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.

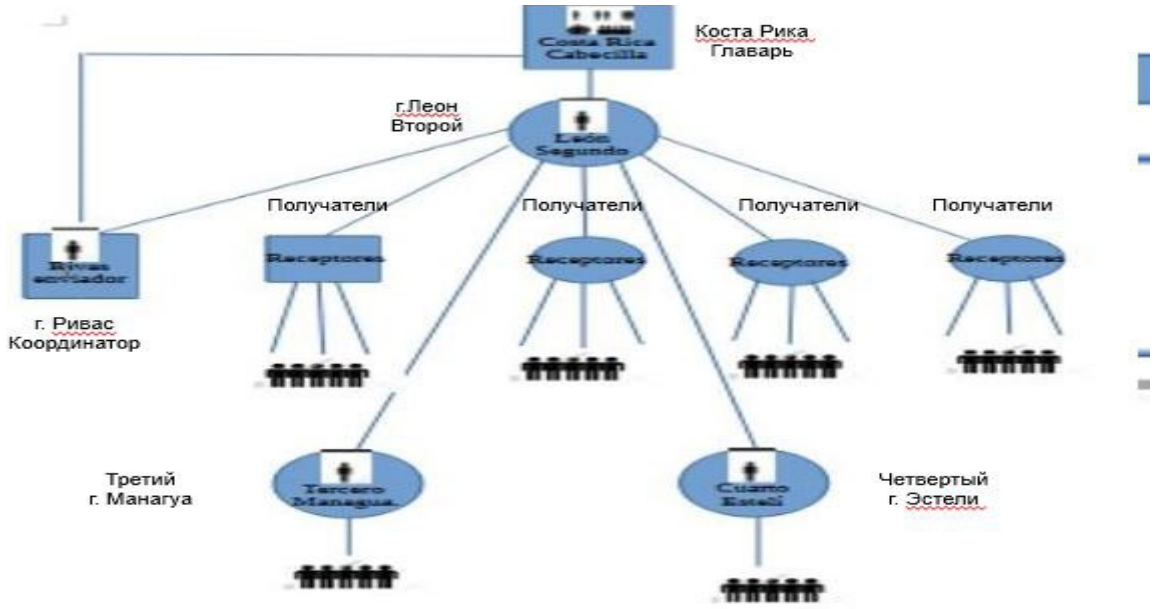
10 октября 2024 года в 09:10 потерпевший с инициалами B.A.I. получил сообщение через WhatsApp с номера <…>. Отправитель представился как «Карлос Фунес», начальник службы безопасности банка Banpro, сообщил, что карта потерпевшего (в долларах США) была клонирована колумбийскими преступниками, которые специализируются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

карт, а также что преступники отправляют его денежные средства на другие банковские счета.

Чтобы «остановить» транзакции, он попросил потерпевшего перейти по ссылке, которую ему отправят. Потерпевший нажал на ссылку, которая перенаправила его на фальшивую платформу с логотипом банка. Там он заполнил свои личные данные согласно всем требованиям приложения. После завершения заполнения своих личных данных, он получил на свой мобильный телефон одноразовые пароли (OTP), которые передал «Карлосу Фунесу».

Затем жертве было указано не заходить в свой интернет-банкинг, поскольку процесс приостановки трансакций уже был запущен банком и нужно было подождать 12 часов. И через несколько минут он стал получать из банка на свой телефон одноразовые пароли (OTP). Он предположил, что эти пароли нужны для приостановки транзакций с его карты, поэтому согласился пересылать их на телефон преступника.

Оказалось, что эти пароли были направлены для изменения доступа к его банковским счетам.



Благодаря проведенному расследованию удалось выяснить обстоятельства дела и нейтрализовать преступную группировку, действующую на территории Никарагуа, что позволило Генеральной прокуратуре предъявить обвинение каждому из обвиняемых и добиться для них соответствующего наказания. В ходе проведенного расследования удалось получить обратно 10 000 долларов США, которые были изъяты преступниками у владельцев банковских счетов и передать имущество потерпевшему, у которого украли деньги, о чем был составлен соответствующий акт.

Анализируемый случай показывает, как преступники пользуются доверием людей и их незнанием основ кибербезопасности для совершения крайне

вредоносных мошенничеств. Институциям необходимо удвоить усилия по предотвращению подобных преступлений, усиливая цифровое образование и укрепляя механизмы реагирования и расследования.

В целом по результатам проведенной работы, можно представить следующие рекомендации:

– обучать население основам хорошей практики в области кибербезопасности;

– всегда проверять подлинность любых банковских сообщений;

– не передавать коды, пароли или конфиденциальную информацию через мессенджеры;

– продвигать информационные кампании от банковских учреждений;

– усиливать сотрудничество между банками, полицией и судебными органами в отслеживании подозрительных транзакций;

– использовать безопасные цифровые платформы с двухфакторной аутентификацией.

Йоанна Патрисиа Вальехос Гомес,
Хенссель Антонио Портокарреро Абурто,
Юдит Ванеса Калеро Гайтан,
Элисабет де лос Анхелес Эррера,
Мариа Макенси Мендоса Бустос
Научное руководство при подготовке тезисов:
Д.С. Звягин, кандидат технических наук,
Н.И. Болычев
(Воронежский институт МВД России)

Особенности расследования мошенничества, связанного с использованием социальных сетей

Современный мир переживает важное экономическое явление, которое ознаменовывает новую эпоху – глобализацию. Она представляет собственные уникальные аспекты, которые отличают ее от других периодов в истории человечества, а именно: использование информационно-коммуникационных технологий (ИКТ), которые представляют собой «технологии, использующие информатику, микроэлектронику и телекоммуникации для создания новых форм связи с помощью технологических и коммуникационных инструментов в целях облегчения передачи, доступа и обработки информации».

Эту эпоху также называют «Цифровой или Информационной эрой», которая повлияла как на экономическую, социальную, культурную сферы частной жизни людей и корпораций, так и на само развитие страны.