Dp.ru, Санкт-Петербург, 8 февраля 2017

МВД ЛИКВИДИРОВАЛО КРУПНЕЙШУЮ В РОССИИ ГРУППИРОВКУ БАНКОВСКИХ КИБЕРПРЕСТУПНИКОВ

Автор: Виталий Алексеев

МВД отчиталось о завершении масштабной операции по ликвидации группировки хакеров: она, по данным силовиков, могла привести к коллапсу банковскую систему РФ. Аналитики в сфере кибербезопасности подтверждают, что задержаны представители одной из крупных группировок, но на свободе остаются их не менее опасные конкуренты.

Сотрудники МВД и ФСБ в ходе масштабной операции пресекли деятельность группировки хакеров, которая действовала с 2013 года. По данным пресс-службы МВД, 50 участников хакерской ОПГ из 17 регионов страны за несколько лет сняли больше 1 млрд рублей со счетов клиентов российских банков. Они также проникали в системы критически важной инфраструктуры, в том числе на стратегических промышленных предприятиях.

Полицейские провели обыски по 34 адресам, изъяли свыше 90 единиц компьютерной техники, носителей информации и средств связи, а также 4,5 млн рублей наличными и холодное оружие. 27 организаторов и участников группы привлечены к уголовной ответственности, из них 19 подозреваемых отправили в СИЗО. Фигурантам дела предъявлено обвинение в организации преступного сообщества и мошенничестве в сфере компьютерной информации. Этот этап операции был завершен в мае 2016 года.

В конце января 2017 года в пяти регионах России (Москва, Петербург, Краснодарский край, Тверская и Свердловская области) были задержаны еще девять хакеров - авторов "банковского трояна" Lurk и участников одноименной группировки киберпреступников. Источник Интерфакса подтвердил, что эта группировка причастна к целому ряду хакерских атак, в том числе на сайты российских СМИ и отечественные банки.

Облава на ОПГ

В феврале прошлого года о задержании некоторых членов этой группировки хакеров рассказал глава управления по борьбе с преступлениями в сфере компьютерной безопасности МВД Алексей Мошков. На Инфофоруме-2016 он заявил, что киберпреступники планировали не только парализовать банковскую систему РФ, атаковав банки из первой сотни, но и организовать нападение на кредитно-финансовые учреждения США, ЕС и Азии.

Операция по ликвидации ОПГ проводилась в несколько этапов. Под наблюдение силовиков и сотрудников служб безопасности банков преступники попали еще в начале 2015 года, задержания руководства группировки прошли уже в ноябре, следующим этапом стала операция в июне 2016-го при участии Сбербанка, ликвидация ОПГ в мае 2016 года и арест подозреваемых в начале 2017 года, о чем сегодня сообщило МВД.

Группировкой руководил 30-летний москвич, с ним были знакомы только четверо подчиненных, курировавшие десяток групп по разным направлениям, пояснил "Фонтанке" представитель управления "К" Александр Вураско. Хакеры арендовали несколько офисов в Москве, а также загородный дом в Подмосковье с тренировочной базой для скиммеров, где и прошли основные задержания киберпреступников.

Помимо атак на банковскую инфраструктуру хакеры занимались установкой скимминговых устройств на банкоматы, созданием программно-аппаратных комплексов, позволяющих получать контроль над банковскими терминалами, разработкой программ для взлома онлайн-банкинга, а также систем, которые стоят в самих организациях и позволяют с компьютера бухгалтера перемещать деньги на счетах, находящихся в банке.

Банковский троян Lurk, о котором говорят силовики, известен минимум с 2011 года. Его разработку и практическое применение следствие приписывает группе, задержанной еще в июне 2016 года в результате совместной операции ФСБ и МВД, поясняют в ESET. "Полная информация о количестве участников хакерской группы, жертвах и инцидентах будет доступна после завершения расследования. Идентифицировать участников кибератаки в принципе затруднительно, а делать выводы без исчерпывающих доказательств - недопустимо", - подчеркивает глава отдела технического маркетинга ESET Russia Алексей Оськин.

Ущерб на 12 млрд рублей

По оценкам главы компании Group-IB (предотвращение и расследование киберпреступлений) Ильи Сачкова, в 2016 году потери российского бизнеса от кибератак составили около 12 млрд рублей, максимальную сумму хищения при одной атаке эксперт оценил в 600 млн рублей. Помимо группировки Lurk, в России действуют еще несколько крупных сообществ киберпреступников, наносящих миллиардный ущерб банкам.

В частности, группировке Buhtrap в период с августа 2015-го по январь 2016-го удалось осуществить серию успешных атак на российские банки на общую сумму 1,8 млрд рублей. Руководитель сервиса кибербразведки Bot-Trek Intelligence Дмитрий Волков отмечал, что такие группировки, как Anunak, Corkow, Buhtrap - это только три из пяти активных групп, атакующих банки России.

"Уже сейчас мы видим еще две группы, которые только готовятся к атакам на банки. Традиционные средства защиты не способны предотвратить их. Эволюция угроз для финансового сектора требует повышения эффективности защиты банков и понимания действий атакующих, в том числе на основе данных кибербразведки", - отмечал эксперт в докладе "Buhtrap: эволюция целенаправленных атак на банки".

По оценкам аналитиков, средняя сумма хищения в результате хакерской атаки на банки составляет 140 млн рублей. В 2017 году эксперты в сфере цифровой безопасности ожидают прироста числа инцидентов с участием русскоязычных хакеров, которые, получив успешный опыт в атаках на банки России и Украины, будут уходить в другие регионы мира.

Согласно отчету Group IB, команды хакеров, занимавшиеся логическими атаками на банкоматы, будут пробовать себя в атаках на банковскую систему SWIFT, будут появляться новые инструменты и сервисы для целевых атак, хакеры начнут уделять больше внимания поиску инсайдеров для предоставления нужной информации и первичного заражения.

https://www.dp.ru/a/2017/02/08/MVD_likvidirovalo_krupnej/