СВЯЗАННЫЕ ОДНОЙ СЕТЬЮ

В ПОСЛЕДНЕЕ ВРЕМЯ ПРЕСТУПЛЕНИЯ В ИНТЕРНЕТЕ СТАЛИ ЕДВА ЛИ НЕ БОЛЕЕ РАСПРОСТРАНЕННЫМ ЯВЛЕНИЕМ, ЧЕМ ПРИВЫЧНАЯ УЛИЧНАЯ ПРЕСТУПНОСТЬ. ГЛАВНАЯ ОПАСНОСТЬ ЗЛОДЕЯНИЙ, СОВЕРШАЕМЫХ В ГЛОБАЛЬНОЙ СЕТИ, СОСТОИТ В ТОМ, ЧТО ДЛЯ КИБЕРПРЕСТУПНИКОВ НЕ СУЩЕСТВУЕТ ГРАНИЦ. А ЗНАЧИТ, У ЕВРОПЕЙСКОГО СОЮЗА И РОССИИ НЕТ ИНОГО ВЫХОДА, КРОМЕ КАК ИСКАТЬ СПОСОБЫ СОВМЕСТНОГО ПРОТИВОСТОЯНИЯ ОБЩЕМУ ВИРТУАЛЬНОМУ ПРОТИВНИКУ. ЕЛЕНА КУШНИР

СЕТИ РАЗДОРА В этом году Европейский союз впервые столкнулся с массированной атакой хакеров против одного из своих членов. Апрельские события в Эстонии, связанные с переносом советского Бронзового солдата с таллинской площади Тынисмяги на кладбище Фильтри-Тее, привели не только к политическому противостоянию России и небольшой прибалтийской республики. После того как по инициативе эстонских властей монумент воину-освободителю сменил место дислокации, серверы эстонских государственных учреждений стали мишенями виртуальных мстителей, недовольных демонтажем памятника. Синхронным атакам подверглись сайты парламента, президента, госканцелярии, МИДа, минобороны, крупнейших банков и газет. Продолжавшиеся несколько недель кибератаки почти парализовали эстонскую банковскую систему и временно вывели из строя правительственные серверы.

Виртуальный противник застал эстонские власти врасплох. Дело в том, что для Эстонии сфера IT имеет столь же важное значение, как, к примеру, нефтегазовая отрасль для России. Республика считает себя родиной компьютерных гениев, среди которых разработчики интернет-телефона Skype и ведущие сотрудники компании Microsoft. Кабинет министров страны гордится тем, что давно отказался от бумажного делопроизводства и перешел на систему «электронного государства».

Неудивительно, что после мощных кибератак Таллин забил тревогу, позвав на помощь европейское сообщество и даже НАТО. Некоторые эстонские официальные лица заявляли о причастности российских структур к организации этих атак. Фактически Таллин намекнул на то, что кибератаки были санкционированы Кремлем. От Европейского союза потребовали оперативно отреагировать на угрозу.

Чтобы на месте разобраться с ситуацией, в Таллин прибыл внушительный десант экспертов из ЕС, НАТО и США. А в кулуарах Европейского союза стали всерьез поговаривать о том, что следует изучить возможность внесения изменений в профильные правовые акты. За Эстонию вступился и Европейский парламент, принявший специальную резолюцию по этому поводу, в которой говорилось, что атаки против одной из стран—членов ЕС стали проверкой солидарности всей организации.

В Москве подобные обвинения назвали несостоятельными. Российский сенатор Михаил Маргелов, кстати возглавляющий группу европейских демократов в ПАСЕ, признал, что парализующие компьютеры атаки хакеров действительно напоминают терроризм, заявив при этом, что они проводятся «не только против Эстонии, но и против частных и правительственных институтов многих государств». Тем самым Россия фактически признала наличие общей проблемы виртуальной уязвимости и продемонстрировала желание бороться с этим явлением.

РЕАЛЬНАЯ ВИРТУАЛЬНОСТЬ Эстония стала самым громким примером того, как целая страна может стать жертвой распоясавшихся хакеров. Между тем от активности виртуальных преступников ежедневно страдают тысячи реальных граждан по всему миру, и Европейский союз не исключение. Так, специалисты криминологической компании 1871 Ltd, исследовавшей уровень преступности в британском сегменте интернета, обнаружили, что в 2006 году в сети было совершено около 3 млн правонарушений.



AFP

В ЭТОМ ГОДУ ЕС РЕШИЛ УДВОИТЬ КОНТРОЛЬ ЗА ТЕМ, КТО И В КАКИХ ЦЕЛЯХ ИСПОЛЬЗУЕТ ИНТЕРНЕТ

Экспертами подсчитано, что большинство преступлений касаются онлайн-перебранок с элементами угроз, оскорблений и шантажа. Однако в сети нередко совершаются и менее безобидные злодеяния — взломы компьютеров с последующим похищением базы данных, а также преступления в сексуальной сфере. Особое место в сфере IT-преступлений занимают финансовые махинации с кредитными картами и банковскими счетами. Такой вид интернет-мошенничества, прозванный фишингом, заключается в том, что преступники всеми возможными способами пытаются выведать конфиденциальную информацию о личности или финансовой деятельности пользователей всемирной паутины, в частности пароли и данные о кредитных картах. От такого вмешательства в частную жизнь не застрахован никто, причем вне зависимости от страны проживания. К примеру, в прошлом месяце полиция Германии задержала десять человек, подозреваемых в совершении преступлений в сети интернет. Среди задержанных есть граждане России, Украины и Германии. Злоумышленники избирали своей мишенью клиентов банков и рассылали на электронные адреса жертв письма от имени таких известных компаний, как eBay (интернет-аукцион) или Deutsche Telekom. В почтовых файлах содержались шпионские вирусы, позволявшие взламывать системы безопасности компьютеров жертв и получать необходимые данные для дальнейших операций с их кредитками.

В списке интернет-преступлений числится также незаконная деятельность в сфере сексуальных услуг: за последний год эксперты отмечают резкий рост числа интернет-ресурсов педофильской направленности. Глобальную сеть также нередко используют для пропаганды насилия, национальной розни, экстремизма и терроризма. Нынешним летом в России наделал много шума интернет-ролик, в котором была показана казнь выходцев из Таджикистана и Дагестана. В нем палачи, именовавшие себя боевым крылом радикального Национал-социалистического общества, известного организацией митингов скинхедов и разгромом гей-парадов, жестоко расправились с двумя молодыми людьми нерусской национальности. Расследованием дела, вызвавшего общественный резонанс, занялось специализированное управление «К» МВД РФ. После появления ролика в России с новой силой заговорили о необходимости ограничения свободы в интернете. «Интернет — это единственное место, где такую запись сейчас можно разместить. Это лишний раз говорит о том, что над сетью нужен контроль, чтобы ограничить появление таких роликов в будущем. Если эти фашисты будут знать, что их деяния никто не будет транслировать публично, степень их ненависти будет на порядок меньше»,— заявил тогда глава комиссии по толерантности Общественной палаты Валерий Тишков.

ПРАВОВЫЕ ПУТЫ И в России, и в Европейском союзе осознают, что борьбу с киберпреступностью и кибертерроризмом невозможно вести обособленно. А значит, вне зависимости от внешнеполитической конъюнктуры Москве и Брюсселю придется вырабатывать совместную стратегию противодействия сетевым преступникам. Российская столица уже не раз становилась площадкой проведения международных конференций по вопросам борьбы с киберпреступностью. Например, в прошлом году в таком мероприятии, проходившем с привлечением порядка 200 экспертов из 50 стран мира, принимал участие глава МВД РФ Рашид Нургалиев, представители Госдумы и Совета безопасности России. Министр тогда признал, что побочным эффектом развития телекоммуникаций является рост криминальной активности в данной области, и выразил готовность участвовать в «построении современного безопасного общества, основанного на широком применении информационных технологий».

Между тем помимо деклараций эффективное противостояние киберпреступникам требует совершенствования законодательных инструментов. Еще в 2003 году Европейский совет по телекоммуникациям принял решение о создании Европейского агентства по безопасности сетей и информации, задачей которого является предотвращение кибератак на ключевые информационные ресурсы Европы. Но уже в мае этого года на волне эстонских событий Европейская комиссия решила активизировать деятельность в этом направлении и приняла специальное коммюнике, касающееся общей политики ЕС по борьбе с правонарушениями в сфере интернета. По словам комиссара ЕС Франко Фраттини, ответственного за юстицию, свободу и безопасность, подобная политика наряду с улучшенным взаимодействием между членами ЕС должна предусматривать политическое и правовое сотрудничество с третьими странами.

В упомянутом коммюнике предпринята попытка классифицировать злодеяния в сети. Для удобства их разделили на три категории: традиционные формы преступления типа мошенничества или подделки, распространение в киберпространстве публикаций незаконного содержания — сексуальных материалов или подстрекательств к расовой ненависти, атаки информационных систем. Однако список явно будет расширяться, поскольку быстрое развитие интернета и других информационных систем открывает для преступников новые возможности использования глобальных сетей в своих целях. В ЕС также признают, что правоприменительная деятельность в области интернета испытывает сейчас определенные затруднения, ведь преступник и жертва нередко живут в разных уголках Европы, а то и мира. Вдобавок пока не существует никакого согласованного определения киберпреступления. Поэтому на первых порах Франко Фраттини предложил заняться координацией совместных мер противодействия сетевым злоумышленникам, подчеркивая, что борьбу с ними следует вести на национальном, общеевропейском и международном уровне, причем ее обязательным условием должно стать взаимодействие между полицейскими органами и частными интернет-операторами.

Приступить к практическому воплощению планов по борьбе с виртуальными противниками в ЕС собираются уже этой осенью. На ноябрь запланировано проведение внутриевропейской конференции по сотрудничеству государственных органов и частного сектора, на которой планируется обсудить противодействие распространению детской порнографии. В дальнейшем Европейский союз планирует взять на себя активизацию международного сотрудничества в области создания системы интернет-безопасности. Это означает, что в Брюсселе растет понимание важности значения сотрудничества с Россией в этой сфере. ■

И В РОССИИ, И В ЕВРОПЕЙСКОМ СОЮЗЕ ОСОЗНАЮТ, ЧТО БОРЬБУ С КИБЕРПРЕСТУПНОСТЬЮ И КИБЕРТЕРРОРИЗМОМ НЕВОЗМОЖНО ВЕСТИ ОБОСОБЛЕННО. А ЗНАЧИТ, МОСКВЕ И БРЮССЕЛЮ ПРИДЕТСЯ ВЫРАБАТЫВАТЬ СОВМЕСТНУЮ СТРАТЕГИЮ ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ ПРЕСТУПНИКАМ

САМЫЕ ГРОМКИЕ ХАКЕРСКИЕ АТАКИ В ЕВРОПЕ И РОССИИ

11 февраля 2000 года хакеры взломали сайт агентства «Росбизнесконсалтинг», на котором разместили от имени «чеченских вооруженных сил» текст с объявлением РФ партизанской войны.

5 февраля 2001 года хакерская группа Virtual Monkeywrench, взломав сервер Международного экономического форума в Давосе, похитила конфиденциальную информацию о его участниках, среди которых были Билл Гейтс, Ясир Арафат, Кофи Аннан. Номера кредитных карточек, паспортов и мобильных телефонов они поместили в открытый доступ. Виновных не нашли.

4 февраля 2002 года хакеры организовали атаку на серверы одного из старейших британских интернет-провайдеров Cloud Nine Communications. Ущерб был настолько велик, что вскоре компания прекратила работу.

В 2003 году испанец Сантьяго Гарридо использовал компьютерного червя для организации DDoS-атаки (отправка большого количества ложных запросов на сервер, приводящая к сбоям в его работе) на IRC-чат Hispano, откуда его изгнали за неподобающее поведение. В результате без выхода в сеть временно остались около трети интернет-пользователей Испании. 9 февраля 2006 года хакер был приговорен к двум годам тюрьмы и €1,3 млн штрафа.

С октября 2003 года по июнь 2004 года российские программисты Иван Максаков, Александр Петров и Денис Степанов проводили DDoS-атаки на сайты британских букмекерских контор. За то, чтобы сайты были оставлены в покое, хакеры требовали по $10–20 тыс. Осенью 2004 года злоумышленников задержали, и 3 ноября 2006 года приговорили каждого к восьми годам тюрьмы и штрафу 100 тыс. рублей.

26 января 2004 года червь Novarg, созданный, по мнению экспертов, российскими хакерами, инфицировал более полумиллиона компьютеров по всему миру. Программа 1 февраля организовала DDoS-атаки на сайт IT-компании SCO и парализовала его работу на два дня. 3 февраля червем был атакован сайт Microsoft.

В августе 2006 года клиентам крупнейшего банка Швеции Nordea были разосланы письма якобы от лица администрации, в которых предлагалось инсталлировать программу, помогающую бороться со спамом. Вирус-троян, содержавшийся в программе, открыл хакерам доступ к счетам 250 клиентов, с которых похитили около $1,1 млн. По данным шведской полиции, ограбление совершила группа российских хакеров.