Автор: Леонид Чуриков РАССЛЕДОВАНИЯ, ИРКУТСК 6077 02.04.2012, 13:15 749

Преступная сеть

Нынешней весной сотрудники МВД задержали банду интернет-грабителей банков в полном составе. Впервые в России удалось выявить всю цепочку преступной группы, включая организатора, владельца сети зараженных компьютеров, с которой велись атаки на клиентов банков, и «вирусописателя».

Информацию о раскрытии этого дела одновременно распространили МВД и компания Group IB, помогавшая правоохранительным органам в расследовании. Преступников, которыми оказались восемь россиян, в первую очередь интересовали корпоративные клиенты банков, использующие системы дистанционного банковского обслуживания («Банк-Клиент»). Для получения контроля над средствами пользователей систем интернет-банкинга хакеры использовали сеть зараженных компьютеров, большинство из которых (95%) расположены на территории России. За кражу денег отвечали вредоносные программы Win32/Carberp и Win32/Rdpdor.

Различий между богатыми и бедными, также как и между госучреждениями и частниками, преступники не делали и грабили всех подряд. По словам генерального директора компании Group IB Ильи Сачкова, в числе пострадавших оказались и крупные, и небольшие коммерческие структуры, а также оборонные предприятия и индивидуальные предприниматели. Забирали все практически до копейки — у одной из компаний мошенники похитили примерно 15 тыс. рублей. Максимальная сумма, которую злоумышленникам удалось похитить, составила около 21 млн рублей.

По словам экспертов Group IB, в числе пострадавших — клиенты крупнейших российских и международных банков, назвать имена которых (кроме Сбербанка) не позволяет тайна следствия. При этом большинство обманутых фирм ведет свой бизнес на территории РФ. Но здесь уже география преступлений была очень обширна: Москва, Санкт-Петербург, Ростов-на-Дону, Новосибирск, Хабаровск, Екатеринбург. И это далеко не полный перечень городов, до которых «дотянулись» интернет-мошенники.

Самым сложным в расследовании киберпреступлений является сбор материалов, подтверждающих причастность мошенника к конкретному уголовному делу. Здесь, как заявляют в организациях, причастных к расследованию, особую сознательность проявил Сбербанк, который не только финансировал работы по проводимым исследованиям, но и осуществлял сбор и предоставление необходимой информации правоохранительным органам. Данные о пострадавших клиентах были корректно сохранены Сбербанком и другими кредитными учреждениями и оперативно передавались на исследование. Это позволило подтвердить причастность конкретной преступной группы к 27 хищениям у клиентов Сбербанка на общую сумму более 10 млн рублей, а также хищениям у клиентов других коммерческих банков на общую сумму более 30 млн рублей.

Помощь следствию оказывали зарубежные банки (через российские представительства), иностранные спецслужбы и частные организации, специализирующиеся на расследовании киберпреступлений. В Group IB, в частности, отмечают содействие со стороны голландской организации FOX-IT, с которой российские киберполицейские сотрудничают на протяжении двух лет. В данном случае у голландцев был прямой интерес — ликвидированная преступная группа действовала в том числе и против клиентов нидерландских банков.

Процесс сбора доказательств компьютерных преступлений против клиентов банков в Group IB описывают следующим образом. После обращения пострадавшего на место инцидента отправляется специалист для сбора цифровых доказательств. Затем данные доставляются в лабораторию компьютерной криминалистики на исследование, что помогает восстановить хронологию событий и раскрыть детали совершенного хищения. Отчет криминалистов передается в отдел расследования, сотрудники которого выявляют панели управления вредоносным программным обеспечением и собирают о них детальные сведения. Это позволяет установить личность злоумышленника, управляющего бот-сетью (сетью зараженных вирусом компьютеров, с которых велись атаки), и его фактическое местонахождение. В дальнейшем полученная информация передается правоохранительным органам, которые уже начинают проводить оперативно-разыскные и следственные мероприятия.

Поимка киберпреступников не гарантирует того, что всем пострадавшим от интернет-мошенников будут возвращены украденные средства. Следует знать, что возместить ущерб можно только в рамках судебного

разбирательства и в каждом случае необходимо иметь заключение эксперта, который в ходе криминалистического исследования определяет, действительно ли компания пострадала от рук конкретной преступной группы.

Общая сумма, украденная ныне арестованными грабителями за два года существования группировки, не называется, но, по информации Group IB, только за последний квартал злоумышленникам удалось похитить 130 млн рублей. Такой масштаб проблем, созданных всего-навсего восемью преступниками, не может не настораживать. Обнадеживающим же можно считать тот факт, что постепенно в России создается оперативная система взаимодействия банков, российских и иностранных спецслужб и частных организаций, направленная на противодействие киберпреступности.

Источник: banki.ru

Автор: Леонид Чуриков © Babr24.com РАССЛЕДОВАНИЯ, ИРКУТСК 6077 02.04.2012, 13:15 749
URL: https://babr24.com/?ADE=104333 Bytes: 5042 / 5035 Версия для печати

Автор текста: **Леонид Чуриков**.

Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта