ОЦЕНКА РЫНКА КИБЕРПРЕСТУПНОСТИ В РОССИИ

Курбанов Али Омарович
Дагестанский Государственный Университет, Факультет информатики и информационных технологий (367000, республика Дагестан, г.Махачкала, ул.Дзержинского, 12), e-mail: ali051996@list.ru

Данная статья посвящена краткому обзору статистики киберпреступлений, совершенных по отношению к российским компаниям и организациям. Рассмотрены наиболее распространенные виды компьютерных преступлений, также представлены их доли на рынке киберпреступности. В результате анализа деятельности киберпреступников за последние 3 года был выявлен общий заработок преступников. А также в статье отражены наиболее популярные организации, которые являются целями незаконных действий киберпреступников.

Ключевые слова: киберпреступность, анализ рынка киберпреступности, Group-IB, БСТМ МВД.

CYBERCRIME ASSESSMENT OF THE MARKET IN RUSSIA

Kurbanov Ali Omarovich
Dagestan State University, Faculty of Informatics and Information Technologies (367000, Republic of Dagestan, Makhachkala, Dzerzhinsky, 12) e-mail: ali051996@list.ru

This article provides a brief overview of cybercrime statistics, committed against Russian companies and organizations. The most widespread types of computer crimes, as represented by their share of the cybercrime market. An analysis of the activities of cyber criminals overall earnings have been identified over the past 3 years. Also in the article the most popular organizations, which are the objectives of the illegal actions of cybercriminals.

Key words: cybercrime, market analysis cybercrime, Group-IB, BSTM MVD.

Подобно многим революционным технологиям, глобальная сеть Internet предоставляет огромные возможности, как для прогресса, так и для злоупотреблений. Атаки в сети, мошенничества с пластиковыми платежными карточками, кражи средств на банковских счетах, корпоративный шпионаж, распространение детской порнографии - это лишь некоторые преступления, которые дубятся в сети Internet. Такие противоправные деяния составляют для нашего государства, как и для многих других стран мира, значительную общественную опасность, реально угрожая информационной безопасности - составляющей национальной безопасности.[2]

С целью обеспечения информационной безопасности организованны множество компаний. Некоторые занимаются разработкой программных продуктов, призванных обеспечить целостность и сохранить конфиденциальность информации. К ним относятся такие организации как «Лаборатория Касперского», Softlin, Информзащита и тд. А расследованием инцидентов нарушений информационной безопасности занимаются Бюро специальных технических мероприятий МВД России (БСТМ МВД), Group-IB (Группа Информационной Безопасности) и тд.

По данным Бюро специальных технических мероприятий МВД России (БСТМ МВД), число компьютерных преступлений в России в 2013 году увеличилось на 8,6%. Основным

мотивом киберпреступников стало извлечение материальной выгоды, отмечают в правоохранительных органах. Практически все случаи неправомерного доступа к информации (19% от всех компьютерных преступлений) направлены на хищение денежных средств. Количество преступлений, организованных с целью хулиганства, крайне незначительно.

В 2013-2014 гг. наиболее крупная доля компьютерных преступлений, по данным БСТМ МВД, приходится на мошенничество (37%), за которым следует неправомерный доступ к компьютерной информации (19%) и распространение детской порнографии (16%). По 8% от всех совершенных за этот период компьютерных преступлений приходится на компьютерное пиратство и распространение вредоносных программ.

В числе основных тенденций компьютерной преступности в БСТМ МВД отмечают, что все большее число традиционных видов преступлений перемещается в сеть, все большее число преступление совершается из корыстных целей, а целью преступников все чаще становятся мобильные устройства.

За первую половину 2014 года в России было зарегистрировано более 7 тыс. киберпреступлений. По итогам 2013 года их количество превысило 11 тыс. [3]

По данным отчета Group-IB(рис.1), со второй половины 2013 года по первую половину 2014 года русскоговорящие киберпреступники заработали в России и СНГ порядка $2,5 млрд. Из указанной суммы $426 млн пришлось на интернет-мошенничество, существенная часть которого - $289 млн - происходит в системах интернет-банкинга. На обналичивании денежных средств в России киберпреступники заработали $59 млн, на банковском фишинге и мошенничестве с электронными деньгами - $50 млн, на хищении электронных денег - $28 млн.

Тренд (млн. $)	2011	2012	2013-14
Интернет-мошенничество, итого:	**697**	**615**	**426**
Мошенничество в системах интернет-банкинга (России и СНГ)	490	446	289
Обналичивание денежных средств	122	89	59
Банковский фишинг и мошенничества с электронными деньгами	55	57	50
Хищение электронных денег	30	23	28
Кардинг, итого:			**680**
Кардинг			680
Итого:			
Спам, итого:	**830**	**786**	**841**
Спам	553	493	549
Медикаменты и различная контрафактная продукция	142	173	180
"Поддельное" программное обеспечение	135	120	112
Внутренний рынок (C2C), итого:	**230**	**261**	**288**
Продажа трафика	153	167	196
Продажа эксплоитов	41	52	48
Продажа загрузок	27	33	35
Предоставление услуг по анонимизации	9	9	9
DDoS-атаки, итого:	**130**	**110**	**113**
DDoS-атаки	130	110	113
Иное, итого:	**168**	**166**	**153**

Рис.1 Оценка рынка киберпреступности в России и СНГ

Впервые в Group-IB отдельным пунктом оценили и объем денежных средств, украденный при мошенничестве с платежными картами в России: согласно отчету, в 2013-2014 гг. он составил порядка $680 млн. В свою очередь, на спаме в 2013-2014 гг. «высокотехнологичные преступники» заработали $841 млн, на DDoS-атаках - $113 млн.

Основная часть киберпреступлений совершается в отношении организаций финансового сектора и госсектора, отмечают в Group-IB. В последнем киберпреступления чаще всего совершаются в целях промышленного шпионажа. При этом увеличивается число целевых атак на такие организации. За 2013-2014 гг. злоумышленники провели более 35 успешных атак на банки, а среди других организаций, связанных с финансовым сектором, ставших жертвами киберпреступников - Qiwi, «Почта России», «Московская Биржа ММВБ-РТС». В случае с Qiwi, в частности, злоумышленники похитили 88 млн руб., о чем компания упомянула в своем годовом отчете для иностранных частных эмитентов. .[3]

В Group-IB отмечают, что из известных им целевых атак на банки только в 3% случаев организация выявили их сами. В 28% случаев атаки были выявлены после того, как в банке случился инцидент, а в 69% случаев об атаках банки оповестила сама Group-IB. .[3]

В госсекторе среди объектов атак - Администрация Президента Республики Башкортостан, где на 5 компьютерах было обнаружено вредоносное ПО, а конечной целью злоумышленников являлась финансовая информация в системе «БашФин». Атакам киберпреступников также подверглись Департамент здравоохранения Москвы, ФГУП «Главный центр специальной связи» и ряд других. .[3]

В числе тенденций на рынке киберпреступности в России помимо целевых атак в Group-IB выделяют возрастающую долю мобильных угроз. Согласно исследованиям мобильных бот-сетей, 40% пользователей мобильных устройств имеют счет в банке, привязанный к зараженному мобильному телефону. .[3]

Серьезной проблемой в сфере борьбы с киберпреступностью в России в Group-IB отмечают тот факт, что несмотря на увеличивающееся число преступлений остается актуальной нехватка специалистов в правоохранительных структурах, которые ими занимаются.[3]

Список литературы

1. Воронина Ю. Специалисты оценили ущерб экономики РФ от киберпреступности // Редакция «Российской газеты» [электронный ресурс]. – Режим доступа: https://rg.ru/2016/04/13/ekonomika-rf-poteriala-bolee-203-mlrd-rublej-ot-kiberprestupnosti.html (дата обращения 26.05.16)
2. Киберпреступность – угрозы и прогнозы // Служба реагирования на компьютерные инциденты [электронный ресурс]. – Режим доступа: http://kz-cert.kz/ru/presscenter/publication/?doc=23 (дата обращения 26.05.16)
3. Киберпреступность и киберконфликты: Россия // TADVISER. Государство. Бизнес. ИТ [электронный ресурс]. – Режим доступа: http://tadviser.ru/a/240126 (дата обращения 26.05.16)
4. О компании // GROUP IB [электронный ресурс]. – Режим доступа: http://www.group-ib.ru/about.html (дата обращения 26.05.16)
5. Преступления в сфере информационных технологий // Википедия Свободная энциклопедия [электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_технологий (дата обращения 26.05.16)