УДК 004.05

Кунакбаев Е.Г.,
студент
2 курс, факультет «Информационная безопасность»
Нефтекамский филиал Башкирского Государственного Университета
Россия, г. Нефтекамск
Научный руководитель: Аюпова А.Р.,
доцент кафедры математического анализа и информационной безопасности
Нефтекамский филиал Башкирского Государственного Университета
Россия, г. Нефтекамск

УСОВЕРШЕНСТВОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

Аннотация: *в статье рассматривается систем, которая создает уникальный цифровой отпечаток устройств, «связывает» с ними пользователя и его аккаунты, благодаря чему с большей точностью можно отличить его действия клиента от действий мошенников, а так же проблемы безопасности связанные с корпоративными виртуальными устройствами.*

Ключевые слова: *цифровую личность, глобальной идентификации пользователя, банковские системы, проблемы безопасности корпоративных виртуальных устройств, кибератаки, эксплойты.*

Annotation: *the article discusses a system that creates a unique digital fingerprint of devices, "connects" the user and his accounts with them, so that you can more accurately distinguish his client actions from the actions of fraudsters, as well as security problems associated with corporate virtual devices.*

Key words: *digital identity, global user identification, banking systems, security issues of corporate virtual devices, cyber-attacks, exploits.*

С финансовым мошенничеством сегодня может столкнуться любая компания. Это и коррупционные схемы, и недобросовестные заемщики, и ненадежные контрагенты, и корпоративные споры. При этом из-за развития современных технологий способы подобных афер могут быть самыми разными. А их расследование фактически невозможно без анализа устройств, с которых осуществлялись коммуникации, исследования огромных массивов цифровых данных, а зачастую и извлечения или корректного восстановления информации, которую кто-то захочет скрыть. По статистике, 78% российских компаний признают, что пострадали от экономических преступлений хотя бы раз за последние три года [1].

В последнее время компания Group-IB представила способ защитить «цифровую личность» клиентов банков. С помощью данной системы за первые шесть месяцев 2020 года в пяти крупных российских банках было предотвращено нанесение ущерба киберугрозы на сумму 320 млн рублей в пяти крупных российских банках. Ежедневно данная платформа защищает порядка 130 млн пользователей. Fraud Hunting Platform анализирует в режиме реального времени каждую сессию и поведение пользователя и на веб-ресурсах, и в мобильных приложениях. Таким образом, система создает уникальный цифровой отпечаток устройств, «связывает» с ними пользователя и его аккаунты, благодаря чему с большей точностью можно отличить его действия клиента от действий мошенников, даже если те завладели мобильным телефоном или платежными данными жертвы. Эта технология получила название Global ID — глобальной идентификации пользователя.

Данная система является уникальной для защиты от онлайн-мошенничества. Высокая производительность, легкая интеграция и

использование запатентованных технологий обнаружения атаки до ее реализации [2].

Так же не надо забывать и о безопасности мобильных приложений, с помощью которых работают многие банковские системы. Согласно последнему отчету Orca Security о безопасности виртуальных устройств 2020, защита виртуальных устройств отстает, поскольку цифровая трансформация в различных отраслях ускоряет переход к облаку.

В докладе рассматриваются основные проблемы безопасности корпоративных виртуальных устройств, и обнаруживается, что большое количество известных и исправляемых уязвимостей быстро распространяется.

Чтобы помочь отрасли безопасности облачных вычислений повысить уровень защиты и снизить риски для клиентов,в отчете было проанализировано 2 218 образов виртуальных устройств от 540 поставщиков программного обеспечения, проанализированы известные уязвимости и другие риски, чтобы дать объективные оценки и рейтинги.

Отчет выявил 17 критических уязвимостей, которые считаются критическими, если виртуальное устройство имеет такие незащищенные уязвимости. Некоторые из этих известных и простых в использовании уязвимостей включают：

- EternalBlue
- DejaBlue
- BlueKeep
- DirtyCOW
- Heartbleed

Как показано на рисунке ниже, более половины проверенных виртуальных устройств имеют более низкий средний рейтинг, 56% из которых получают оценку C или ниже, а 15% получают только оценку F (не пройденный тест).(F-15,1%, D-16,1%, C-25%).

После того, как вышеприведенные результаты были опубликованы, 287 обновлений безопасности от соответствующих поставщиков программного обеспечения были повторно протестированы и обнаружили, что средний рейтинг этих виртуальных устройств увеличился с B до A.

С течением времени и отсутствием обновлений несколько виртуальных устройств подвергаются риску безопасности. Исследование показало, что большинство поставщиков не обновляли или не прекращали свои устаревшие или устаревшие (EOL) продукты.

Исследование показало, что только 14% (312) файлов изображений виртуальных устройств были обновлены за последние три месяца.

Между тем, 47% (1,049) не обновлялись в прошлом году; по крайней мере 5% (110) вопросов были проигнорированы в течение трех лет, в то время как 11% (243) версий или операционных систем EOL были запущены.

Однако некоторые устаревшие виртуальные устройства были обновлены после первоначального тестирования. Например, продукт Redis Labs забил F из-за устаревшей операционной системы и многих уязвимостей, но теперь получил оценку A+ после обновления.

Основываясь на принципе координации раскрытия уязвимостей, исследователь отправляет электронное письмо непосредственно каждому поставщику, призывая его к решению проблем безопасности. К счастью, производители облачных систем безопасности имеют очень позитивное отношение и отзывчивость.

По состоянию на выпуск отчета несколько известных производителей устранили 36259 из 401571 уязвимостей путем исправления или удаления виртуальных устройств. Некоторые из этих ключевых исправлений или обновлений включают：

- Dell EMC выпустила важные бюллетени по безопасности для своей виртуальной версии CloudBoost;

- Cisco выпустила исправление для 15 проблем безопасности, которые были обнаружены в одном из виртуальных устройств, отсканированных в исследовании ;
- IBM обновила или удалила три виртуальных устройства за неделю ;
- Symantec снял три продукта с более низким счетом ;
- Splunk, Oracle, IBM, "Лаборатория Касперского" и Cloudflare также вышли на полки ;
- Zoho обновил половину самых уязвимых продуктов ;
- Qualys обновил виртуальное устройство с 26-месячной историей, которая включает в себя уязвимость перечисления пользователей, обнаруженную и сообщенную самим Qualys в 2018 [3].
- Департамент финансов США также добавил в своем докладе, что сегодня, когда мировая экономика ускоряется в эпоху цифровых технологий, цифровые идентификационные продукты и услуги, как ожидается, повысят доверие, безопасность, конфиденциальность и удобство идентификации физических и юридических лиц, тем самым повышая безопасность процессов, которые имеют решающее значение для движения денег, товаров и данных.
- Системы цифровой идентификации также могут принести такие преимущества, как экономия средств и повышение эффективности для компаний финансовых услуг. Например, надежные системы цифровой идентификации могут повысить эффективность идентификации клиентов и проверки на борту, а также разрешить доступ к учетным записям, общее управление рисками и меры по борьбе с мошенничеством.
- Совместная работа с данными / Unicom (в отличие от силосов данных), то есть подключение и управление различными данными в автономном режиме и в интернете, является неотъемлемой частью модернизации отрасли. Отчёт Министерства финансов и бюллетень OCC были опубликованы после принятия закона О стимулировании экономического

роста, ослаблении нормативных требований и защите прав потребителей (подписанного 24 мая 2018 года).Этот длинный законопроект упрощает некоторые положения, в том числе позволяет пользователям открывать счета в финансовых учреждениях или получать финансовые продукты или услуги от финансовых учреждений, используя отсканированные копии водительских прав или личных удостоверений личности.Кроме того, он отменяет хранение бумаги и позволяет банкам хранить или хранить такую информацию в любом электронном формате.

- После того, как OCC объявила о принятии National Banking license для компаний, занимающихся банковским бизнесом, не связанных с депозитом FinTech (Fintech) в США, Американская ассоциация банкиров, банкиры независимого сообщества США, Национальная Ассоциация кредитных союзов и Национальная ассоциация федеральных кредитных союзов, вместе отправили письмо подкомитету по цифровой торговле и защите потребителей Палаты представителей США.В этом письме содержится следующее заявление:

- Любой принятый закон должен гарантировать, что все организации, обрабатывающие конфиденциальные финансовые данные потребителей, должны иметь надежный, гибкий и масштабируемый процесс защиты этих данных, а также должны быть объединены с эффективными нормативными и исполнительными процедурами для обеспечения подотчетности и соответствия требованиям. Эти требования имеют решающее значение, поскольку они ограничивают нарушения, снижают потребительский риск и могут привести к значительным потерям затрат для клиентов. Этот стандарт должен применяться ко всем организациям, обрабатывающим конфиденциальные личные и финансовые данные, чтобы обеспечить значимую и последовательную защиту для потребителей по всей стране.

Таким образом, многие люди с нетерпением ждут безопасной эпохи открытого банкинга. Учитывая растущую ситуацию с кибератаками и

эксплойтами, потребители ожидают, что разработчики политики смогут взглянуть на общую картину, понять ситуацию и разработать надежный механизм аутентификации клиентов в соответствии с их потребностями [4].

Использованные источники:

1. Право.ru. Финансовые преступления: как их расследуют киберкриминалисты. [Электронный ресурс]. URL: https://pravo.ru/story/226969/?desc_chrono_7_2= (Дата обращения: 3.11.2020)

2. Известия. Group-IB представила способ защитить «цифровую личность» клиентов банков. [Электронный ресурс]. URL: https://iz.ru/1080662/2020-10-30/group-ib-predstavila-sposob-zashchitit-tcifrovuiu-lichnost-cheloveka (Дата обращения: 3.11.2020).

3. Orca Security. The Orca Security 2020 State of Virtual Appliance Security. Доклад о состоянии безопасности виртуальных устройств 2020 [Электронный ресурс]. URL: https://orca.security/wp-content/uploads/The-Orca-Security-2020-State-of-Virtual-Appliance-Security.pdf (Дата обращения: 3.11.2020).

4. A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation. Адрес детального доклада "финансовая система, создающая экономические возможности: небанковские финансы, финтех и инновации". [Электронный ресурс]. URL: https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities—Nonbank-Financi….pdf (Дата обращения: 3.11.2020).