От автора

Все цитаты, используемые в этой книге без ссылок,
взяты из интервью, проведенных автором лично.
Я глубоко благодарен множеству людей,
которые нашли время, чтобы мне помочь.

Введение

Киберпреступность не случайно упоминается в новостях все чаще. Дело не только в том, что возрастает зависимость общества от уязвимых технологий. И не только в том, что мишенями хакеров становится все больше журналистов, политиков и влиятельных организаций. Расцвет киберпреступности связан с произошедшим слиянием влиятельных мировых хакерских групп, оставшимся, однако, почти незамеченным. В первые годы нового тысячелетия эти теневые игроки стали делиться друг с другом своими инструментами и тактиками, что привело к возникновению известной технологической угрозы и сделало киберпреступность вездесущей. Когда наше общество вышло в Сеть, они принялись наносить удары по важной для всех критической инфраструктуре: больницам, электростанциям, СМИ и структурам, обслуживающим политические процессы.

У новой волны атак три движущие силы: организованные банды киберпреступников, движения "хактивистов" и хакеры из государственных спецслужб.

Организованная преступность появилась почти одновременно с компьютерным хакингом и к настоящему моменту глубоко укоренилась, поскольку преступники поняли, насколько безопаснее грабить людей и организации виртуально, а не лично. Они берут количеством при низкой прибыльности своего дела: если украсть по пять фун-

тов у миллиона человек, жертвы, возможно, этого и не заметят, но хакеры все равно прикарманят целых пять миллионов. В результате появилась развитая отрасль, которая руководит своими доходными преступными организациями, как стартапами Кремниевой долины. Но когда выясняется, какие инструменты эти банды используют для многочисленных атак, потери оказываются далеко не только финансовыми.

Группы хактивистов изначально представляли собой цифровое протестное движение, но вскоре их тактику подхватили киберпреступники — и теперь ее активно применяют и многие другие люди, которые руководствуются более циничными и коварными мотивами. Их способность привлекать к себе внимание и переманивать журналистов на свою сторону губительно сказывается на жертвах хактивистов, компании которых теряют свою репутацию или и вовсе оказываются уничтоженными.

Наибольшие опасения, пожалуй, вызывает тот факт, что на арену киберпреступности выходит все больше государственных спецслужб, которые добавляют команды хакеров в арсенал своих военных и разведывательных структур. Это не преступные подпольные организации, а высококлассные профессиональные подразделения, получающие прекрасное финансирование. В прошлом они часто работали тайно и только с четко определенными целями. Однако вы увидите, что ситуация изменилась.

В последние десятилетия, по мере роста зависимости человечества от интернета и технологий, эти три группы постепенно расширяли свое влияние. Теперь их миры постепенно сливаются друг с другом. Организованная преступность перенимает действенные техники хакеров из государственных спецслужб. Хактивисты опускаются до атак, которые не отличить от атак организованной преступности. Спецслужбы пользуются тактикой публичного осуждения, характерной для хактивистов, а также применяют разрушительные и часто неизбирательные инструменты онлайн-аферистов.

Если ранее понятие “киберпреступность” связывалось главным образом с мошенничеством с кредитными картами и кражами из интернет-банков, то теперь, благодаря слиянию трех описанных групп, очертить его границы становится все сложнее. Как я покажу в этой книге, киберпреступность более не сводится к деньгам — в некоторых случаях взлому подвергается сама структура общества.

Читатели погрузятся в мрачный мир хакерских движений и узнают увлекательные и порой малоизвестные истории о том, как совершались их преступления и как происходили столкновения друг с другом. Повествование начинается с рассказа о хиппи-хакерах 1970-х и доходит до наших дней — и даже заглядывает в возможное будущее.

Стоит подчеркнуть, что в этом мире господствуют мужчины. В настоящий момент в преступных хакерских сообществах и даже в легальной отрасли обеспечения кибербезопасности женщины в меньшинстве. Есть основания говорить, что гендерный баланс в этой сфере меняется, но медленно.

Сложно написать о киберпреступности книгу, которая была бы одновременно обстоятельной, убедительной и сжатой. На этих страницах не упоминается ряд хакерских атак, которые кое-кто сочтет ключевыми; хронология сжимается для поддержания темпа повествования; а также — что страшнее всего — опускается множество технических подробностей, поскольку очень важно было сделать эту книгу легкой для восприятия.

Если вы технарь, не забывайте, что книга, которую держите в руках, ориентирована на широкую аудиторию. Надеюсь, вы простите ее несовершенства, понимая, что с ее помощью менее подкованные в техническом отношении читатели могут узнать о том мире, в котором вы столь хорошо разбираетесь, и проникнуться к нему уважением.

Читателям, которые не относят себя к специалистам в этой сфере, скажу: если (как я надеюсь) эта книга пробудит в вас интерес к безгранично любопытному и все более важ-

ному миру кибербезопасности, загляните в небольшой список литературы для дополнительного чтения, приведенный в самом конце.

Как вскоре станет очевидно, угроза киберпреступности сегодня настолько велика и настолько вездесуща, что наши правительства, работодатели и сами технологические компании не имеют возможности защитить нас от каждой из совершаемых атак. Если не соблюдать осторожность, пока технологии занимают все более важное место в управлении нашим миром, наше будущее окажется в руках преступных хакеров — тех, кто понимает, контролирует и использует технологии в своих целях. Мы должны защитить себя, и первый шаг к этому — обретение знаний.

Глава 1
Знакомство с хакерами

На улице тридцать градусов в тени, и я стою, обливаясь потом, у входа в огромный рынок в районе Киапо в Маниле, столице Филиппин.

В руках я держу бумажку с именем человека, которого ищу: филиппинца Онеля де Гусмана. Я слышал, что он, кажется, работал где-то среди множества палаток, которые стоят передо мной… возможно… несколько лет назад.

Я начинаю показывать бумажку людям, которых встречаю на рынке. Задача кажется невыполнимой. Я ищу микроскопическую иголку в гигантском стоге сена.

Я не знаю, как де Гусман выглядит сейчас, поскольку у меня есть лишь одна его фотография, сделанная почти двадцать лет назад. Хуже того, это размытый снимок с суматошной пресс-конференции, а де Гусман запечатлен на нем в темных очках, да еще и прикрывает лицо носовым платком.

У юного студента была веская причина прятаться. Его обвиняли в рассылке наделавшего шума и чрезвычайно успешного вируса *Love Bug*, который заразил около сорока пяти миллионов компьютеров по всему миру и нанес урон на много миллиардов долларов[1].

Этот вирус стал настоящим прорывом. И дело было не в его технической сложности и не в ущербе, который он причинил,

1 *Love Bug May Have Been Accident // www.news.bbc.co.uk,* 11.05.2000. *(Здесь и далее примеч. авт., если не указано иное.)*

но в том, что он показал, как использовать кое-что гораздо более действенное, чем код. Он был ориентирован не столько на компьютерную уязвимость, сколько на человеческую, и эта тактика впоследствии стала применяться в бесчисленном множестве киберпреступлений. Но де Гусман ни в чем не признался. Он отделался уклончивыми ответами на пресс-конференции, дал несколько невнятных интервью СМИ и ушел от ответственности. Затем он залег на дно и двадцать лет не давал о себе знать. У него не было ни страниц в социальных сетях, ни онлайн-профиля. Он стал призраком в цифровом мире, в терроризировании которого его однажды обвиняли.

У меня ушел целый год, чтобы найти хоть какую-то зацепку и предположить, где он скрывается. Ходили слухи, что он в Германии, что он работает на ООН в Австрии, что он переехал в США и что даже устроился на работу в *Microsoft*. Теперь же я шел по манильскому рынку и показывал торговцам его имя, надеясь, что кто-нибудь его узнает.

Если бы я сумел его разыскать, возможно, я смог бы расспросить его о вирусе и узнать, понимает ли сам де Гусман степень его влияния. Возможно, по прошествии двадцати лет я убедил бы его сказать мне, правда ли этот вирус был его рук делом.

Однако сколько бы я ни показывал бумажку с его именем, я лишь встречал непонимающие взгляды и слышал настороженные вопросы. Но в конце концов один из палаточников мне улыбнулся.

— Тот парень с вирусом? Да, я его знаю.

Прежде чем продолжать историю Онеля де Гусмана, важно немного изучить технологические и, что важнее, социальные тектонические плиты, которые сдвинулись за несколько лет до того, как *Love Bug* оказался у всех на устах в 2000 году.

Такие вирусы — относительно новое явление, но у них тоже есть своя история. Современный хакер формировался не один десяток лет и впитал в себя знания нескольких отдель-

ных групп. Чтобы разобраться в киберпреступности, нужно понять, как появились эти группы, а для этого — вернуться к началу начал.

В конце 1969 года, через несколько месяцев после высадки человека на Луне, американские ученые совершили открытие, которое, пожалуй, повлияло на цивилизацию сильнее, чем лунный рывок, предпринятый NASA.

Министерство обороны США искало надежный способ передавать сообщения в своей распределенной компьютерной сети. Специалисты придумали разбивать сообщения на одинаковые по размеру фрагменты и посылать их с одного компьютера на другой по серии транзитных участков, задействуя для этого телефонную систему. Идея связать компьютеры друг с другом с помощью телефонных линий была не нова: вопрос всегда состоял в том, как создать достаточно масштабную систему, которую можно будет легко расширить, включив в нее новых участников. Разработанный для этого метод позволял любому компьютеру, зарегистрированному в общей системе, присоединяться к группе, а следовательно, отправлять и получать фрагменты данных. Таким образом была проложена дорога к беспрепятственному и быстрому развитию системы, которая стала применяться не только в военной сфере. В результате появилась взаимосвязанная сеть компьютеров, или интернет, и система для передачи сообщений от одного компьютера к другому, называемая интернет-протоколом (IP). Каждая машина, зарегистрированная в системе, получала уникальный адрес (IP-адрес), и, чтобы передать данные с одного компьютера на другой, нужно было просто прикрепить правильный адрес, тем самым показав всем остальным компьютерам в сети, куда их следует направить[1].

1 Leiner B. M., Cerf V. G., Clark D. D.,. Kahn R. E., Kleinrock L., Lynch D. C., Postel J., Larry G. Roberts, Wolff S. *Brief History of the Internet* // Internet Society. 1997. P. 2–4.

Интернет часто отождествляют со Всемирной паутиной, или вебом. На самом деле последняя появилась существенно позже, в 1989 году. До этого документ, которым делились в интернете, мог выглядеть по-разному на разных компьютерах. Всемирная паутина, по сути, дала способ публиковать данные в интернете и стандартизировать внешний вид материалов, доступных для разных машин[1].

В сочетании с интернетом всемирная паутина привела обе технологии к глобальному доминированию с начала 1990-х годов. Но почти за двадцать лет до этого интернет прекрасно существовал и без веба. Именно в тот период появились первые компьютерные хакеры, и их развитие и становление подпитывала система, которая фактически представляла собой винтажную версию фейсбука[2].

Как вы узнаете из этой книги, представление о том, что хакеры — сплошь необщительные одиночки, как правило, ошибочно. Порой их поведение действительно асоциально, но в большинстве своем они, как и другие люди, стремятся найти единомышленников. Многие первые пользователи компьютеров обрели приятелей через электронные доски объявлений (*bulletin board system*, BBS) — почти забытую ныне технологию, около двадцати лет существовавшую параллельно с интернетом. Эти доски были предельно простыми общедоступными службами обмена сообщениями, где пользователи проводили время и общались друг с другом. Они читали посты и отвечали на них — и иногда этот процесс растягивался на несколько дней. Как отметил один пользователь BBS, “это было похоже на разговор, только очень, очень медленный”[3].

Непосвященным, которые наблюдали за происходящим со стороны, это часто казалось не технологической

1 *History of the Web* // *www.webfoundation.org.*
2 Деятельность компании MetaInc (Facebook, Instagram) запрещена на территории РФ решением суда.
3 Scott J. *The BBS Documentary* //Режим доступа: bbsdocumentary.com.

революцией, а бессмысленной тратой времени. Но из бесед с первыми пользователями BBS становится очевидно, что именно их привлекало в досках объявлений. В тот период мало кто разбирался в компьютерах, и любовь к технологиям превращала их в аутсайдеров. И вдруг появилась непонятная система, которая связывала людей с общими интересами.

В культурном отношении электронные доски объявлений сыграли ключевую роль в технологической эволюции. На заре своего существования интернет в основном контролировался исследователями, сидящими в хорошо финансируемых лабораториях. Но дух этого нового мира, его обычаи и нравы все больше прорабатывались на BBS. В итоге именно там и нашли друг друга первые хакеры. Несколько сил слились воедино на просторах свободных чатов BBS в зарождающемся киберпространстве, и так возникла хакерская культура. Первая из этих сил зародилась благодаря группе психоделических скитальцев, бегущих от коллапса движения хиппи.

На исходе эпохи “силы цветов”, когда рассвет Вудстока сменился мрачными сумерками бунтов на Альтамонтском фестивале, в США появился журнал *Whole Earth Catalog*. Он продвигал идеи самодостаточности и жизни вне привычных рамок.

Вполне естественно, что следующим шагом стало создание его компьютеризированной версии. Его необходимо было постоянно обновлять, а электронный формат упрощал эту задачу. Кроме того, некоторые из людей, занимавшихся развитием журнала, в 1970-х годах принимали участие в американских экспериментах по строительству коммунальной жизни и хотели создать такую же атмосферу на цифровых форумах каталога. Его онлайн-версия под названием *Whole Earth ‘Lectronic Link* (WELL) была запущена в 1985 году и бы-