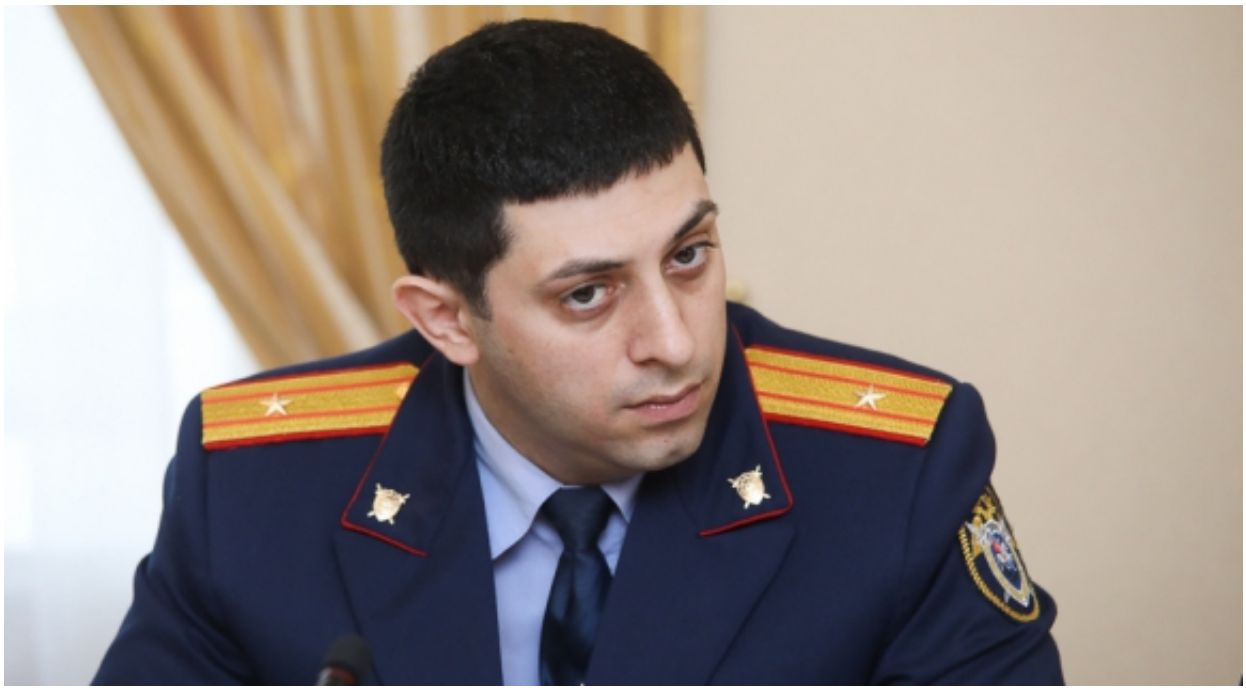
Высокие технологии (''Молодой ленинец'' от 29 сентября 2020 года)



В августе в Даркнете оказалось около 1,1 млн номеров и серий паспортов избирателей. Как сообщает издание «Коммерсантъ», это данные участников электронного голосования. Продавцы подтвердили журналистам, что база «полностью свежая» и спрос на нее велик — продано уже 30 тысяч строк ($1 оптом и $1,5 в розницу).

Другая важная новость пришла из Министерства цифрового развития, связи и массовых коммуникаций России — там создали межведомственную рабочую группу по рассмотрению вопросов противодействия телефонному мошенничеству. Эта мера вынужденная — на технически подкованных аферистов нужно срочно сообща искать управу.

Под маской старика

Например, банковские мошенники уже научились с помощью технологий подделывать любые голоса. Недавно на сессии инвестиционного форума в Сочи зампред одного из ключевых российских банков включил аудиозапись, где условный губернатор голосом Иннокентия

Смоктуновского попросил у собеседника 5 млрд рублей на строительство моста в регионе...

В Пензе тоже есть свои технические гении, которые направляют свою энергию в уголовное русло. Так, недавно был вынесен приговор по делу о краже из банкоматов... 20 с лишним миллионов рублей! Виновным признали жителя Саратовской области — раньше он занимался техническим обслуживанием платежных терминалов и отлично знал, как и что в них устроено.

Злоумышленник все продумал до мелочей: сшил сумку для денег под размер кассет банкомата, запасся формой сотрудника инкассаторской службы и... реалистичной латексной маской, имитирующей внешность пожилого мужчины!

Более того, конспиратор повесил на свой личный автомобиль поддельные номера — точь-в-точь как на машине аналогичной модели и цвета, принадлежавшей жителю Тамбова (то ни сном ни духом не знал о пензенском злоумышленнике).

Преступник приехал в Пензу за месяц до кражи и присмотрел себе два банкомата — в торговых центрах Арбекова и района Север. Дальше все было делом техники: облачиться в свой «каранвальный» костюм, открыть терминалы ключом и забрать оттуда деньги. Их мужчина хранил в тайнике на техническом этаже своего дома. Теперь саратовец приговорен к 4 годам колонии общего режима, а его автомобиль изъят в доход государства.

Чужие среди своих

Любопытное дело сейчас находится в следственном отделе по Октябрьскому району Пензы. Заведено оно на 42-летнего мужчину, который раньше работал в компании-операторе сотовой связи. Но когда сотрудник увольнялся, он «прихватил» с собой логином и пароль своего коллеги, а тот, конечно, был не в курсе.

«Позднее, уже из дома, мужчина с помощью этих данных вошел в информационную базу, где хранились сведения о телефонных соединениях абонента из другого региона, - рассказывает **заместитель руководителя отдела процессуального контроля следственного управления СКР по Пензенской области Олег Ключников, -** Эти данные злоумышленник продал третьему лицу. Теперь экс-сотруднику предстоит отвечать перед законом по ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров».
Свою преступную схему изобрел и 46-летний житель Бессоновки. Он долгое время работал в организации-провайдере цифровых услуг. Незадолго до увольнения мужчина установил в приемной начальника два микрофона, а затем, вплоть до весны этого года, вел прослушку и слежку. Кроме того, бывший сотрудник удаленно подключался к компьютеру одного из экс-коллег и копировал оттуда служебную информацию. О незаконной деятельности узнали сотрудники УФСБ России по Пензенской области.

В отношении мужчины возбуждено дело по той же 138 статье УК РФ. Кстати, на допросе

фигурант признался, что на преступление пошел из любопытства - ему хотелось быть в курсе происходившего на прежнем месте работы. Дело закончилось штрафом в 15 тысяч рублей. Решение пока не вступило в законную силу.

В Октябрьском районе по этой же статье под суд пошли сразу три подельника, но тут в деле уже был замешан меркантильный интерес. «В январе 2020 года один частный детектив попросил знакомого помочь ему — за вознаграждение установить на телефон программу, которая бы давала к нему удаленный доступ, - рассказывает Олег Ключников. - Тот посоветовал одну техническую компанию. Обещанный гонорар устроил ее генерального директора, и тот поручил это задание программисту. Однако лицензию на производство специальных технических средств, предназначенных для негласного получения информации, фирма, конечно, не имела».

Тем не менее подельники взяли за свои труды 60 тысяч рублей. Но эти деяния не скрылись от бдительного взгляда сотрудников УФСБ... Тут и выяснилось, что месяцем ранее к этим же директору и программисту с такой же просьбой обращалась женщина — ей за 15 тысяч рублей эти же люди установили в микроволновку «жучок» - чтобы та могла прослушивать разговоры членов ее семьи, и особенно снохи.

Свою вину злоумышленники признали и получили штрафы — в общей сложности 160 тысяч рублей.

Жучок для благоверной

На подобные злодеяния идут и простые обыватели — кто-то из-за подозрений, кто-то из мести. В любом случае ничего хорошего из этого не выходит.

Так, 41-летнюю пензячку обвинили в незаконном приобретении специальных техсредств для негласного получения информации. Пять лет назад женщина купила через Интернет программу, позволяющую незаметно для человека контролировать его телефонные переговоры, переписку, определять местонахождение смартфона. Эту программу дама установила на телефон супруга, и пять лет он был у нее как на ладони!

А 42-летний пензяк с помощью подобной программы три года следил за звонками и перепиской жены. Сейчас уголовное дело уже в суде, мужчине грозит лишение свободы до четырех лет.

Некоторые люди при этом чуют за собой слежку (например, по подозрительному эху, сопровождающему телефонные звонки) и обращаются к правозащитникам. Так, юрист Виктория Зарецкая сейчас работает с клиенткой, которая пожаловалась, что муж ежедневно следит за ней с квадрокоптера! «С утра пораньше он поджидает меня у подъезда, и пока я веду ребенка в садик, над нами летает дрон и записывает каждый наш шаг», - пожаловалась женщина. Она уже обратилась в полицию: интересно, сочтут ли правоохранители коптер специальным техническим средством или нет?

«Впрочем, муж, скорее всего, будет уверят, что он для собственного удовольствия в семь утра пять дней подряд забавлялся с этой «игрушкой», - не исключает юрист. - Будем бороться!»

Виктория Зарецкая напоминает, что уголовная ответственность за приобретение и продажу без лицензии любых предметов (брелоков, ручек, часов), в которых есть скрытая видеокамера или диктофон, была введена еще в 2009 году. Спустя два года оборот специальных техсредств был выделен в отдельную статью уже средней степени тяжести - максимальное наказание увеличили до 4 лет лишения свободы.

Однако до сих пор официального перечня устройств, запрещённых к обороту, не существует, и люди не видят в таких гаджетах ничего предосудительного. Но теоретически под «шпионские» гаджеты могут попасть даже детские «умные часы» с функцией одностороннего звонка — особенно если взрослые начнут их использовать друг против друга.

«Если вы покупаете даже ту же модель какого-то устройства, которая продаётся в соседнем магазине, это не гарантирует отсутствия претензий к вам: все посылки проходят проверку на таможне с помощью рентгена! Так что при дистанционной покупке рекомендую оставлять комментарии к заказам о том, что вы приобретаете эту вещь в личных целях для обеспечения своей безопасности», - подытоживает юрист.

Кибердетектив из Пензы

Наш разговор о цифровых «шпионских» штучках был бы неполным без участия нашего земляка Павла Седакова, который сейчас в Москве работает... кибердетективом!

«Я тружусь в компании, которая занимается предотвращением кибератак и киберкриминалистикой, - поясняет Павел. - Мы расследуем миллионные кражи из банков, кибердиверсии, DDoS-атаки, ищем хакеров по всему миру: собираем цифровые доказательства и строим цепочку связей, которые помогут отправить преступников за решетку. За 15 лет компания провела 1500 расследований в 30 странах мира, и 120 из них завершились тюремными сроками.

Среди самых крупных фигурантов — группировка Cron, которая похищала деньги с банковских счетов пользователей смартфонов с ОС Android. Они ежедневно заражали 3 500 (!) телефонов и меньше чем за год установили вредоносное ПО на 1 млн устройств. Два

десятка киберпреступников одновременно задержали в 6 регионах России.

Еще была Carberp — самая большая в России организованная преступная группа, похитившая $250 млн. со счетов клиентов российских банков. Организаторы осуждены на сроки от 5 до 7 лет.

Были международные расследования, например, группа Cobalt, которая, по оценкам Европола, похитила около 1 млрд евро у 100 банков в 40 странах.

В нашем штате есть инженеры, разрабатывающие технологии, аналитики, изучающие вредоносные программы, компьютерные криминалисты, ищущие цифровые следы на месте преступления, кибердетективы, специалисты по борьбе с интернет-пиратством, аналитик киберугроз, специалист по развитию искусственного интеллекта в кибербезопасности, специалист по защите криптобирж.

В целом, я считаю, что время хакеров-романтиков, взламывающих сети Пентагона, чтобы найти секретные материалы об НЛО, давно ушло. Большинство преступников воруют огромные деньги или ценные данные. В России в результате кибератак ежемесячно теряют деньги 1-2 банка, ущерб от одного хищения составляет в среднем $2 млн.

В то же время, за которое происходит одно ограбление квартиры, фиксируется 3000 различных компьютерных атак! Не пройдет и пяти лет, как эта угроза займет первую строчку бизнес-рисков».

Ксения ИВАНОВСКАЯ

29 Сентября 2020

Адрес страницы: https://penza.sledcom.ru/folder/879102/item/1521749