (31 атака), программная ошибка (16 атак), ошибка пользователя (3 атаки), технический сбой (1 ошибка).

Специалисты Verizon Business также попытались определить сложность атак по следующей собственной шкале:

· *отсутствующая* — не требуется никаких специальных знаний или ресурсов, ее мог бы осуществить средний пользователь;

· *низкая* — используются базовые методы без какой-либо настройки и/или небольшие ресурсы, такие атаки, как правило, осуществляются с использованием готовых модулей, утилит и блоков кода;

· *средняя* — достаточно сложные методы, определенная настройка и/или существенные ресурсы;

· *высокая* — сложные методы и специальные навыки, существенная настройка и/или огромные ресурсы.

Очевидно, что данная оценка сложности является качественной и весьма субъективной, но, тем не менее, позволяет сделать ряд выводов. Во-первых, по числу атак в зависимости от их сложности атаки с отсутствующей и низкой составили 10 % и 42 % соответственно. На средние по сложности атаки пришелся 31 % атак, а на сложные — лишь 17 %. Во-вторых, ***сложные атаки позволили злоумышленникам получить доступ к 95 % с.д***. В-третьих, ориентированность злоумышленников на конкретную систему может привести к ее взлому за конечное время с применением определенных ресурсов, однако ввиду ограниченности последних атаки, вероятнее всего, будут совершаться на менее защищенные системы. Так, в 2008 г. случайные жертвы были выбраны злоумышленниками в 28 % случаев, с учетом известных уязвимостей в атакуемых системах — в 44 %, намеренно — в 28 % случаев, причем ***намеренные атаки на выбранные системы привели к компрометации 90 % с.д***. Поскольку различные финансовые институты обладают огромными массивами информации, относящейся к персональной, клиентской, в том числе и финансовой, именно они являются наиболее привлекательными для атак.

4. Скомпрометированные данные

Особое внимание в исследовании уделено активам, подвергшимся атакам. Так, в 2008 г. ***данные, находящиеся в сетевом доступе (online), были скомпрометированы в 94 % атак и составили 99,9 % от общего количества с.д***. 17 % атак были направлены на оконечные системы пользователей. Для сравнения, в 2004 г. число скомпрометированных данных, находящихся в сетевом доступе, составляло 73 % от общего количества. Более детальная информация по атакованным в 2008 г. активам представлена в следующей таблице.

Таблица 1. Атакованные активы в 2008 г.

Актив	Тип актива	% от числа атак	% от числа с. д.
Торговые системы (Point Of Sale – POS)	онлайн	32	6
Серверы БД	онлайн	30	75
Серверы приложений	онлайн	12	19
Веб-серверы	онлайн	10	0,004
Файловые серверы	онлайн	8	0,1
Компьютеры с общим доступом и выходом в Интернет	онлайн	2	0,4
Серверы аутентификации, каталогов	онлайн	2	0,1
Ленты резервных копий	офлайн	1	0,04
Документы	офлайн	1	0,000
Рабочие станции	оконечная система пользователя	8	0,01
Переносные компьютеры	оконечная система пользователя	4	0,000
Устройства ввода ПИН-кодов	оконечная система пользователя	2	0,004

Суммарная величина с.д. в 2008 г. превосходит общее число с.д. за предыдущие четыре года и, как уже было отмечено, ***составляет 285 млн. При этом 93 % от этого числа относятся всего лишь к пяти крупным инцидентам.***

По типу скомпрометированных данных статистика за 2008 г. следующая:

- ***данные платежных карт – 81 % инцидентов и 98 % с.д.***;
- персональная информация – 36 % и 1,5 %;
- данные аутентификации – 31 % и менее 0,1 %;
- номера счетов – 16 % и 0,5 %;
- интеллектуальная собственность – 13 % инцидентов;
- денежные активы – 11 % инцидентов;
- корпоративная финансовая информация – 6 % инцидентов;
- иные типы – 11 % инцидентов.

В результате исследования установлено, что все чаще объектом атаки становятся данные, относящиеся к платежным картам, включая номер карты, срок действия и коды верификации карты, используемые для операций без присутствия карты; данные магнитной полосы карты; ПИН-код карты. Крупные атаки на счета держателей карт в 2008 г. с использованием ПИН-кодов четко соотносятся с фактами массовой компрометации данных платежных карт в рассматриваемых инцидентах. Увеличение числа скомпрометированных данных магнитных полос платежных карт, так называемых дампов (dumps), на черном рынке привело к снижению стоимости дампа с 10–16 долл. США в середине 2007 г. до менее 0,5 долл. США в 2008 г.

Поскольку чаще всего атакам подвергались данные платежных карт, возникает вопрос: применялись ли какие-либо требования безопасности обработки этих данных в АС? В настоящее время для организаций, осуществляющих обработку данных платежных карт, обязательным является соблюдение требований Стандарта безопасности индустрии платежных карт –

Payment Card Industry Data Security Standard[3]. Стандарт содержит 12 основных требований, объединенных в 6 групп: построение и поддержание безопасной сети, защита данных держателей карт, поддержание систем управления уязвимостями, применение механизмов строгого контроля доступа, регулярный мониторинг и тестирование сетей, поддержание политики ИБ. В 81 % инцидентов организация не соответствовала требованиям стандарта или даже не проходила аудит на соответствие ему, в 19 % такое соответствие было подтверждено в результате независимой оценки Сертифицированным аудитором безопасности (Qualified Security Assessor — QSA). Требования шифрования данных при передаче по открытым сетям и использования антивирусного ПО выполнялись организациями в 68 % и 62 % случаях (проверка была осуществлена после проведения атак), однако они показали свою неэффективность, поскольку компрометация происходила в частных сетях или АС, а антивирусное ПО было неспособно выявить специально созданное для атак вредоносное ПО. Кроме того, ***40 % атакованных организаций вообще не использовали антивирусное ПО***.

В связи с этим возникает обоснованный вопрос: ***обеспечивает ли безопасность организации***, обрабатывающей данные платежных карт, соблюдение требований стандарта PCI DSS? Приведенные факты, а также крупные взломы сертифицированных на соответствие требованиям Стандарта процессинговых центров (ПЦ) Heartland Payment Systems (ежемесячно обрабатывавший 100 млн транзакций) и RBS Worldpay (скомпрометированы данные 1,5 млн держателей карт) в 2008 г. свидетельствуют об обратном [4—6]. Следует отметить, что в двух последних случаях взлома ПЦ встал вопрос о временном отзыве статуса сертифицированной организации, что подтверждено в опубликованном списке сертифицированных организаций международной платежной системы Visa International за январь 2009 г. [7]. ***Очевидно, что либо в настоящее время требования стандарта PCI DSS являются недостаточными, либо процедуры проведения аудита организаций на соответствие его требованиям нуждаются в изменениях***.

В большинстве анализируемых Verizon Business в 2008 г. инцидентов атаки были весьма протяженными во времени, в 75 % случаев они длились неделями и месяцами, при этом скорость атак несколько возросла по сравнению с предыдущим годом. Этап исследования системы перед атакой в 26 % случаев занимал у злоумышленников часы, и в 26 % случаев — месяцы. С момента проникновения в систему до компрометации в 29 % случаев проходили дни, в 27 % — считанные минуты, в 21 % — часы, в 17 % — недели. С момента компрометации до обнаружения этого факта в 49 % инцидентов проходили месяцы, в 25 % — недели, в 16 % — дни. После обнаружения факта компрометации до принятия решений по уменьшению последствий и устранению уязвимостей чаще всего требовались недели — 42 % случаев, реже дни (37 %) и месяцы (15 %). Чаще всего инциденты обнаруживаются третьей стороной — 69 % случаев, на внутреннее активное и пассивное обнаружение приходятся соответственно 24 % и 7 %. На способах обнаружения следует особенно заострить внимание.

Как показало исследование, *71 % инцидентов были выявлены на основе анализа журналов системных устройств*, а на долю систем обнаружения вторжений (Intrusion Detection System — IDS) пришлись лишь 30 %. Столь невысокая эффективность названных систем объясняется тем, что далеко не все компании их используют, некоторые приобретают, но не активируют, а в 12 % инцидентов такие системы не были настроены на мониторинг активов, подвергшихся атаке. Для сравнения, автоматизированный анализ журналов позволил обнаружить 20 % инцидентов.

Интересно, что весьма часто выявляется ситуация, когда атакованная организация обнаруживает определенное незнание своей инфраструктуры, обрабатываемой информации и привилегий пользователей. Так, неизвестные для владельца АС сетевые соединения выявлены в 24 % случаев, неизвестные привилегии — в 17 %. Также неизвестными для жертв в 38 % инцидентов

оказались сами атакованные данные, поскольку их обработка и/или хранение в системе даже не подразумевались. Однако часто неизвестное хранение оказывалось несанкционированным и осуществлялось посредством работы вредоносного ПО, внедренного злоумышленниками.

В более чем трети случаев злоумышленники пытались затруднить расследование инцидентов, применяя различные методы, включающие удаление данных (31 % случаев), сокрытие (9 %) и повреждение (3 %) данных.

Выводы

В заключение своего исследования специалисты Verizon Business утверждают, что ***87 % инцидентов могли быть предотвращены применением простых (53 %) или средних по сложности (34 %) методов и мер***, давно известных в индустрии, являющихся привычными и ежедневно используемыми (обеспечение соответствия процессов и политик ИБ, защита каналов взаимодействия с партнерами, мониторинг журналов, разработка планов реагирования на инциденты, повышение уровня осведомленности сотрудников об угрозах и уязвимостях, регулярное тестирование методов и средств защиты). Затратные и сложные меры следовало бы применить лишь в 13 % случаев.

Таким образом, анализ рассматриваемого исследования позволяет сделать ряд выводов:

1. Большая часть скомпрометированных данных относится к финансовой информации, в том числе к данным платежных карт. Активы, позволяющие злоумышленникам получать непосредственную выгоду от их компрометации, являются самыми привлекательными, а значит, должны защищаться особенно тщательно.

2. Часто инциденты случаются по причине несоблюдения элементарных процедур обеспечения безопасности в организации, а для осуществления успешных атак злоумышленникам не требуется специальных знаний.

3. Стандарт безопасности индустрии платежных карт PCI DSS не способен в настоящее время обеспечить защиту данных платежных карт, поэтому либо должен быть доработан, либо процедуры проведения аудита на соответствие его требованиям должны быть изменены.

СПИСОК ЛИТЕРАТУРЫ:

1. Network Facts. — Verizon Business [Электронный ресурс]. — Режим доступа: http://verizonbusiness.com.
2. 2009 Data Breach Investigations Report. — Verizon Business [Электронный ресурс]. — Режим доступа: http://verizonbusiness.com.
3. PCI DSS. — PCI Security Standards Council [Электронный ресурс]. — Режим доступа: https://www.pcisecuritystandards.org.
4. Heartland Payment Systems Uncovers Malicious Software In Its Processing System. — Heartland Payment Systems [Электронный ресурс]. — Режим доступа: http://www.2008breach.com.
5. Heartland Struggles To Measure Extent Of Massive Security Breach. — Dark Reading | Security | Protect The Business [Электронный ресурс]. — Режим доступа: http://www.darkreading.com.
6. RBS WorlPay Hacked, 1.5 mln. Cardholders At Risk. — Best Security Tips brings you daily news, hot topics, advices and tips about spyware, phishing [Электронный ресурс]: Security Incidents, 28.12.2008. — Режим доступа: http://www.bestsecuritytips.com.
7. List of PCI DSS Compliant Service Providers As Of 1/20/2009. — Visa USA [Электронный ресурс]. — Режим доступа: http://usa.visa.com.