– поддерживать международное сотрудничество для преследования таких преступлений, совершаемых за пределами нашей страны;

– предотвратить случаи насилия, преследований и неправомерного использования личных данных;

– проводить постоянное обучение сотрудников Национальной полиции по противодействию киберпреступности;

– продолжать укреплять и предоставлять цифровые ресурсы отделу по борьбе с киберпреступностью Управления судебного расследования и отделу компьютерной криминалистики Института Криминалистики для достижения лучших результатов в поиске цифровых доказательств;

– сообщать о любых киберпреступлениях в Национальную полицию для проведения надлежащего расследования.

Мильтон Хавьер Портильо,
Оскар Данило Ривас Мартинес,
Херонимо Хосе Лопес,
Эрика Родригес Родригес,
Александер Освальдо Флорес Дельгадильо
Научное руководство при подготовке тезисов:
Д.С. Звягин, кандидат технических наук,
Н.И. Болычев
(Воронежский институт МВД России)

Противодействие незаконному доступу к компьютерной информации

Киберпреступность началась с попыток хакеров взломать компьютерные сети. Некоторые делали это просто ради острых ощущений от доступа к высокозащищенным сетям, но другие стремились получить конфиденциальные и секретные материалы. Со временем преступники начали заражать компьютерные системы вирусами, что приводило к сбоям в работе персональных и офисных компьютеров.

В настоящее время, по статистическим данным, более 60% населения пользуются информационно-коммуникационными технологиями. Это использовалось как средство совершения преступлений без контакта и на расстоянии. Это одна из основных проблем, с которой мы сталкиваемся как полицейское учреждение в условиях растущего уровня преступности, которая затрагивает имущество, неприкосновенность и другие законные активы, защищаемые нашим Уголовным кодексом Никарагуа, основанным на нашей конституционной политике.

В мире, который все больше зависит от технологий, вмешательство в работу компьютерных систем стало угрозой цифровой безопасности, что привело к развитию видеонаблюдения и совершенствованию методов взлома. Понимание этого явления необходимо для разработки эффективных стратегий защиты.

В мире, который все больше зависит от технологий, вмешательство в работу компьютерных систем стало серьезной угрозой цифровой безопасности. Это явление привело к значительному увеличению частоты видеонаблюдения и усложнению методов проникновения, что обусловило необходимость понимания этих механизмов для разработки эффективных стратегий защиты.

По инициативе Президента Республики Национальное собрание единогласно утвердило 11 сентября инициативу по реформам и дополнениям к закону № 1042, Специальный закон о киберпреступности, который укрепляет предотвращение, конфронтацию, расследование и судоохранение преступлений, которые физические или юридические лица комментируют внутри или за пределами страны, с помощью компьютерных систем, новых технологий и социальных сетей, и которые влияют на спокойствие и социальный мир людей, семей и общества.

13 апреля 2023 года в 09:00 часов было принято заявление от гражданки Аны Хулии Перес Мартин, генерального директора телекоммуникационной компании Claro, которая сообщила, что примерно в течение последних полутора лет фиксируются аномалии в технических показателях коммуникационных систем компании, особенно в части неоправданного и нерегулярного потребления интернет-данных и минут телефонной связи. В связи с указанными обстоятельствами заявительница обратилась в компетентные органы с целью официального оформления жалобы и инициирования соответствующего технического и судебного расследования по данному случаю.

После получения заявления была немедленно сформирована специальная следственно-оперативная группа полиции, в состав которой вошли:

– руководитель подразделения по расследованию киберпреступлений (ETI);

– специалист по технологическим преступлениям;

– сотрудник, ответственный за проведение осмотров места происшествия;

– оперативный водитель.

Прибыв в офис компании Claro, руководитель подразделения по расследованию киберпреступлений запросил у генерального директора Аны Хулии Перес Мартин техническую справку с перечнем и контролем IP-адресов серверов связи (Reuters), показатели которых содержали существенные отклонения. В общей сложности были выявлены 58 серверов, среди которых один сервер с идентификационным кодом HTTP242425262982 имел аномальные показатели потребления интернет-данных и телефонных минут.

Указанный сервер был закреплен за техническим отделом, ответственность за его обслуживание и мониторинг несла гражданка Мария де Лурдес Мантика, которая являлась единственным лицом с привилегированным доступом к этому серверу. В результате указанных обстоятельств Мантика была незамедлительно задержана и допрошена в качестве подозреваемой.

Подозреваемая Мария де Лурдес Мантика прямо признала свою ответственность за незаконное перенаправление интернет-данных и телефонных минут примерно на протяжении последних полутора лет, осуществлявшееся с использованием сервера с кодом HTTP242425262982, принадлежащего

Claro. Она пояснила, что перенаправление производилось через иностранную SIM-карту, зашифрованную с помощью специализированного программного обеспечения, название и технические характеристики которого ей неизвестны. Также она сообщила, что данная SIM-карта была предоставлена ей третьим лицом по имени Хуан Франсиско Эчаваррия, с которым она познакомилась во время поездки в Коста-Рику.

Кроме того, Мантика пояснила, что по ее домашнему адресу были установлены и использовались несколько маршрутизаторов, подключенных к вышеуказанной зашифрованной SIM-карте, посредством которых осуществлялась незаконная передача пакетов интернет-данных и телефонных минут, принадлежащих Claro.

На основании сведений, полученных в ходе допроса подозреваемой, специализированная группа произвела технический осмотр помещений службы технической поддержки Claro в присутствии Марии де Лурдес Мантики, которая указала сервер HTTP242425262982 как устройство, в котором была установлена вышеуказанная иностранная зашифрованная SIM-карта, подтвердив, что именно она осуществляла его обслуживание.

Затем, учитывая уже имеющиеся доказательства, следственная группа направилась по домашнему адресу подозреваемой, где был произведен санкционированный судебный обыск, в результате которого были изъяты шесть (6) маршрутизаторов, принадлежащих Claro.

В ходе обыска с поличным был задержан гражданин Пабло Данило Мехия, супруг подозреваемой, который в ходе допроса признал, что именно он являлся оператором изъятых устройств, указав, что они были предоставлены ему супругой. Кроме того, он признался, что отвечал за создание кодов для третьего соучастника, Хуана Франсиско Варгаса, задачей которого являлось привлечение клиентов, заинтересованных в получении интернет-услуг и телефонных минут по ценам, ниже стандартных тарифов Claro. Также Пабло Данило Мехия занимался сбором доходов от данной противоправной деятельности через банковский счет на его имя в финансовом учреждении LAFISE-BANCENTRO.

В завершение расследования в сотрудничестве с подразделением по розыску и задержанию был задержан Хуан Франсиско Варгас, подтвердивший свое соучастие с Марией де Лурдес Мантикой и Пабло Данило Мехией в схеме незаконного перенаправления услуг Claro. Он пояснил, что его основной задачей было привлечение клиентов; на момент задержания у него насчитывалось 32 пользователя, с каждого из которых ежемесячно взималось примерно 10 долларов США, что обеспечивало незаконный ежемесячный доход около 320 долларов США, распределявшийся между тремя соучастниками согласно предварительным договоренностям.

Национальная полиция Никарагуа провела следственные действия по делу о киберпреступности правильно и в соответствии с законом (документальные, свидетельские и технические, экспертные и научные доказательства). Вышеупомянутые лица были привлечены к ответственности за хранение оборудования или предоставление услуг, нарушающих компьютерную безопасность, предусмотренное в статье 11 Специального закона о киберпреступности №1042, и приговорены к 3 годам лишения свободы.

Всем сотрудникам полиции Никарагуа рекомендуется пройти обучение по предотвращению киберпреступности, чтобы актуализировать свои знания об операционных системах и приложениях о защите электронных устройств и оборудования, что позволит им противодействовать этим постоянно меняющимся формам преступлений.

Хулио Александер Парралес Парралес,
Вернер Берни Данли Эскобар,
Луис Аломар Окампо Карденас,
Мельба Алехандра Донаире Роке,
Джеферсон Исраэль Урбина Ортега
Научное руководство при подготовке тезисов:
Д.С. Звягин, кандидат технических наук,
Н.И. Болычев
(Воронежский институт МВД России)

Раскрытие дистанционного мошенничества, связанного с использованием мобильных приложений

За последние годы в Никарагуа было зафиксировано значительное увеличение числа заявлений, связанных с компьютерными преступлениями, особенно с мошенничеством, совершаемым через манипуляции с мобильными приложениями и банковскими платформами. Киберпреступники используют такие стратегии, как подмена личности, отправка фальшивых ссылок, сбор личных данных и использование одноразовых паролей (OTP) для осуществления несанкционированных переводов. Для противодействия этой ситуации государство Никарагуа внедрило правовые инструменты, такие как Закон № 1042, который определяет компьютерные преступления и устанавливает соответствующие наказания.

10 октября 2024 года в 09:10 потерпевший с инициалами B.A.I. получил сообщение через WhatsApp с номера <…>. Отправитель представился как «Карлос Фунес», начальник службы безопасности банка Banpro, сообщил, что карта потерпевшего (в долларах США) была клонирована колумбийскими преступниками, которые специализируются именно на клонировании