ГАЗЕТА ПАРЛАМЕНТСКОГО СОБРАНИЯ СОЮЗА БЕЛАРУСИ И РОССИИ
СОЮЗНОЕ ВЕЧЕ
7 - 13 сентября / 2017 / № 40

Иван НИКОЛАЕВ

НЕО ВЫШЕЛ ИЗ «МАТРИЦЫ»... ПРИХВАТИВ ДЕНЬГИ

Самый желанный куш для IT-криминала - расчетные счета и электронные кошельки. Чего следует опасаться?

БАНКОМАТ, ПОЗОЛОТИ РУЧКУ

Глава Сбербанка Герман Греф считает, что уже через несколько лет хакеры будут способны нанести ущерб мировой банковской системе, исчисляемый одним триллионом долларов. Это без учета атак на прочие организации. Поэтому решил как следует вложиться в безопасность. Со Сбербанком все ясно, это богатейшая компания, которая может позволить себе лучшие IT-разработки. А как же быть остальным?

- Сейчас главная мишень киберпреступников - небольшие региональные банки, - рассказал **эксперт сетевой безопасности Никита Кислицин.** - Атаки стали изощреннее и зачастую происходят с использованием методов социальной инженерии. Например, сотрудники одного из финансовых учреждений получили на рабочую почту рассылку о вакансиях в Центробанке. Многие не удержались и открыли письмо с трояном.

Атакуют не только счета клиентов. Через зараженные компьютеры внутренней сети банков «черви» забираются в банкоматы и тихо сидят там. А дальше начинается грабеж средь бела дня. Злоумышленник подходит к банкомату, вводит особый код и забирает самые крупные купюры.

ИГРА НА КАРТЫ

Если раньше кибер-преступниками становились настоящие гении и гуру программирования, то теперь достаточно знать банальные приемы «промывания мозгов».

Соцсеть «Вконтакте», которая популярна как в России, так и в Беларуси, стала настоящим полем чудес для мошенников. В Следственном комитете РБ сообщили, что в 2017 году участились случаи обмана добропорядочных белорусов. Злоумышленники взламывали чужие аккаунты, пользуясь тем, что пароли были очень простыми. Затем начинали от чужого имени рассылать сообщения всем «друзьям», мол, «пришли реквизиты или фото банковской карты, а я тебе деньги перечислю». На карте, кто не знает, находится исчерпывающая информация, чтобы списать с нее средства. Вот и оставались граждане с носом, как Буратино.

А один продавец в минском торговом центре поступал еще проще. Тихонько фотографировал карты покупателей с двух сторон на свой телефон. И потом обчищал их. Схема самая примитивная, но следователям пришлось поломать голову, прежде чем на него вышли.

Подобных случаев не счесть и в России. Например, в феврале стало известно, что жительница Пермского края придумала схему хищения с помощью услуги «Мобильный банк». Через соцсети она покупала у людей старые сим-карты и использовала их как ключи от онлайн-сейфов, получая СМС с паролями. Полсотни человек лишились в сумме десяти миллионов рублей.

Катерина МАРТИНОВИЧ/kpmedia.ru

ПРОГНОЗЫ

ВОССТАНИЕ АРМИИ УТЮГОВ

Футурологи уверены: если мы не защитим от хакеров технические новинки, то не видать нам светлого будущего.

- Через четыре года в мире будет насчитываться больше двадцати миллиардов устройств интернета вещей. Большинство из них будет с минимальной киберзащитой. «Умными» и одновременно уязвимыми станут холодильники, стиральные машины, системы включения света и воды, разные датчики, подключенные к интернету.
- Уже сейчас хакеры могут взломать некоторые модели радионянь и кукол и напугать ребенка. И это еще цветочки. В конце августа в США было отозвано полмиллиона кардиостимуляторов, уязвимых для кибератак!
- Вскоре на дорогах появится множество автомобилей с функциями беспилотника. Спецслужбы уверены, что они могут быть взломаны по Сети и использованы для убийств и терактов.
- Фантаст **Айзек Азимов** придумал законы, согласно которым роботы не смогут навредить человеку. Может, и так. А если ими будут управлять злоумышленники?
- Наши ученые вместе с зарубежными коллегами работают сейчас над квантовой криптографией. Есть надежда, что она станет щитом от грядущих криминальных посягательств.

«Пока не поймали, ты - король»

ИСПОВЕДЬ ХАКЕРА

Сергей ПАВЛОВИЧ, известный белорусский кибермошенник, отсидевший в тюрьме десять лет, автор книги «Как я украл миллион, исповедь раскаявшегося кардера»:

youtube.com

- Больше всего киберпреступников в СНГ - преимущественно от безденежья. Мозгов у людей хватает, а реализовать себя в бизнесе по ряду причин не могут, вот и идут в криминал. Я никогда не смог бы украсть кошелек в общественном транспорте. Когда ты крадешь в интернете, ты не чувствуешь той грани, после которой начинается преступление, совесть тебя не мучает. Мне не казалось, что я занимаюсь чем-то сильно криминальным.

При этом я не назвал бы это легкими деньгами. Пока тебя не поймали, ты - король, ты получил десять, сто тысяч долларов. Однако глаза открываются, как только попадаешь за решетку. И если разделить количество украденных денег на количество месяцев заключения, понимаешь, что за это время ты мог бы легко заработать больше денег абсолютно легально. Понятное дело, не на заводе, но в IT-сфере, например.

На меня очень сильно повлиял **Стив Джобс,** который хотел «поднять мир на новую высоту» - в тюрьме я несколько раз перечитал его биографию. И теперь понимаю, что есть действия, ведущие только к регрессу, - это те же киберпреступления, которые несут выгоду только тебе, а другим людям приносят страдания. Поэтому к тому, чем я раньше занимался, сейчас отношусь крайне негативно.

КАК НЕ СТАТЬ ДОБЫЧЕЙ МОШЕННИКОВ

ВЫРЕЖИ И СОХРАНИ

Эксперты уверены: большинство проблем возникает от незнания элементарных правил безопасности.

- Делайте сложные пароли, меняйте их периодически, не используйте один пароль для разных сайтов. Если не можете запомнить все ключи, используйте менеджеры паролей (LastPass, 1Password и др.).
- **Везде, где только можно, сделайте привязку авторизации и смены пароля через номер мобильного.**
- Не оставляйте телефон без присмотра. Не раздавайте старые SIM-карты.
- **На просьбы друзей в соцсетях предоставить реквизиты платежных карточек свяжитесь с ними по телефону.**
- В соцсетях не показывайте всем свое местоположение и номера сотовых.
- **Не переходите по ссылкам в спам-сообщениях и не скачивайте сомнительные файлы. Если скачали - проверьте антивирусом. Опасные материалы могут прийти и со взломанных аккаунтов друзей.**
- Ставьте все обновления операционной системы, программ и антивируса. Не лишним будет установить межсетевой экран (firewall).
- **PIN-коды карт не записывайте в мобильнике или на компьютере, а тем более на самой карте. Не пересылайте фото банковских карт. В магазинах и кафе все действия с картой должны происходить в вашем присутствии. Лучше стереть CVC-код - последние три цифры на оборотной стороне карты.**
- К основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Используйте виртуальные карты или сервис PayPal. Поставьте лимит на сумму ежедневных списаний.
- **Не называйте пароли и PIN-коды даже сотрудникам банка. Не логиньтесь в онлайн-банках, сидя в бесплатном Wi-Fi.**
- Смотрите внимательно адресную строку - можете попасть на сайт-дублер. Не доверяйте укороченным ссылкам. Проверяйте наличие безопасного соединения (значок замочка в браузерах, https в начале строки).
- **Если от лица официальных структур у вас запрашивают данные по e-mail, позвоните туда.**
- Храните важную информацию на внешних носителях.
- **Многие пользователи компьютеров Apple уверены, что вирусы им не страшны. Это заблуждение.**
- Откажитесь от нелегального ПО. Сайты с пиратским контентом и порно - рассадники вирусов.