Отчет группы IBM X-Force отмечает резкий рост случаев фишинга и угроз безопасности, связанных с использованием документов

Злоумышленники нацелены на легкие в использовании и обещающие крупную наживу уязвимости в Web-браузерах и программах для просмотра документов

АРМОНК, штат Нью-Йорк, 02 марта 2010 г. — Корпорация IBM (NYSE: IBM) сегодня представила результаты исследования, опубликованные в ежегодном отчете группы IBM X-Force® о тенденциях и рисках информационной безопасности по итогам 2009 года (2009 Trend and Risk Report). Результаты и выводы, приводимые в отчете, свидетельствуют, что существующие ИТ-угрозы, такие как фишинг (разновидность интернет-мошенничества) и уязвимости форматов документов, продолжают расти, несмотря на то, что большинство клиентов предприняли определенные шаги для улучшения безопасности.

В отчете IBM X-Force® приводятся три основных вида угроз, которые показывают, что атакующие все чаще нацеливаются на людей, используя Интернет для кражи их денег или информации. За прошедший год отмечен стремительный рост количества вредоносных Web-ссылок. Во втором полугодии 2009 года также резко увеличилось число случаев онлайнового финансового мошенничества, называемого фишингом (хакерский прием, направленный на незаконное получение конфиденциальной персональной информации через электронную почту при помощи запросов, которые выглядят как официальные письма). Продолжает быстро расти и число уязвимостей программ для просмотра и редактирования документов, особенно документов формата Portable Document Format (PDF).

Среди других тенденций и рисков ИТ-безопасности, отмеченных в отчете X-Force по итогам 2009 года:

- **Число новых уязвимостей уменьшилось, но пока еще остается на рекордно высоких уровнях.** В целом, в 2009 году была выявлена 6601 уязвимость, что на 11% меньше, чем в 2008 году. В отчете отмечается снижение числа зловредных «новинок» в самых распространенных категориях уязвимостей, таких как "SQL injection" (SQL-инъекция, когда злоумышленники внедряют вредоносный код в программы легитимных Web-сайтов (обычно с намерением инфицировать машины их посетителей) и ActiveX (подключаемый модуль Web-браузера Internet Explorer для выполнения специальных задач). Эта тенденция может указывать на то, что некоторые из наиболее легко обнаруживаемых уязвимостей в этих категориях были устранены, и общая безопасность улучшилась.

- **В ряде ключевых категорий значительно уменьшилось число опасных и критических уязвимостей, не устраненных с помощью программных «заплаток» (patch).** Количество уязвимостей в Web-браузерах и программах просмотра/редактирования документов, в целом, уменьшилось, что свидетельствует о большей активности поставщиков в борьбе с угрозами безопасности.

- **Существенно растет число случаев выявления уязвимостей в программах просмотра и редактирования документов и в мультимедийных приложениях.** В 2009 году было обнаружено более чем на 50% больше уязвимостей этих категорий, чем в 2008 году.

- **По всему миру также стремительно растет число новых вредоносных Web-ссылок.** За период с 2008 года по 2009 год их количество увеличилось на 345%. Эта

тенденция служит еще одним доказательством того, что злоумышленники вполне успешны в хостинге вредоносных Web-страниц, а также того, что уязвимости, связанные с Web-браузерами, и их эксплуатация приносят, по всей видимости, серьезный доход.

- **Уязвимости Web-приложений продолжают оставаться крупнейшей категорией обнаруживаемых угроз безопасности.** Число уязвимостей Web-приложений, выявляемых организациями, не уменьшается, и они не становятся менее опасными. Сорок девять процентов всех уязвимостей связаны с Web-приложениями, причем по числу обнаруженных уязвимостей технология взлома Cross-Site Scripting (также известная как XSS-атака, когда атакующий пытается внедрить клиентский скрипт, который будет в дальнейшем выполнять нужные для злоумышленника действия) опережает SQL-инъекции и имеет все шансы занять первую строчку этого своеобразного антирейтинга. По состоянию на конец 2009 года не были устранены 67% уязвимостей Web-приложений.

- **Значительно выросло число Web-атак с маскировкой.** Часто запускаемые с помощью автоматического инструментария для «эксплуатации» Web-уязвимостей, многие атаки используют технологию маскировки их нападений на Интернет-браузеры, пытаясь скрыть эти эксплоиты (программный код, «эксплуатирующий» уязвимости в программном обеспечении для проведения атак) в документах и на Web-страницах, чтобы избежать обнаружения системами информационной безопасности. В 2009 году услуги IBM по управлению безопасностью из портфеля IBM Managed Security Services помогли выявить в 3-4 раза больше подобных атак с маскировкой по сравнению с 2008 годом.

- **Число случаев фишинга, которое уменьшилось по итогам первого полугодия прошлого года, вновь резко подскочило к концу 2009 г.** Большинство фишинговых атак в 2009 году организовывалось из Бразилии, США и России, которые вытеснили Испанию, Италию и Южную Корею с первых позиций в отчете 2008 года.

- **Фишинговые атаки по-прежнему активно используют возможности финансовой индустрии в своих противозаконных целях по обману потребителей.** Одни модели фишинга ориентированы на «выуживание» регистрационных имен и паролей, другие пытаются обманом заполучить конфиденциальную персональную информацию пользователей при помощи якобы официальных запросов от государственных организаций. В целом по отрасли, 61% фишинговых электронных писем отправляются мошенниками как бы от финансовых институтов, тогда как 20% выглядят как официальные письма государственных организаций.

«Несмотря на постоянно меняющуюся ситуацию с угрозами информационной безопасности, поставщики решений улучшили свою работу по борьбе с уязвимостями, — считает Том Кросс (Tom Cross), руководитель отдела IBM X-Force Research. — Совершенно очевидно, однако, что злоумышленников это не отпугнуло, поскольку использование вредоносных эксплоитов на Web-сайтах растет беспрецедентными темпами».

Группа исследований и разработок IBM X-Force® занимается каталогизацией, анализом и изучением уязвимостей ИТ-безопасности с 1997 года. Каталог X-Force, содержащий более 43000 уязвимостей, является крупнейшей в мире базой данных уязвимостей программного кода. Эта уникальная база данных помогает специалистам X-Force лучше понять динамику процесса, что помогает в исследовании известных уязвимостей и эффективном выявлении новых угроз.

«IBM продолжает инвестировать в стратегические исследования подобно этому с целью создания конкурентных преимуществ для наших клиентов и для пользы всей индустрии безопасности в целом, — подчеркнул Эл Золлар (Al Zollar), генеральный менеджер подразделения IBM Tivoli Software, входящего в IBM Software Group. — Благодаря знаниям, которые дает нам наша исследовательская группа X-Force, а также с помощью наших профессиональных услуг и сервисов по управлению безопасностью, мы можем помочь в создании и эксплуатации самых защищенных ИТ-инфраструктур, удовлетворяя нужды клиентов по управлению рисками, управлению и контролю безопасности и соблюдению нормативных требований регулятивных органов».

Корпорация IBM является одним из ведущих мировых поставщиков решений для обеспечения информационной безопасности и управления рисками. Через предложения своих продуктов, профессиональных услуг в области безопасности и услуг по управлению безопасностью, IBM предоставляет клиентам гибкость выбора и широкий спектр решений по ИТ-защите как доверенный и компетентный в этой сфере партнер. Клиенты со всего мира сотрудничают с IBM в стремлении уменьшить сложность своей системы безопасности и стратегически управлять рисками. Ни один из поставщиков не может предложить такой профессиональный уровень и такую эффективность комплексных решений и услуг для обеспечения информационной безопасности и управления рисками, как IBM – от целевых исследований, аппаратных средств и программных продуктов до специализированных сервисов и глобальной сети бизнес-партнеров. Благодаря сочетанию этих преимуществ IBM может оказать клиентам эффективную помощь в укреплении информационной защиты их бизнес-операций и внедрении интегрированной системы управления рисками в масштабе организации.

Для получения более подробной информации о тенденциях развития технологий информационной безопасности и прогнозах IBM о состоянии информационной безопасности, включая статистические графики и диаграммы, посетите Web-сайт IBM по адресу www.ibm.com/security/xforce , где опубликована полная версия отчета группы IBM X-Force.