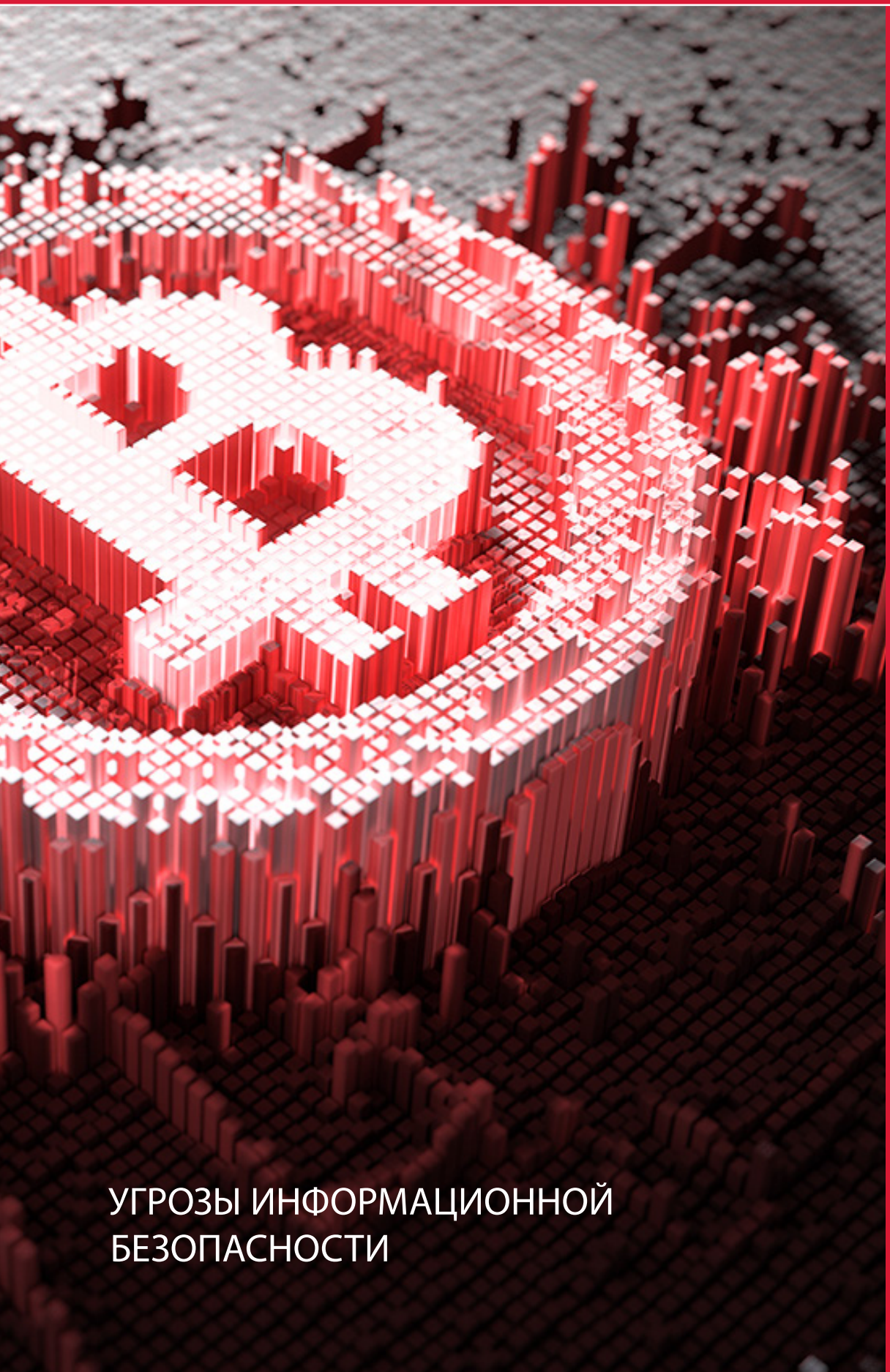
POSITIVE TECHNOLOGIES

INITIAL COIN OFFERING



УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

По разным оценкам, объем инвестиций, привлеченных с помощью Initial Coin Offering (ICO) в 2017 году, превысил 5 млрд долл. США. Среди самых прибыльных проектов EOS, который принес компании 883,4 млн долл. США, Filecoin — 257 млн долл. США, Tezos — 232 млн долл. США. Но кроме капитала ICO-стартапы привлекли также и внимание злоумышленников. При проведении ICO в 2017 году киберпреступники похитили около 300 млн долл. США, что составило порядка 7% всех заработанных на ICO средств за этот год. Чтобы во время проведения ICO избежать финансовых потерь, необходима тщательная подготовка, особенно с точки зрения кибербезопасности.

Специалисты Positive Technologies в 2017 году реализовали множество проектов по анализу безопасности и защите от киберпреступников как процедуры ICO, так и внедрения блокчейн-технологий в банках в России и за рубежом. Проекты охватывали анализ безопасности инфраструктуры, веб-ресурсов, защиты от атак на организаторов и социальной инженерии в адрес инвесторов, поиск уязвимостей в смарт-контрактах и в методах аутентификации. Мы проанализировали результаты проведенных проектов и выяснили, где у ICO самые проблемные места.

РЕЗЮМЕ

В каждом проекте ICO
в среднем содержалось
5 уязвимостей.

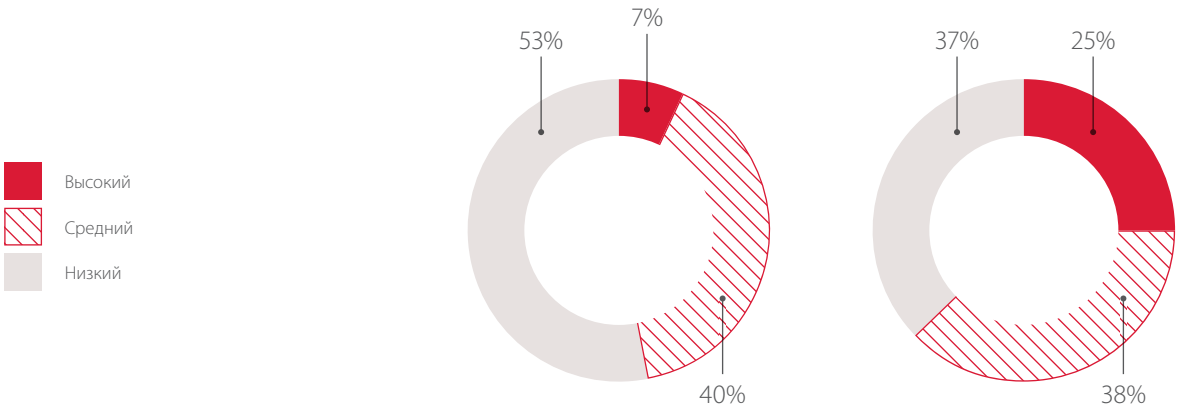
Злоумышленникам достаточно всего одной, чтобы присвоить деньги инвесторов

Всего один из проанализированных проектов не содержал существенных недостатков. И общедоступный отчет экспертов Positive Technologies стал для 15 000 участников гарантией безопасности при принятии решения, стоит ли вкладывать в этот проект деньги. Компания успешно завершила процесс ICO, собрав 31 млн долл. США.

Основные причины, по которым ICO-стартапы теряют деньги, это:

+ ошибки, допущенные при написании смарт-контрактов из-за недостаточного знания программистами принципов безопасной разработки;
+ ошибки, допущенные при настройке инфраструктуры, развертывании блокчейн-платформ;
+ непродуманная модель угроз, не учитывающая актуальные угрозы и реальные методы атак киберпреступников;
+ отсутствие мониторинга подозрительных транзакций.

Большинства ошибок (а значит — и финансовых потерь) можно избежать, если заранее проанализировать безопасность процедуры ICO. Специалисты Positive Technologies выявили множество уязвимостей, из которых 7% были высокого уровня риска, 40% — среднего и 53% — низкого. Однако, когда речь идет об ICO, то любая на первый взгляд незначительная уязвимость может оказаться роковой.



Доли уязвимостей различного уровня риска

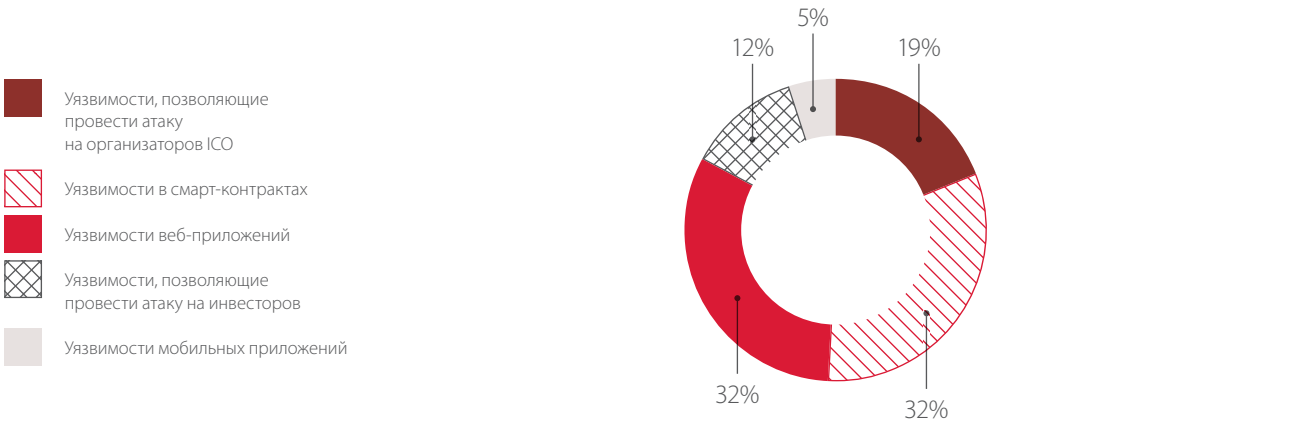
Доли проектов по максимальному уровню риска выявленных уязвимостей

Далее мы подробней рассмотрим, какие уязвимости могут содержаться в проектах ICO и как ими могут воспользоваться злоумышленники.

ВЕКТОРЫ АТАК НА ICO

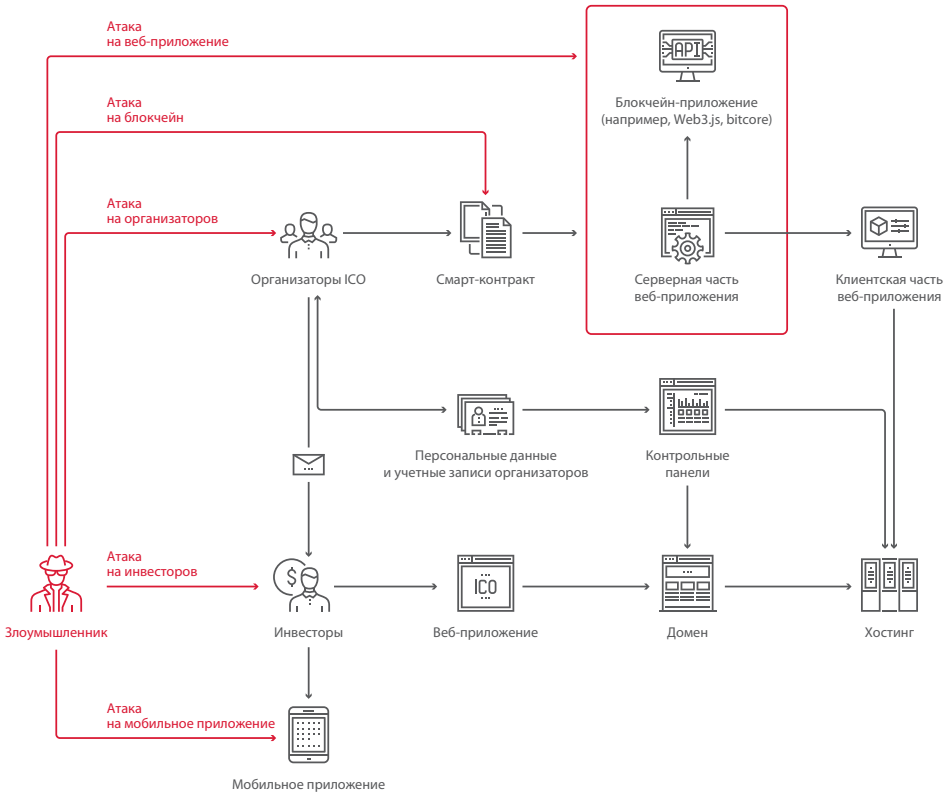
В ходе работ специалисты Positive Technologies анализировали безопасность инфраструктуры, веб-ресурсов, защиту от атак на организаторов и социальной инженерии в адрес инвесторов, искали уязвимости в смарт-контрактах и в методах аутентификации. На основании результатов завершенных проектов все недостатки были разделены на пять групп:

1) уязвимости, позволяющие провести атаку на организаторов ICO;
2) уязвимости в смарт-контрактах;
3) уязвимости веб-приложений;
4) уязвимости, позволяющие провести атаку на инвесторов;
5) уязвимости мобильных приложений.



Доли различных уязвимостей, выявленных в ходе проектов 2017 года

Рассмотрим атаки, которые злоумышленники могут совершить на инфраструктуру ICO, используя уязвимости каждой из перечисленных групп.

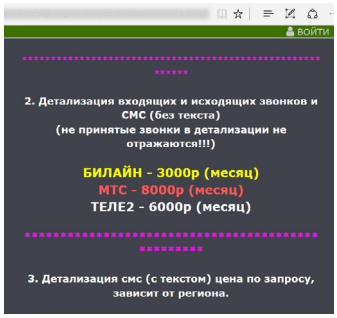


Векторы атак на ICO

АТАКИ НА ОРГАНИЗАТОРОВ ICO

В каждом третьем проекте были выявлены недостатки, позволяющие атаковать организаторов ICO

В ряде проектов была продемонстрирована возможность хищения электронной почты организатора ICO (запрашивалось восстановление пароля, а затем происходила его смена). Информация об адресах электронной почты сотрудников была доступна в поисковых системах; кроме того, практически на каждом веб-сайте ICO приводится список сотрудников (часто с фотографиями), благодаря чему можно без труда найти конкретного человека, например CEO компании, в социальных сетях. Примечательно, что информации из социальных сетей зачастую достаточно, чтобы определить логин электронной почты, а затем восстановить от нее пароль, угадав ответы на контрольные вопросы. Даже если для электронной почты настроена двухфакторная аутентификация и для восстановления пароля требуется СМС-подтверждение, это тоже не является достаточной защитой. В России для всех основных сотовых операторов на черном рынке киберпреступники могут купить детализацию входящих СМС-сообщений для любого номера телефона.



Продажа нелегального доступа к СМС

В случае реализации атаки и получения доступа к электронной почте злоумышленник может писать письма от имени организаторов (например, об изменении адреса сайта или кошелька для сбора инвестиций), а также восстанавливать пароли от различных сервисов и социальных сетей, которые зарегистрированы на эту почту. Восстановление пароля от домена или хостинга позволит киберпреступникам получить над ними полный контроль, после чего злоумышленники, например, могут подменить на сайте адрес кошелька на свой и получать деньги инвесторов. Предположительно так злоумышленникам удалось подменить адрес Ethereum-кошелька в атаке на Coindash.io, в результате чего были потеряны 7 млн долл. США.

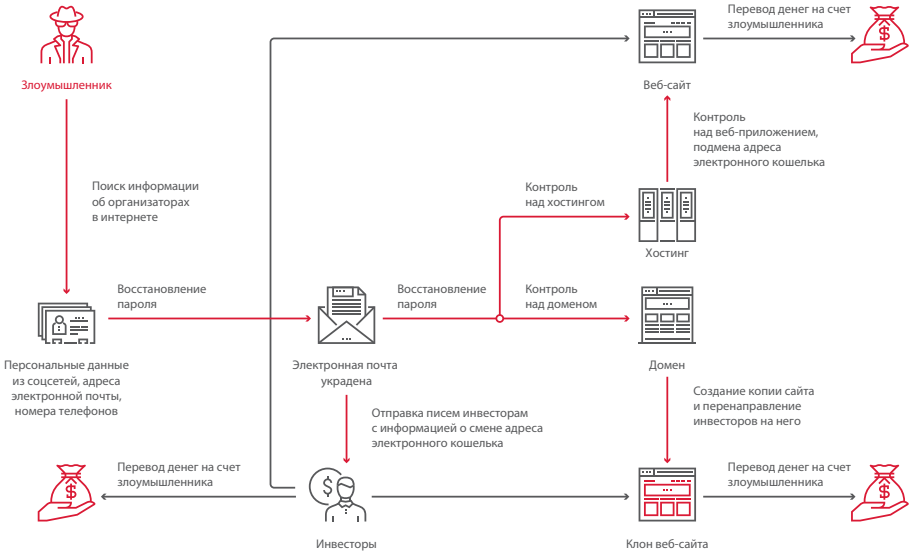


Схема атаки на организаторов ICO

АТАКИ НА СМАРТ-КОНТРАКТЫ

Уязвимости в смарт-контрактах были выявлены **в 71% проектов**, в ходе которых проводился соответствующий анализ

Треть всех уязвимостей (32%) были обнаружены специалистами Positive Technologies в смарт-контрактах. А ведь это тот элемент, который непосредственно определяет процедуру ICO, после ее запуска не может быть изменен и к тому же доступен всем участникам (то есть любой желающий может с ним ознакомиться и «оценить на прочность»).

Блокчейн-технология сегодня применяется не только в ICO, но и для решения других задач, преимущественно в финансовом секторе. Анализ блокчейн-проектов показал, что в среднем в промышленных банковских проектах в смарт-контрактах обнаруживается больше уязвимостей, чем при ICO.

Доли уязвимостей различного уровня риска, выявленных в смарт-контрактах

Наиболее часто в смарт-контрактах встречаются следующие недостатки:

- несоответствие стандарту ERC20, который описывает интерфейс токена для электронных кошельков и криптобирж;
- некорректная генерация случайных чисел;
- неверное определение области видимости;
- некорректная верификация отправителя транзакции;
- целочисленное переполнение (integer overflow);
- «состояние гонки» (race condition), в частности возможность проведения reentrancy-атак;
- ошибки в бизнес-логике.

Уязвимости в смарт-контрактах возникают из-за нехватки знаний у программистов и недостаточно тщательного тестирования исходного кода. Вот наиболее громкие инциденты:

- в июне 2016 года инвестиционный проект The DAO, построенный на базе Ethereum, за несколько часов потерял десятки миллионов долларов из-за ошибки, допущенной разработчиками при описании одной из функций;
- летом 2017 года у пользователей Parity похитили 30 млн долл. США через уязвимость в коде клиента этой криптовалютной сети Ethereum;
- в ноябре 2017 года из-за критически опасной уязвимости в новой версии смарт-контракта оказались заморожены 285 млн долл. США клиентов Parity.

АТАКИ НА ВЕБ-ПРИЛОЖЕНИЯ

В половине проектов были выявлены уязвимости в веб-приложениях

Один из главных аспектов обеспечения безопасности ICO это защищенность веб-ресурсов, ведь несанкционированный доступ к управлению сайтом и контентом может обернуться для компании потерей миллионов долларов за несколько минут.

При этом больше четверти (28%) всех выявленных недостатков в ICO были связаны именно с веб-приложениями.

Доли уязвимостей различного уровня риска, выявленных в веб-приложениях ICO

Ряд уязвимостей связан с безопасностью самого блокчейна и механизма его внедрения в серверную часть веб-приложения (например, при использовании web3.js). Так, например, узким местом является неправильная настройка CORS — механизма безопасности, который позволяет веб-приложению обращаться к приложению блокчейна. Именно спецификация CORS позволяет определять, какие запросы разрешены, а какие нет.

Некоторые уязвимости ICO свойственны всем веб-приложениям вне зависимости от сферы их использования: это инъекции, раскрытие чувствительной информации веб-сервером, небезопасная передача данных, чтение произвольных файлов и другие.

Например, в одном из проектов была обнаружена уязвимость чтения произвольных файлов (arbitrary file reading). Для эксплуатации этого недостатка злоумышленники могут зарегистрировать учетную запись у того же хостинг-провайдера, что и атакуемое веб-приложение, и получить доступ к тому же серверу, где расположен домен веб-приложения ICO. Если веб-сервер подвержен уязвимости чтения произвольных файлов, то злоумышленник может получить доступ к файлам конфигурации. В случае если преступники получат доступ к учетным данным администратора и смогут загружать на сервер произвольные файлы, они получат контроль и над веб-приложением ICO. В ходе ряда проектов специалистам Positive Technologies удалось продемонстрировать подобного рода атаку и, загрузив оболочку командной строки на веб-сервер, получить полный контроль над веб-приложениями ICO.

Проведя атаку на уязвимый сайт, злоумышленники могут подменить адрес кошелька, и тогда деньги инвесторов направятся к преступникам, а не к организаторам ICO.

АТАКИ НА ИНВЕСТОРОВ

В 23% проектов были выявлены недостатки, позволяющие атаковать инвесторов

Заботиться о безопасности инвесторов важно, потому что именно от этих людей зависит успех ICO-проекта. Довольно часто злоумышленники используют методы социальной инженерии, чтобы присвоить деньги инвесторов. Например, во многих проектах встречался один и тот же недостаток: учетные записи в социальных сетях и доменные имена, схожие по написанию с легитимными, а также региональные домены были доступны для регистрации (например, адрес проекта icoproject.com, а злоумышленник может зарегистрировать icoproject.io). Такая уязвимость оценивается нами ниже среднего уровня риска. Однако злоумышленники могут зарегистрировать учетную запись в социальной сети (например, twitter.com, facebook.com и др.), в точности повторяющую название ICO (или со схожим написанием) и выдавать себя за организаторов: публиковать там новости, адреса кошельков и ссылки на поддельные веб-приложения. Мы рекомендуем проверить и зарегистрировать во всех социальных сетях всевозможные варианты написания проекта, а также занять созвучные доменные имена до начала проведения ICO.

Есть множество примеров, когда злоумышленники воспользовались этим. Так, в ходе атаки на пользователей американской криптовалютной биржи Bittrex пользователи вместо авторизации на официальном bittrex.com, не заметив подмены, вводили свои аутентификационные данные на фишинговом ресурсе blttrex.com (в адресе вместо i была использована буква L). Затем с помощью полученной информации злоумышленники забирали со счетов криптовалюту жертв через официальный веб-сайт.

Схема атаки на инвесторов

АТАКИ НА МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ

В 100% мобильных приложений для ICO были выявлены уязвимости

Современные реалии таковы, что люди охотнее пользуются мобильными приложениями, а не веб-сайтами, так как много времени проводят именно с телефоном в руках. И для удобства пользователей некоторые организаторы ICO специально разрабатывают мобильные приложения.

В ходе работ по анализу безопасности и защите процедуры ICO специалисты Positive Technologies отметили, что мобильные приложения содержат в 2,5 раза больше уязвимостей, чем веб-приложения тех же ICO-проектов. Среди наиболее распространенных недостатков были небезопасная передача данных, хранение пользовательских данных в резервных копиях, служебная информация, оставленная разработчиками в коде приложения, раскрытие идентификатора сессии. Эти недостатки позволяют получить дополнительные сведения о проекте, организаторах и инвесторах и могут быть использованы злоумышленниками в ходе дальнейших атак. А в случае получения доступа к мобильному телефону жертвы злоумышленник может получить доступ к приложению и выполнять действия от его лица, в том числе вывести средства. Конечно, такая атака сложна в реализации, однако, учитывая, как быстро совершенствуется вредоносное ПО, позволяющее получить удаленный контроль над смартфоном, такой сценарий действий киберпреступников вполне возможен.

Примечательно, что аналогичные уязвимости, соответствующие недостаткам в мобильных приложениях, в веб-приложениях отсутствовали. Можно сделать вывод, что разработчики уделяли больше внимания безопасности сайтов.

Схема атаки на мобильное приложение

ВЫВОДЫ

Процедура ICO краткосрочна, крайне важно предусмотреть векторы атак до ее начала, иначе высок риск финансовых потерь. Своевременное обнаружение уязвимостей позволяет организаторам принять все необходимые меры защиты заранее, а в рамках ICO направить свое внимание на бизнес. Так, например, после устранения уязвимостей, выявленных специалистами Positive Technologies, utrust.io в ходе успешного ICO собрал 21 млн долл. США, trade.io — 31 млн долл. США, а Blackmoon — 30 млн долл. США. Ни одна из компаний, обратившихся к нам за защитой процедуры ICO, не пострадала от кибератак, и все они успешно завершили процесс ICO.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com facebook.com/PositiveTechnologies facebook.com/PHDays