kaspersky

Угрозы безопасности для систем обработки и хранения биометрических данных

Кирилл Круглов

02.12.2019 Version 1.0

Оглавление

Системы цифровой обработки биометрических данных изначально использовались в основном государственными органами и специальными службами (полиция, таможня и т.п.). Стремительное развитие IT-технологий сделало биометрические системы доступными для «гражданского» использования. Они быстро проникают в нашу повседневную жизнь, дополняя и заменяя традиционные методы аутентификации, например, по логину и паролю. В самом деле, идентификация человека по уникальным, присущим только ему одному, характеристикам – отпечатку пальца, голосу, форме лица или особенностям строения глаза – кажется очевидным и невероятно удобным в использовании методом.

Сегодня аутентификацию по биометрическим данным используют для доступа в офисы государственных и коммерческих организаций, к системам автоматизации промышленных предприятий, к корпоративным и личным ноутбукам и мобильным телефонам. И количество, и разнообразие способов применения этих технологий продолжает расти.

К сожалению, как произошло и со многими другими, бурно развивавшимися в последнее время технологиями, системы биометрической аутентификации оказались не лишены существенных родовых недостатков. Для технологий биометрической аутентификации ключевыми недостатками стали проблемы их информационной безопасности.

В статье мы вкратце расскажем о многих проблемах информационной безопасности технологий биометрической аутентификации и приведём результаты нашего собственного исследования, дающего дополнительную информацию для более объективной оценки рисков, связанных с использованием систем биометрической аутентификации в современном их исполнении.

Особенности обработки и хранения биометрических данных

Представления о биометрических данных как об уникальном неподделываемом идентификаторе человека изначально неверны и могут внушать ложное чувство защищенности.

Во-первых, точность их распознавания системами аутентификации, хотя и относительно высока, может оказаться всё-таки недостаточной для многих применений. Ведь речь идёт не о простом вычислении равенства (или неравенства) двух хэш-сумм, как в случае с парольной аутентификацией. Биометрические системы имеют обычно ненулевые вероятности ложноотрицательного и ложноположительного срабатывания.

Во-вторых, как показывают исследования, многие из биометрических характеристик человека могут быть фальсифицированы (подделаны) злоумышленником. А скопировать оцифрованные биометрические данные может быть даже проще, чем физические.

В третьих (и это – самое важное!), однажды скомпрометированные биометрические данные скомпрометированы навсегда – пользователь не сможет поменять украденные отпечатки пальцев, как меняет пароль в случае его кражи. При этом биометрические данные могут одновременно оказаться скомпрометированными везде, где они используются. Потенциально человек может страдать от этой проблемы на протяжении всей оставшейся жизни.

С учётом всего написанного выше особенно удивительно, как беззаботно относятся разработчики и пользователи систем биометрической аутентификации к задаче защиты от компьютерных атак самих систем и собранных биометрических данных.

Оказывается, данные биометрии могут храниться в легкодоступном для злоумышленника виде. Яркий пример – нашумевшая история с крупнейшей утечкой данных из биометрической системы BioStar 2 – веб-платформы биометрического контроля доступа в помещения. Как заявили исследователи, они обнаружили в открытом доступе базу данных сервиса (более 27,8 миллиона записей, в общей сложности больше 23 гигабайт личных данных сотрудников 5 700 организаций из 83 стран). Среди прочих конфиденциальных данных база содержала около 1 миллиона записей с отпечатками пальцев, а также информацию для систем распознавания лиц. При этом, согласно отчету, «…вместо того, чтобы хранить хэши отпечатков пальцев (не позволяющие воссоздать отпечатки), они хранят оригиналы, которые могут быть скопированы для вредоносных целей».

Проблема, на которую указали исследователи в истории с BioStar 2, к сожалению, отнюдь не надуманная. Уже известны случаи, когда биометрические данные оказывались целью атак злоумышленников. Так в 2015 году, в результате кибератаки в числе прочей информации было украдено почти шесть миллионов отпечатков пальцев людей, имеющих отношение к гос. аппарату США.

С ростом количества возможных применений систем биометрической аутентификации нетрудно предположить, что данные биометрии заинтересуют не только представителей спецслужб (а именно они, согласно предположению пострадавшей стороны, скорее всего, стояли за атакой на Управление кадровой службы США в 2015 году), но и многие другие категории злоумышленников.

Угрозы, заблокированные на системах обработки и хранения биометрических данных

Принимая во внимание риски, описанные выше, мы решили оценить, насколько системы обработки биометрических данных (серверы обработки и хранения, а также рабочие станции, выполняющие функцию сбора биометрических данных) открыты для атак вредоносного ПО, и провели исследование угроз, заблокированных продуктами «Лаборатории Касперского» на таких системах.

Объект исследования

Компьютеры (серверы и рабочие станции), используемые для сбора, обработки и хранения биометрических данных (таких как отпечатки пальцев, геометрия кисти руки, шаблоны лица, голоса и радужной оболочки глаза), на которых установлены продукты «Лаборатории Касперского».

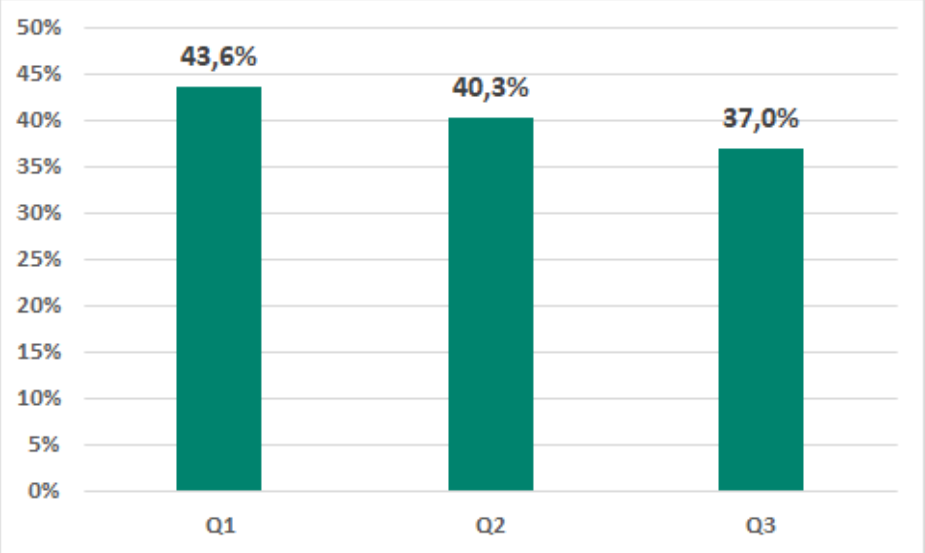
Отчетный период

Третий квартал 2019 года.

Треть систем под угрозой

По данным Kaspersky Security Network (KSN) в третьем квартале 2019 года вредоносное ПО было заблокировано на 37% компьютеров, выполняющих функции сбора, обработки и хранения биометрических данных, т.е. фактически – каждый третий компьютер подвергся риску заражения вредоносным ПО.

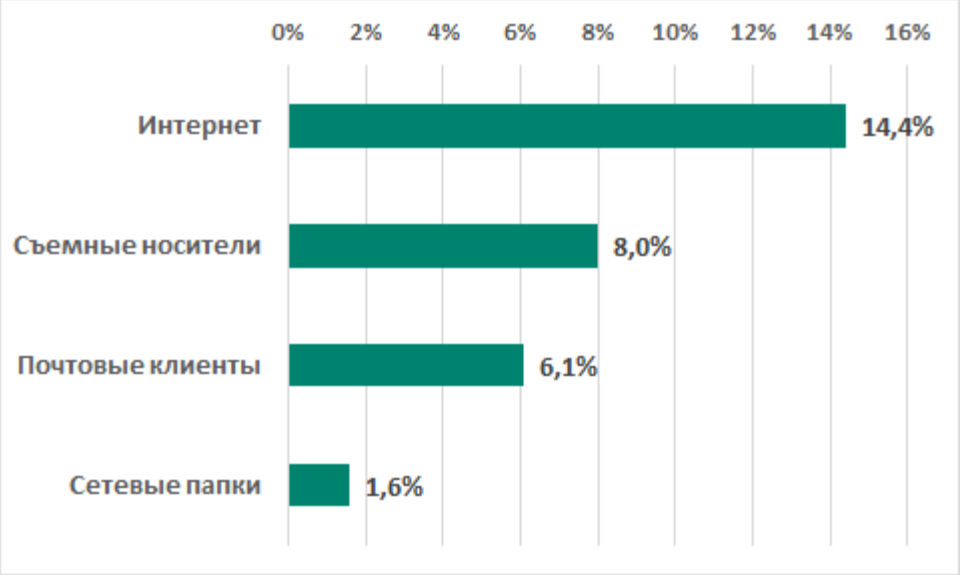
В данных по кварталам видно, что процент компьютеров, на которых было заблокировано вредоносное ПО, с начала 2019 года снизился на 6.6 п.п., но всё же находится на достаточно высоком уровне.



Процент компьютеров систем обработки биометрических данных, на которых было заблокировано вредоносное ПО, первые три квартала 2019 года

Источники угроз

Анализ источников угроз показал, что, как и для многих других систем, которые предполагают повышенные меры защиты (например, системы промышленной автоматизации, системы управления зданиями и др.), для систем обработки биометрии основным источником угроз является интернет.



Основные источники угроз для систем обработки и хранения биометрических данных, третий квартал 2019

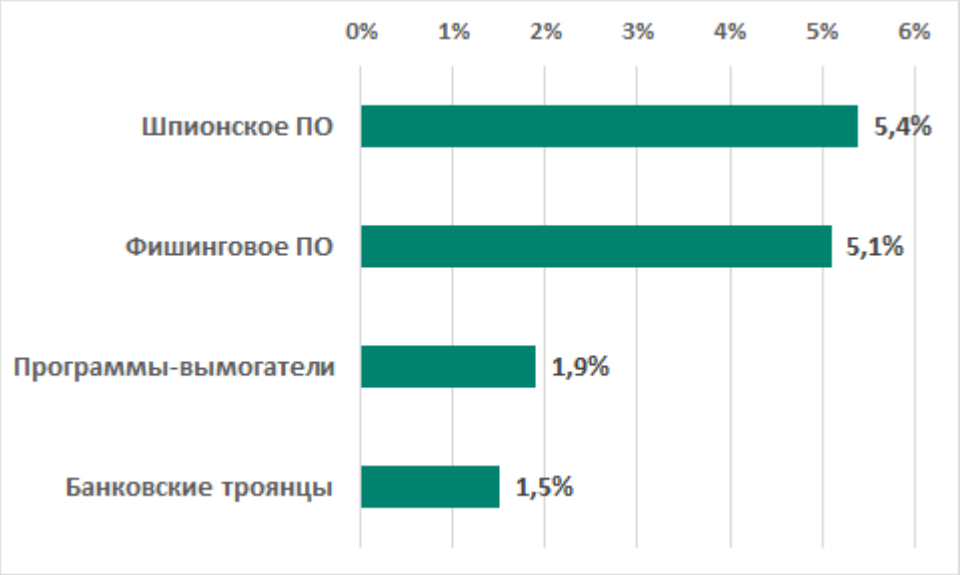
Угрозы из интернета были заблокированы на 14,4% всех систем обработки биометрических данных. В эту категорию входят угрозы, заблокированные на вредоносных и фишинговых сайтах, а также на почтовых веб-сервисах.

Съемные носители (8%) и сетевые папки (6,1%) чаще всего используются для распространения вредоносного ПО типа черви (Worm). Заразив компьютеры, черви, как правило, загружают на них шпионское (Spyware, Remote Access Trojan) и вымогательское (Ransomware) ПО.

Что касается угроз, заблокированных при попытке проникнуть через почтовые клиенты, то в большинстве случаев это были типовые фишинговые письма (фальшивые сообщения о доставке, оплате счетов, RFQ, RFP и т.д.), содержащие ссылки на вредоносные сайты или вложенные офисные документы, в которые встроен вредоносный код.

Особо опасны

Среди угроз, заблокированных на системах обработки и хранения биометрических данных, мы выделили шпионское вредоносное ПО (Spyware/RAT), вредоносные программы, используемые в фишинговых атаках (в основном, Trojan-Downloader и Trojan-Dropper, с помощью которых компьютер заражается вредоносными программами-шпионами), программы-вымогатели (Ransomware) и банковские троянцы (Banking Trojans), которые, на наш взгляд, представляют наибольшую опасность для таких систем.



Некоторые типы вредоносного ПО, заблокированного на системах обработки и хранения биометрических данных

В общей сложности за третий квартал 2019 года шпионское вредоносное ПО было заблокировано на 5,4% компьютеров, используемых для сбора, обработки и хранения данных биометрии. Вредоносные программы, используемые в фишинговых атаках, и вымогательское ПО – на 5,1% и 1,9% соответственно.

Важно отметить, что среди прочих типов встречалось также вредоносное ПО для кражи банковских данных (1,5%). Скорее всего, оно не было предназначено для кражи биометрических данных. Однако можно ожидать, что массовое вредоносное ПО, направленное на кражу биометрических данных в банках и финансовых системах, появится в ближайшем будущем.

Заключение

Итак, в третьем квартале 2019 года 37% компьютеров, используемых для сбора, обработки и хранения биометрических данных, подверглись риску заражения вредоносным ПО. В числе прочих вредоносных объектов продуктами «Лаборатории Касперского» были заблокированы современные троянские программы для удалённого доступа к системе (5,4% всех исследованных компьютеров), вредоносные программы, используемые в фишинговых атаках (5,1%), программы-вымогатели (1,9%) и банковские троянцы (1,5%).

Несмотря на то, что вредоносное ПО, заблокированное на исследуемых компьютерах, не предназначено специально для систем обработки биометрии, не следует недооценивать представляемую им опасность.

Подобное вредоносное ПО способно:

- красть конфиденциальную информацию;
- загружать и выполнять произвольное ПО;
- обеспечивать злоумышленникам возможность удалённого управления зараженными компьютерами.

Хотя эти угрозы не направлены непосредственно на кражу или манипулирование биометрическими данными, технически некоторые из них имеют все возможности для этого. Кроме того, побочные явления, связанные с активным заражением, могут серьёзно влиять на доступность систем аутентификации и целостность биометрических данных.

Поэтому мы считаем, что подвергать биометрические данные воздействию случайных киберугроз – это огромный риск как для провайдера сервиса, так и для людей, которые доверили ему свои биометрические данные.

Отметим также, что, как мы обнаружили в ходе исследования, системы обработки и хранения биометрических данных (в частности, базы биометрических данных) часто разворачивают не на специально выделенных компьютерах, а на общих с другими системами серверах приложений. Другими словами, если злоумышленник взломает, скажем, почтовый сервер или базу данных веб-сайта организации, использующей в своей работе системы биометрической аутентификации, то есть шанс, что он обнаружит на том же сервере и базу биометрических данных.

С учётом всего, написанного выше, сложившаяся ситуация с безопасностью биометрических данных кажется нам критической и требует внимания не только отраслевых и государственных регуляторов, сообщества экспертов по информационной безопасности, но и широкой общественности. Ведь в зоне риска в данном случае может оказаться каждый – вне зависимости от рода деятельности, профессиональной принадлежности и навыков.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com