KASPERSKY lab

Анализ защищённости корпоративных систем в 2017 году

Август 2018

www.kaspersky.ru
#truecybersecurity

Содержание

Введение 3

Анализ защищённости со стороны внешних нарушителей 4

Векторы преодоления сетевого периметра 5

Атаки через уязвимости веб-приложений 5

Атаки через интерфейсы управления 7

Статистика наиболее распространённых уязвимостей и недостатков защиты 8

Анализ защищённости со стороны внутренних нарушителей 9

Наиболее часто используемые атаки и техники 12

Статистика наиболее распространённых уязвимостей и недостатков защиты 19

Анализ защищённости веб-приложений 20

Анализ уязвимостей 23

Статистика по общему количеству уязвимостей 24

Статистика по приложениям 25

Рекомендации по повышению защищённости веб-приложений 26

Заключение 26

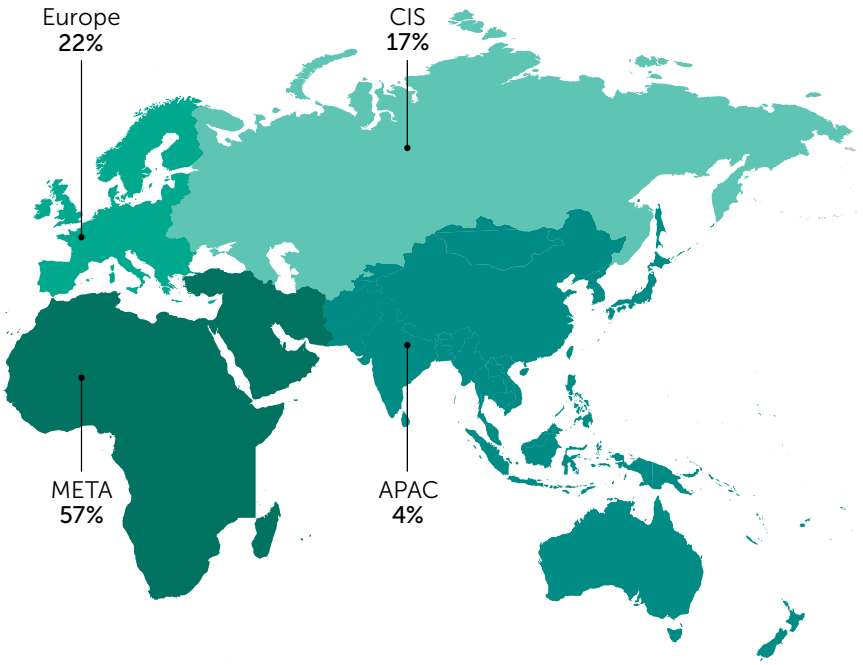
Введение

Отдел экспертных сервисов Лаборатории Касперского ежегодно проводит десятки проектов по анализу защищённости российских и зарубежных компаний. Мы подвели основные итоги и статистику по анализу защищённости корпоративных информационных систем в 2017 году.

Основная цель данной публикации – информационная поддержка специалистов по обеспечению информационной безопасности в области актуальных уязвимостей и векторов атак на современные корпоративные информационные системы.

Суммарно было проанализировано несколько десятков проектов для компаний из разных отраслей: государственные учреждения, финансовые организации, телекоммуникационные и ИТ-компании, промышленные организации, и энергетические компании.

Распределение анализируемых компаний по отраслям и регионам



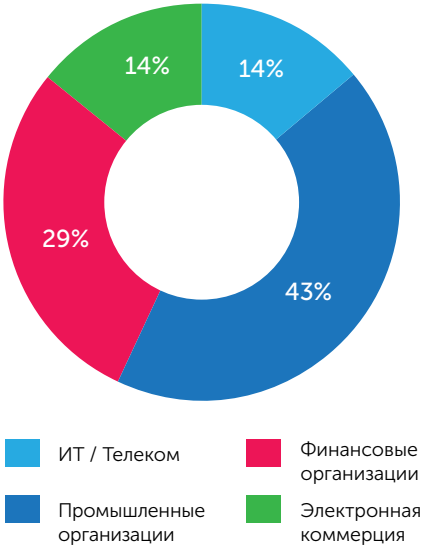
Итоги и статистика по уязвимостям были подведены раздельно по предоставляемым услугам:

- **Внешнее тестирование на проникновение** – анализ защищённости организации с позиции нарушителя, находящегося в сети Интернет и обладающего только общедоступной информацией.
- **Внутреннее тестирование на проникновение** – анализ защищённости организации с позиции нарушителя, находящегося в корпоративной сети заказчика, обладающего только физическим доступом к анализируемым объектам без каких-либо привилегий во внутренней сети.
- **Анализ защищённости веб-приложений** – поиск уязвимостей и недостатков защиты, допущенных в ходе проектирования, разработки и эксплуатации веб-приложения, включающий практическую демонстрацию возможности использования уязвимостей.

В отчете приведена статистика наиболее распространённых уязвимостей и недостатков защиты, которые были обнаружены специалистами «Лаборатории Касперского» и которыми потенциально могут воспользоваться злоумышленники для несанкционированного проникновения в инфраструктуру компаний.

Анализ защищённости со стороны внешних нарушителей

Анализируемые компании



Для оценки уровня защищённости использовалась шкала:

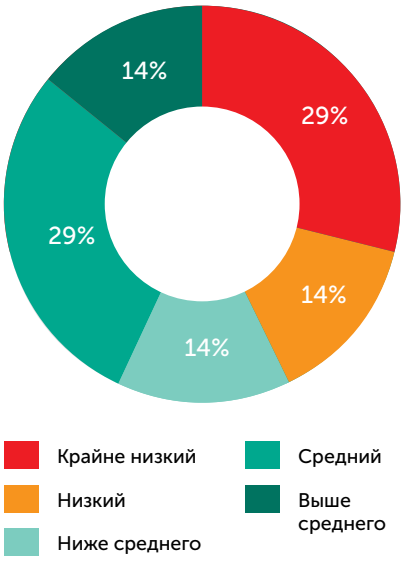
- **Крайне низкий**
- **Низкий**
- **Ниже среднего**
- **Средний**
- **Выше среднего**
- **Высокий**

Итоговый уровень защищённости оценивался на основе собственной методики «Лаборатории Касперского», учитывающей полученный уровень доступа, степень критичности информационных ресурсов, сложность получения доступа, а также требуемые временные затраты.

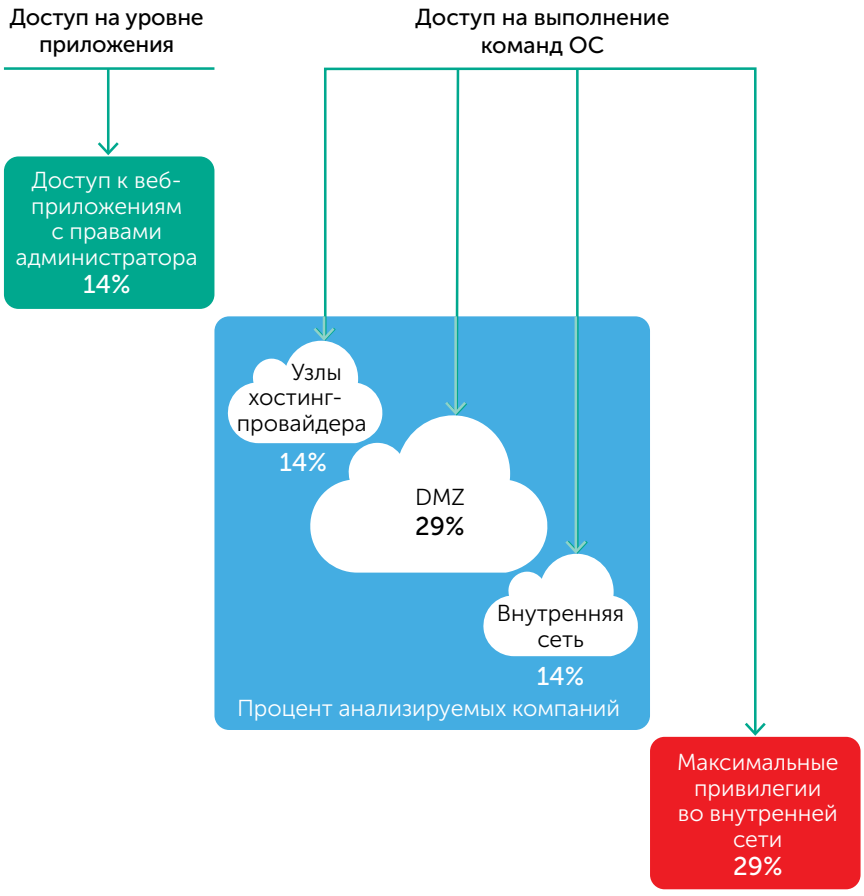
Крайне низкому уровню защищённости соответствует случай, когда удалось преодолеть внешний периметр и получить доступ к критически важным ресурсам внутренней сети (максимальные привилегии внутренней сети, полный контроль над ключевыми бизнес-системами, доступ к критически важной информации). Более того, получение указанного доступа не требует высокой квалификации и больших временных затрат.

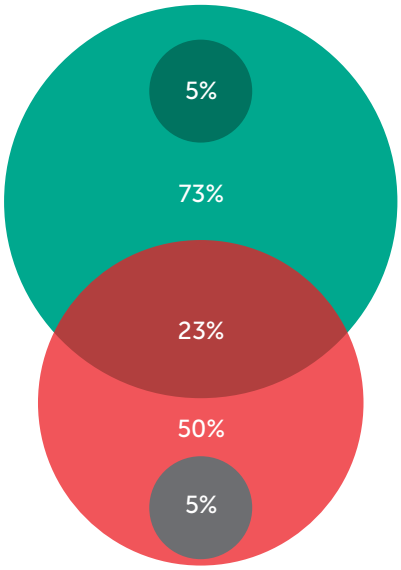
Высокий уровень защищённости соответствует случаю, когда на сетевом периметре заказчика были выявлены только незначительные уязвимости, эксплуатация которых не несет рисков для компании.

Уровень защищённости компаний



Распределение анализируемых компаний по полученному уровню доступа





- Эксплуатация известных уязвимостей веб-компонентов (веб-сервера, библиотеки)
- Атаки через уязвимости веб-приложений
- Атаки через интерфейсы управления и эксплуатацию уязвимостей веб-приложений
- Атаки через интерфейсы управления
- Эксплуатация известных уязвимостей ПО интерфейсов управления

Векторы преодоления сетевого периметра

Большинство реализованных векторов атак стали возможными из-за недостаточного межсетевого экранирования и открытого доступа к интерфейсам управления, использованияю слабых паролей учётных записей и наличия уязвимостей в веб-приложениях.
Несмотря на то, что использование устаревшего уязвимого ПО был обнаружено у 86% всех анализируемых компаний, лишь в 10% векторов преодоления внешнего периметра (28% анализируемых компаний) эксплуатировались уязвимости, связанные с отсутствием актуальных обновлений ПО, поскольку эксплуатация этих уязвимостей зачастую связана с рисками отказа в обслуживании. Указанные ограничения в демонстрации атак обусловлены преимущественно особенностями проведения работ по тестированию на проникновение, когда сохранение работоспособности ресурсов заказчика является приоритетом, однако реальные злоумышленники могут не принимать их во внимание.

Рекомендация:

Помимо процесса управления обновлениями, уделять большее внимание настройке правил сетевой фильтрации, парольной защите, а также устранению уязвимостей веб-приложений.

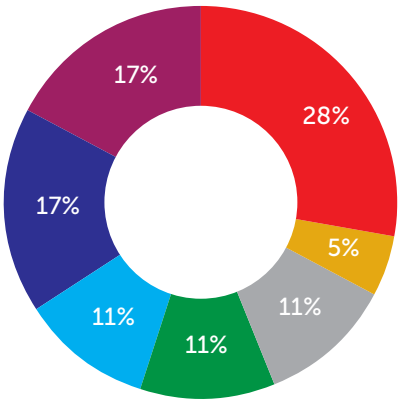
Атаки через уязвимости веб-приложений

Результаты тестирований на проникновение, проведенных в 2017 году, однозначно свидетельствуют о том, что недостаточное внимание уделяется безопасности веб-приложений. В 73% реализованных векторов атак для получения доступа к узлам сетевого периметра использовались веб-уязвимости.
Наиболее распространённая веб-уязвимость, использованная для преодоления сетевого периметра при проведении тестирований на проникновение – «Загрузка произвольных файлов». Она применялась для загрузки интерпретатора командной строки и получения доступа к ОС. Уязвимости типа «Внедрение операторов SQL», «Чтение произвольных файлов», «Внедрение внешних сущностей XML» использовались преимущественно для получения чувствительной информации: паролей или их хэш-сумм (далее хэш). Пароли учётных записей использовались для развития атаки через общедоступные интерфейсы управления.

Рекомендация:

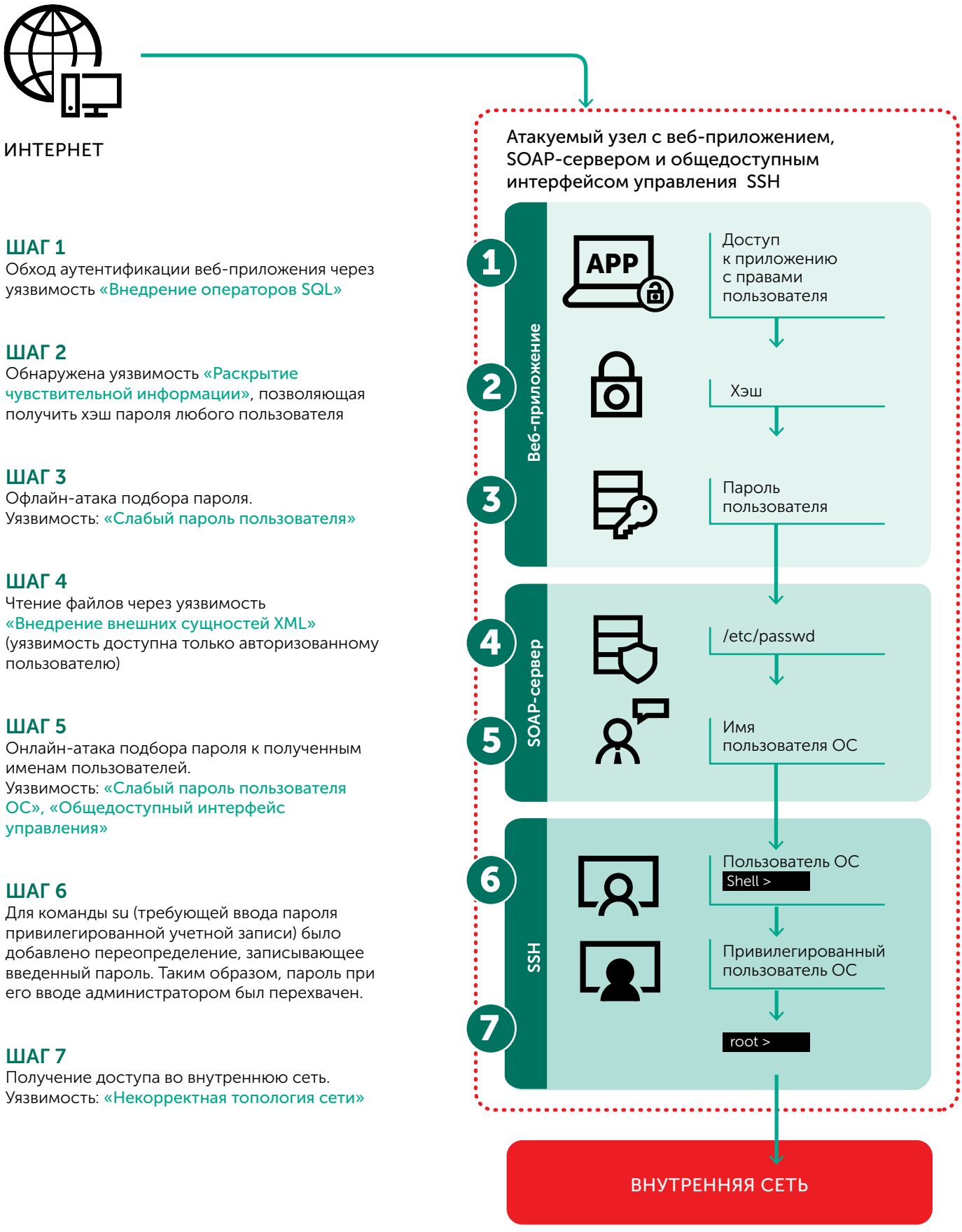
Проводить анализ защищённости всех общедоступных веб-приложений на регулярной основе. Необходимо организовать процесс управления уязвимостями и проводить проверку приложения после внесения изменений в программный код приложения, изменений конфигурации веб-сервера, а также следить за обновлениями используемых сторонних компонентов и библиотек.

Уязвимости веб-приложений, которые использовались для преодоления сетевого периметра



- Загрузка произвольных файлов
- Внедрение внешних сущностей XML
- Другие
- Создание/изменение произвольных файлов
- Чтение произвольных файлов
- Внедрение операторов SQL
- Внедрение кода

Пример получения доступа во внутреннюю сеть через веб-уязвимости и общедоступные интерфейсы управления



ШАГ 1
Обход аутентификации веб-приложения через уязвимость «Внедрение операторов SQL»

ШАГ 2
Обнаружена уязвимость «Раскрытие чувствительной информации», позволяющая получить хэш пароля любого пользователя

ШАГ 3
Офлайн-атака подбора пароля.
Уязвимость: «Слабый пароль пользователя»

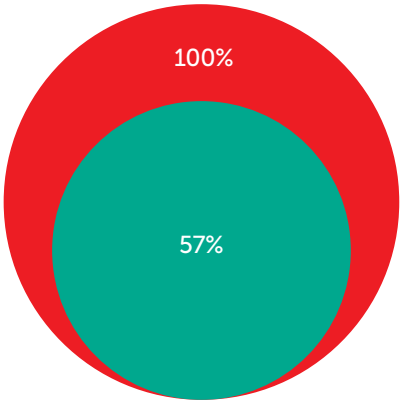
ШАГ 4
Чтение файлов через уязвимость «Внедрение внешних сущностей XML» (уязвимость доступна только авторизованному пользователю)

ШАГ 5
Онлайн-атака подбора пароля к полученным именам пользователей.
Уязвимость: «Слабый пароль пользователя ОС», «Общедоступный интерфейс управления»

ШАГ 6
Для команды su (требующей ввода пароля привилегированной учетной записи) было добавлено переопределение, записывающее введенный пароль. Таким образом, пароль при его вводе администратором был перехвачен.

ШАГ 7
Получение доступа во внутреннюю сеть.
Уязвимость: «Некорректная топология сети»

Атаки через интерфейсы управления



Компании с общедоступными интерфейсами управления

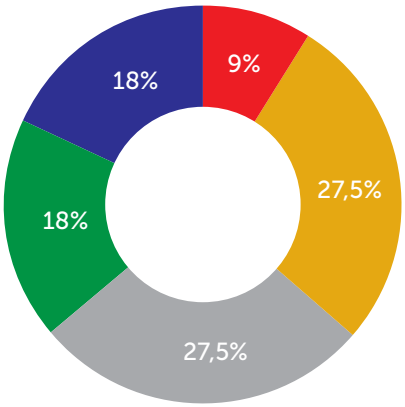
Компании, к ресурсам которых был получен доступ через интерфейсы управления

Несмотря на то, что «Неограниченный сетевой доступ к интерфейсам управления» сам по себе не является уязвимостью и является лишь недостатком конфигурации, данный недостаток использовался в половине всех векторов атак, реализованных в 2017 году в рамках внешних тестирований на проникновение. Доступ к информационным ресурсам 57% компаний был получен через интерфейсы управления.

Наиболее часто для получения доступа через интерфейсы управления использовались пароли, полученные в результате:

- **Эксплуатации других уязвимостей атакуемого узла (27,5%).** Например, эксплуатация уязвимости веб-приложения «Чтение произвольных файлов» позволила получить пароль в открытом виде из конфигурационного файла веб-приложения.
- **Использование паролей по умолчанию для веб-приложений, CMS-систем, сетевого оборудования и т.д. (27,5%).** Необходимые учётные данные для доступа могут быть получены нарушителем из документации.
- **Проведения онлайн-атаки подбора пароля (18%).** Отсутствие защиты от проведения подобных атак и механизмов их детектирования существенно повышают шансы нарушителя подобрать правильный пароль.
- **Компрометации других узлов (18%).** Использование одинаковых паролей для разных систем расширяют потенциальную поверхность атаки.

Получение доступа через интерфейсы управления



Эксплуатация известных уязвимостей ПО интерфейса управления (устаревшее ПО)

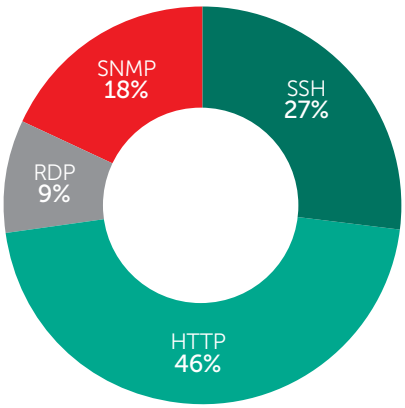
Пароль получен через другую уязвимость

Учетная запись по умолчанию

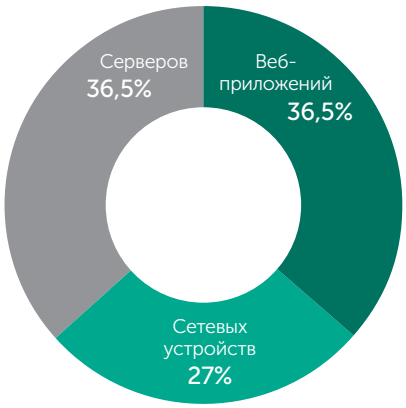
Пароль получен с другого узла

Подбор учетной записи

Интерфейсы управления через которые был получен доступ



Интерфейсы управления



Рекомендация:

Регулярно проводить аудит всех систем, включая веб-приложения, CMS-системы и сетевое оборудование, на предмет использования учётных записей по умолчанию. Установить сложные пароли для административных учётных записей. Использовать разные учётные записи для разных систем. Обновить ПО до последней версии.

Наиболее часто компании забывают ограничить сетевой доступ к веб-интерфейсам удаленного управления и службе SSH. Большинство веб-интерфейсов управления являются административными панелями веб-приложений, CMS-систем. Доступ к административной панели приложения, в большинстве случаев позволил получить полный контроль не только над веб-приложением, но также получить доступ к ОС. При получении доступа в административную панель веб-приложения доступ на выполнение команд ОС может быть получен через возможность загрузки произвольных файлов или редактирование страниц веб-приложения. В некоторых случаях командный интерпретатор является встроенной функцией административной панели веб-приложения.

Рекомендация:

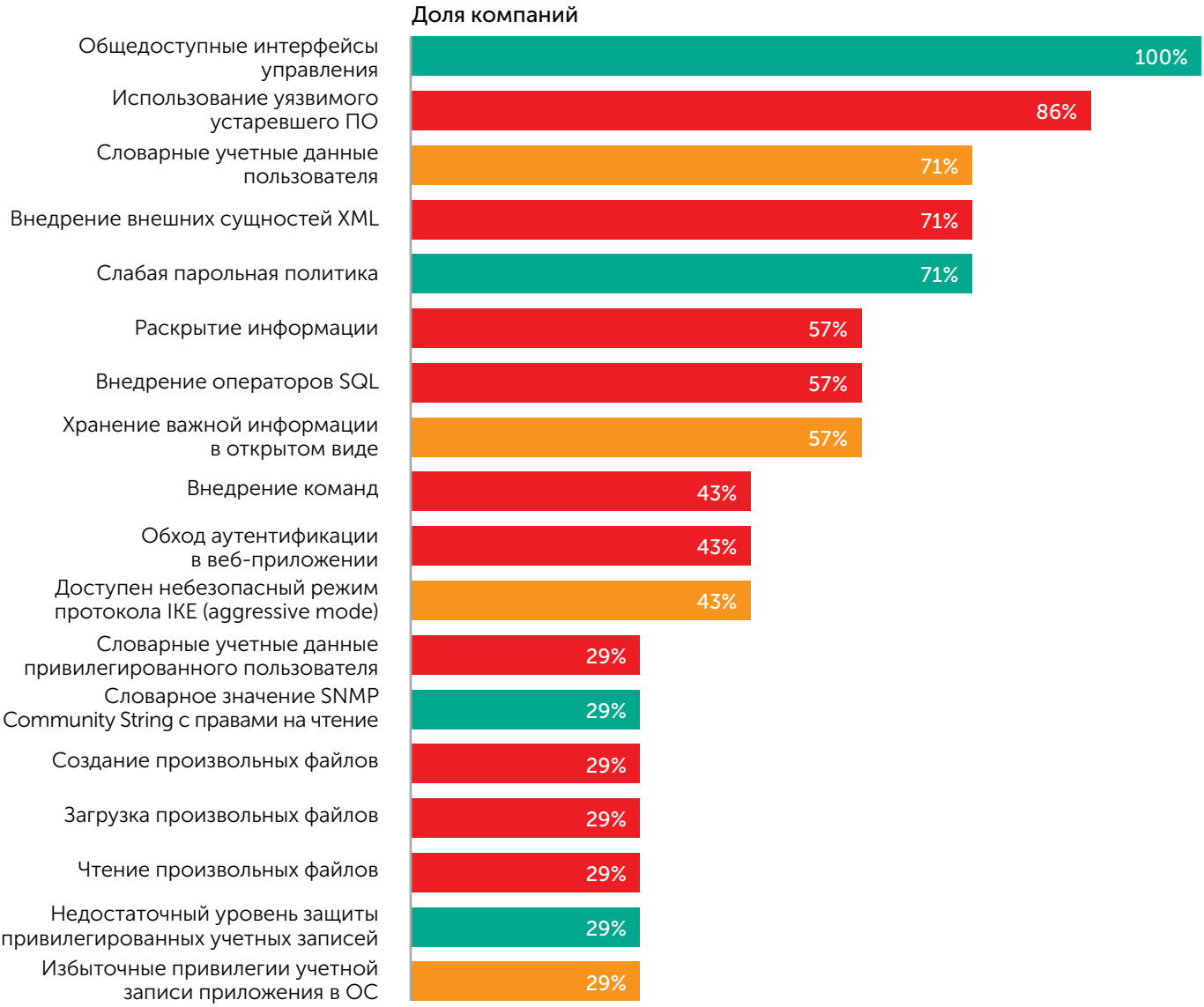
Ограничить сетевой доступ ко всем интерфейсам управления (включая веб-интерфейсы). Доступ должен быть разрешен только с ограниченного количества IP-адресов. Использовать VPN для удаленного доступа.

Пример атаки через интерфейсы управления

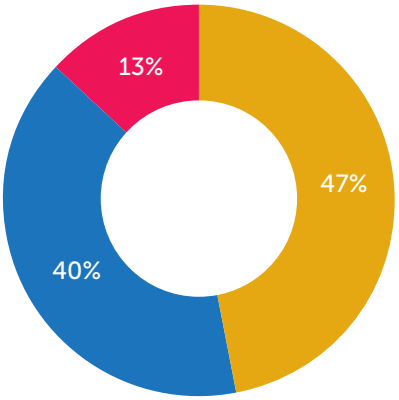
Шаг 1	Обнаружена служба SNMP с учётной записью по умолчанию с правами на чтение
Шаг 2	Через протокол SNMP было обнаружено, что используется устаревшая, уязвимая версия Cisco IOS. Уязвимость: cisco-sa-20170629-snmp. (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp). Уязвимость позволяет атакующему с учётной записью SNMP с правами на чтение получить доступ к устройству с максимальными привилегиями. На базе опубликованной Cisco общей информации об уязвимости, старший специалист по тестированию на проникновение Лаборатории Касперского Артем Кондратенко разработал соответствующий эксплойт (https://github.com/artkond/cisco-snmp-rce), позволяющий продемонстрировать атаку на практике.
Шаг 3	Эксплуатация уязвимости в ADSL-LINE-MIB, получение доступа к маршрутизатору с максимальными привилегиями, что позволило получить доступ к ресурсам внутренней сети заказчика. Технические детали, связанные с эксплуатацией данной уязвимости доступны по ссылке: https://kas.pr/3whh

Статистика наиболее распространённых уязвимостей и недостатков защиты

Наиболее распространённые уязвимости и недостатки защиты



Анализ защищённости со стороны внутренних нарушителей



Финансы и банки
Государственные организации
Промышленность

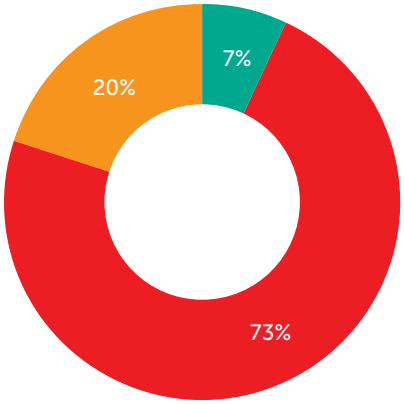
Уровень защищённости оценивался по следующей шкале:

- **Крайне низкий**
- **Низкий**
- **Ниже среднего**
- **Средний**
- **Выше среднего**
- **Высокий**

Итоговый уровень защищённости оценивался на основе собственной методики «Лаборатории Касперского», учитывающей полученный уровень доступа, степень критичности информационных ресурсов, сложность получения доступа, а также требуемые временные затраты.

Крайне низкому уровню защищённости соответствует случай, когда удалось получить полный контроль над ключевыми компонентами ИТ-инфраструктуры заказчика (максимальные привилегии во внутренней сети, полный контроль над ключевыми бизнес-системами, доступ к критически важной информации). Более того, получение указанного доступа не требует высокой квалификации и больших временных затрат.

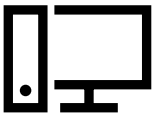
Высокий уровень защищённости соответствует случаю, когда в процессе тестирования на проникновение были выявлены только незначительные уязвимости ресурсов внутренней сети (эксплуатация которых не несет существенных рисков ИБ).



Выше среднего
Крайне низкий
Низкий

Максимальные привилегии в домене Active Directory (привилегии Администратора Домена или Администратора Предприятия) были получены в 86% проектов, где присутствовала доменная инфраструктура. В 64% компаний было выявлено более одного вектора получения наивысших привилегий. В среднем было обнаружено 2-3 вектора получения максимальных привилегий в каждом проведенном проекте. При подсчете векторов атак учитывались только векторы, которые были продемонстрированы на практике в рамках услуги по внутреннему тестированию на проникновение. В целом же, для большинства проектов с помощью специализированных инструментов, таких как bloodhound, обнаруживалось множество других потенциальных векторов атак.

Права администратора получены в 86% анализируемых компаний



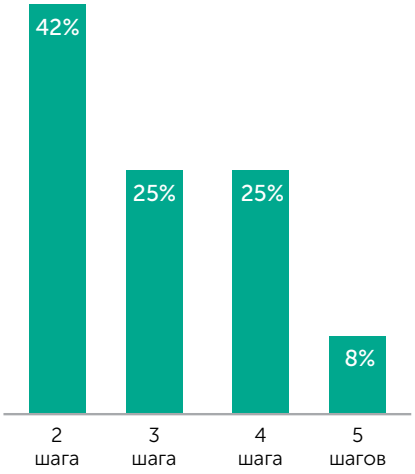
АУДИТОР

В среднем 2-3 вектора
в каждой компании

В среднем 3 шага в векторе

АДМИНИСТРАТОР ДОМЕНА/ АДМИНИСТРАТОР ПРЕДПРИЯТИЯ

Минимальное количество шагов для получения прав администратора домена



Реализованные векторы различались по уровню сложности и количеству шагов (от 2 до 6 шагов). Для получения прав доменного администратора в каждой компании требовалось в среднем 3 шага.

Примеры наиболее простых векторов получения прав администратора домена:

- Проведение атаки NTLM Relay совместно с NBNS Spoofing, позволяющей перехватить NetNTLM-хэш администратора и использовать его для аутентификации на контроллере домена.
- Эксплуатация уязвимости CVE-2011-0923 в HP Data Protector и последующее извлечение пароля доменного администратора из памяти процесса lsass.exe.

Ниже приведен пример более сложного вектора для получения прав администратора домена через эксплуатацию уязвимостей:

- Использование устаревших версий прошивок сетевого оборудования с известными уязвимостями.
- Использование слабых паролей.
- Повторное использование одних и тех же паролей для разных систем и пользователей.
- Использование протокола NBNS.
- Избыточные привилегии учётной записи с SPN.

Пример получения прав администратора домена

ШАГ 1
Эксплуатация уязвимости в веб-сервисе сетевого хранилища D-Link, позволяющая выполнить произвольный код с правами суперпользователя. Создание SSH туннеля для получения доступа в сеть управления (доступ напрямую в которую ограничен правилами межсетевого экранирования). Уязвимость: «Устаревшее ПО (D-Link)»

ШАГ 2
Обнаружен коммутатор Cisco с доступной службой SNMP и учётной записью по умолчанию «public». Через протокол SNMP была определена версия Cisco IOS. Уязвимость: «Пароль по умолчанию SNMP»

ШАГ 3
По версии Cisco IOS определены её уязвимости. Эксплуатация уязвимости CVE-2017-3881. Получение доступа к командному интерпретатору с максимальными правами. Уязвимость: «Устаревшее ПО (Cisco IOS)»

ШАГ 4
Получение из конфигурационного файла хэш-значения пароля локальной учётной записи.

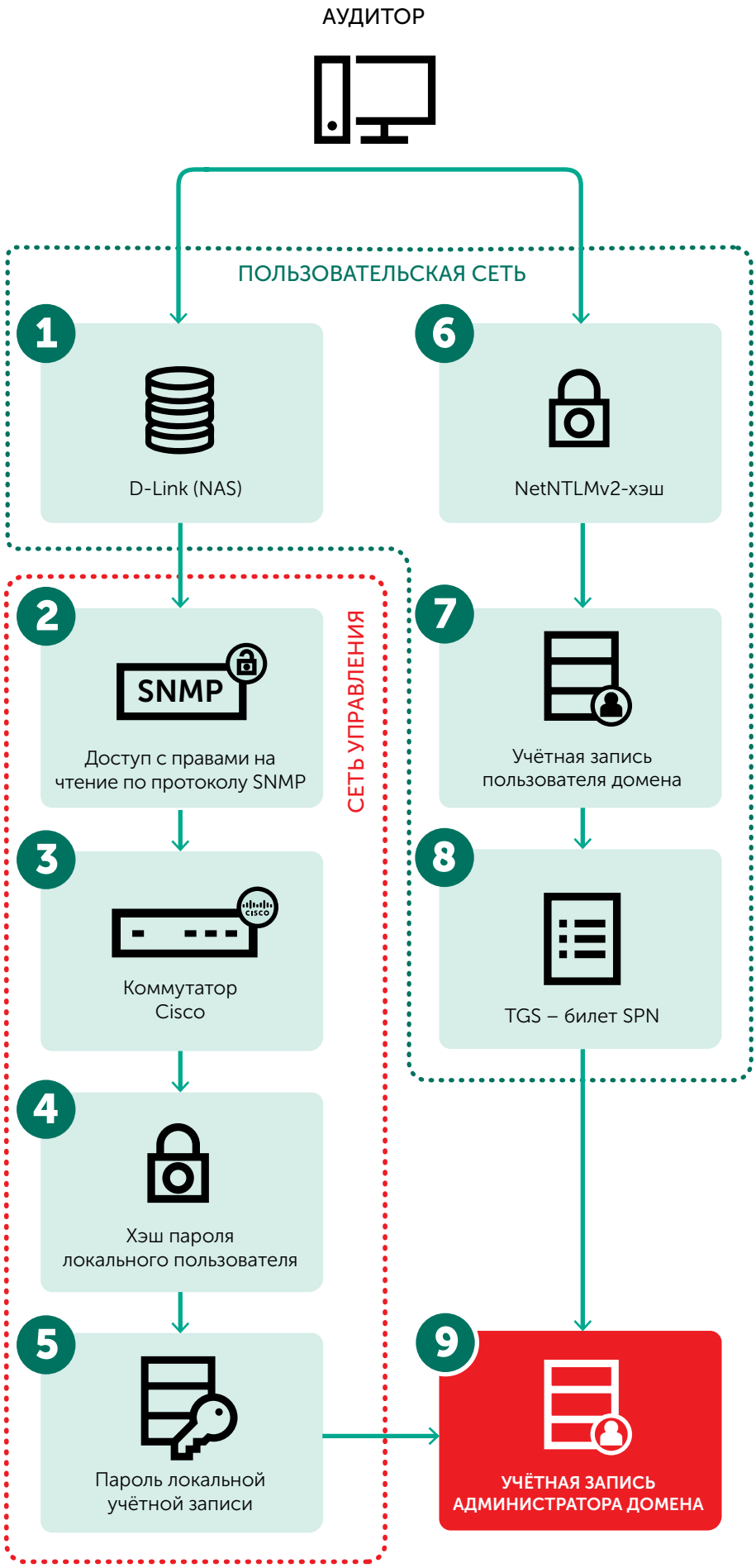
ШАГ 5
Офлайн-атака подбора пароля. Уязвимость: «Слабый пароль привилегированного пользователя»

ШАГ 6
Проведение атаки NBNS Spoofing, перехват NetNTLMv2-хэша. Уязвимость: «Использование протокола NBNS»

ШАГ 7
Офлайн-атака на NetNTLMv2-хэш. Уязвимость: «Слабый пароль учётной записи пользователя»

ШАГ 8
Использование учетной записи пользователя домена для проведения атаки Kerberoasting. Получение TGS-билета SPN.

ШАГ 9
Офлайн-атака подбора пароля к TGS-билету. Пароль локальной учетной записи коммутатора Cisco совпадал с паролем учётной записи с SPN. Уязвимость: «Повторное использование пароля», «Избыточные права учётной записи»



Об уязвимости CVE-2017-3881 (Удаленное выполнение кода в Cisco IOS)

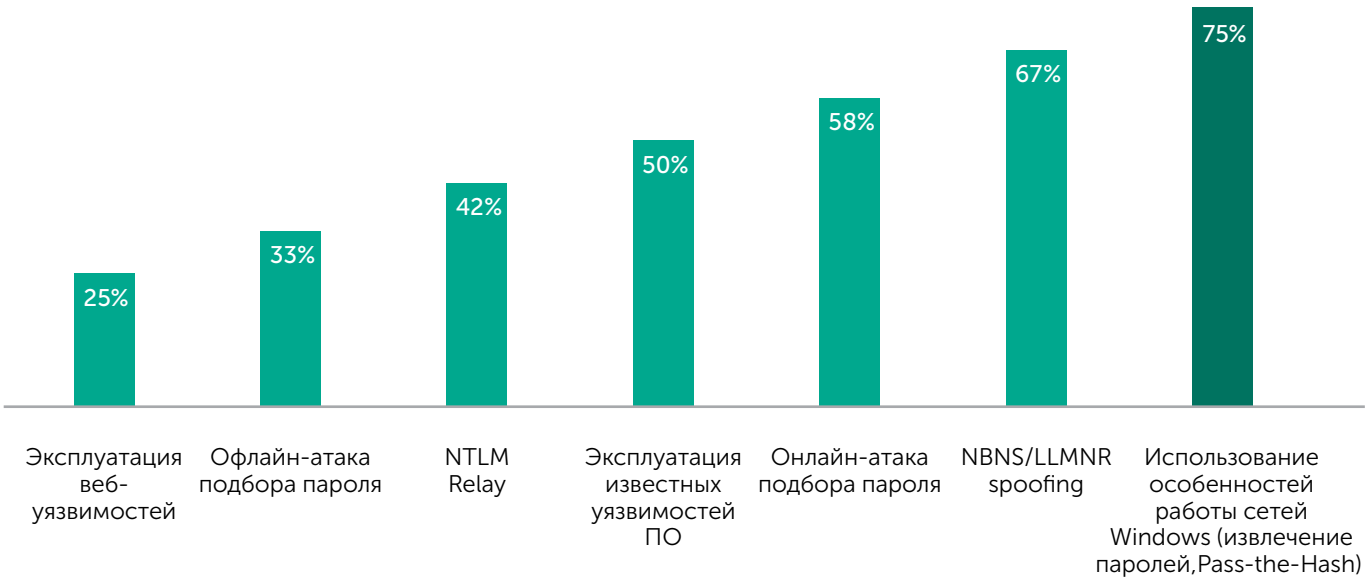
Упоминание о данной уязвимости было обнаружено в документах ЦРУ Vault 7: CIA, опубликованных на ресурсе WikiLeaks в марте 2017 года. Уязвимость имела кодовое название ROCEM и описание её технических деталей почти отсутствовало. Позже этой уязвимости были присвоены идентификаторы CVE-2017-3881 и cisco-sa-20170317-cmp. Уязвимость позволяет неавторизованному атакующему через протокол Telnet выполнить произвольный код в системе Cisco IOS с максимальными привилегиями. В документе ЦРУ были описаны только некоторые детали, связанные с процессом тестирования, необходимым для разработки эксплойта, но исходные коды самого эксплойта отсутствовали. Тем не менее, на базе полученной информации эксперту «Лаборатории Касперского» Артему Кондратенко удалось провести исследование в лабораторных условиях и воссоздать эксплойт для этой критической уязвимости.

Подробное описание процесса разработки эксплойта под данную уязвимость доступно по ссылкам: https://kas.pr/fk8g, https://kas.pr/amv7.

Наиболее часто используемые атаки и техники

При анализе атак и техник, используемых для получения максимальных привилегий в домене Active Directory, были получены следующие результаты:

Доля компаний, в которых успешно применялись различные атаки и техники для получения максимальных привилегий в домене Active Directory



Атака NBNS/LLMNR Spoofing

В 67% компаний применялась для получения максимальных привилегий

87% компаний уязвимы

Использование протоколов NBNS и LLMNR было обнаружено в 87% анализируемых компаний. В 67% компаний, в которых были получены максимальные привилегии в домене Active Directory, применялась атака NBNS/LLMNR Spoofing, позволяющая перехватывать пользовательские данные, в том числе NetNTLMv2-хэши пользователей. Данный хэш может быть использован для проведения атаки NTLM Relay или для проведения атаки методом перебора по словарю.

Рекомендации по защите:

Рекомендуется отключить протоколы NBNS и LLMNR.

Рекомендации по детектированию:

Использовать в сети honeypot, рассылающие по сети широковещательные NBNS/LLMNR запросы с несуществующими именами компьютеров. Получение ответов к отправляемым запросам свидетельствует о наличии нарушителя в сети. Примеры: https://blog.netspi.com/identifying-rogue-nbns-spoofers/, https://github.com/Kevin-Robertson/Conveigh. При наличии доступа к копии всего сетевого трафика следует обратить внимание на множественные LLMNR/NBNS ответы, исходящие с одного IP-адреса в ответ на запросы с разными именами компьютеров.

Атака NTLM Relay

В 42% компаний применялась для получения максимальных привилегий

47% компаний уязвимы

В половине случаев успешного проведения атаки NBNS/LLMNR spoofing перехваченные NetNTLMv2-хэши использовались для атаки NTLM Relay. Если в ходе атаки NBNS/LLMNR Spoofing был перехвачен NetNTLMv2-хэш учётной записи администратора домена, то атака NTLM Relay позволяет быстро получить максимальные привилегии в Active Directory.

Атака NTLM Relay (совместно с NBNS/LLMNR Spoofing) использовалась для получения максимальных привилегий в домене Active Directory в 42% анализируемых компаний. Отсутствие защиты от данного типа атак было обнаружено у 47% анализируемых компаний.

Рекомендации по защите:

Наиболее эффективным методом защиты от данной атаки является блокировка аутентификации через протокол NTLM. Недостатком данного подхода является сложность его реализации.

Для защиты от атаки NTLM relay может использоваться Extended Protocol for Authentication (EPA).

В качестве защитного механизма может также использоваться включение подписывания в протоколе SMB в настройках групповых политик. Стоит отметить, что данный подход обеспечивает защиту только от атак NTLM relay направленных на протокол SMB.

Рекомендации по детектированию:

Индикатором атаки может служить событие сетевого входа (событие 4624 с Logon Type 3), в котором IP-адрес из поля «Source Network Address» не соответствует имени узла-источника «Workstation Name». На данном этапе требуется таблица соответствия имен компьютеров и их IP-адресов (может применяться интеграция с DNS).

Другим подходом для выявления данной атаки может быть выявление сетевых входов с нетипичных IP-адресов. Для каждого узла сети необходимо собрать статистику IP-адресов, с которых наиболее часто осуществляются входы в систему. Сетевой вход с нетипичного IP-адреса может свидетельствовать о возможной атаке. Недостатком данного подхода является большое число ложных срабатываний.

Эксплуатация известных уязвимостей в устаревшем ПО

В 75% компаний обнаружена уязвимость MS17-010

Эксплуатация известных уязвимостей в устаревшем ПО использовалась в трети всех реализованных векторов.

Большинство эксплуатируемых уязвимостей обнаружены в 2017 году:

- Удаленное выполнение кода в Cisco IOS (CVE-2017-3881);
- Удаленное выполнение кода в VMware vCenter (CVE-2017-5638);
- Удаленное выполнение кода в Samba (CVE-2017-7494 - Samba Cry);
- Удаленное выполнение кода в Windows SMB (MS17-010).

Наличие эксплойтов в открытом доступе для многих уязвимостей существенно упрощало задачу эксплуатации уязвимостей (MS17-010, Samba Cry, VMware vCenter CVE-2017-5638).

Распространённой атакой во внутренней сети было удаленное выполнение кода через сетевую службу Java RMI и десериализацию Java-класса в библиотеках Apache Common Collections (ACC), использующуюся в различных продуктах (например, Cisco Lan Management Solution). В целом, атаки на десериализацию, актуальные для множества программных продуктов, используемых крупными компаниями, позволяли быстро получать максимальные привилегии на критически важных серверах инфраструктуры.

Уязвимости ОС Windows последних лет использовались для удаленного выполнения кода (MS17-010 Eternal Blue) и локального повышения привилегий в системе (MS16-075 Rotten Potato). Нашумевшая уязвимость MS17-010 была обнаружена в 60% всех компаний и в 75% компаний, тестирование на проникновение которых проводилось после публикации информации об уязвимости.

Стоит отметь, что уязвимость MS17-010 была обнаружена, как у компаний, тестирование которых проводилось в конце первого и во втором квартале 2017 года (обнаружение уязвимостей было предсказуемым в связи с недавним выходом обновления), так и у компаний, тестирование которых проводилось в четвёртом квартале 2017 года, что свидетельствует о недостаточной эффективности процессов управления обновлениями/уязвимостями и о рисках заражения вредоносным ПО, таким как WannaCry.

Рекомендации по защите:

Мониторинг обнаружения новых уязвимостей в ПО и своевременное обновление ПО. Использование решений класса Endpoint Protection со встроенным модулем IDS/IPS.

Рекомендации по детектированию:

Для выявления попыток эксплуатации уязвимостей ПО рекомендуется обратить внимание на следующие события:

- Срабатывания модуля IDS/IPS в решениях класса Endpoint Protection.
- Порождение нетипичных процессов процессами серверных приложений (веб-сервер Apache запускает bash, MS SQL запускает PowerShell). Для реализации данного подхода необходимо с конечных узлов собирать события запуска процессов, при этом эти события должны содержать информацию как о запущенном процессе, так и о его родительском процессе. Такие события можно получать от коммерческих EDR-решений, от бесплатного Sysmon или от штатного журнала аудита Windows, начиная с Windows 10/ Windows 2016 (в этих версиях в событии запуска процесса 4688 была добавлена информация о родительском процессе, в более старых версиях необходимо реализовывать корреляцию PID-процессов).
- Некорректное завершение работы клиентского и серверного ПО, наиболее подверженного эксплуатации уязвимостей. При использовании данного подхода будет обнаруживаться большое число ложных срабатываний.

Онлайн-атаки подбора паролей

В 58% компаний применялись для получения максимальных привилегий

Наиболее часто онлайн-атаки подбора пароля использовались для получения доступа к учётным записям пользователей Windows и учётным записям администраторов веб-приложений.

Правила парольных политик позволяют пользователям выбирать предсказуемые и легко угадываемые пароли. К таким паролям относятся: p@SSword1, <Company_name>123 и др.

Успешному проведению атак подбора пароля к интерфейсам управления способствовало использование паролей по умолчанию, а также повторное использование одних и тех же паролей для разных учётных записей.

Рекомендации по защите:

Внедрение строгой парольной политики для всех используемых систем (учётные записи пользователей, сервисные учётные записи, административные учётные записи веб-приложений, сетевого оборудования и др.).

Повышение осведомленности пользователей в области парольной защиты: выбор сложных паролей, использование разных паролей для разных систем и учётных записей.

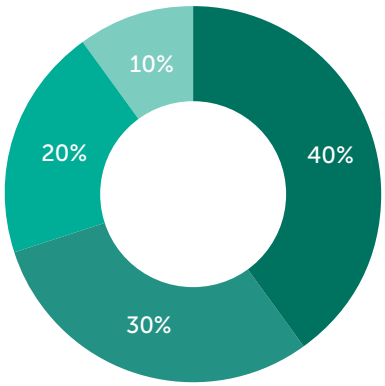
Аудит всех систем, включая веб-приложения, CMS-системы и сетевое оборудование, на предмет использования учётных записей по умолчанию.

Рекомендации по детектированию:

Для детектирования атак подбора пароля учётных записей Windows необходимо обратить внимание на:

- множественные события 4625 на конечных узлах (при подборе пароля локальных и доменных учётных записей);
- множественные события 4771 на контроллере домена (при подборе пароля доменной учётной записи с использованием Kerberos);
- множественные события 4776 на контроллере домена (при подборе пароля доменной учётной записи с использованием NTLM).

Офлайн-атаки подбора паролей



Офлайн-атаки подбора паролей проводились:

- на NTLM-хэши извлеченные из хранилища SAM;
- на NTLMv2-хэши, перехваченные в результате атак NBNS/LLMNR Spoofing;
- для атаки Kerberoasting (см. далее);
- на хэши, полученные из других систем.

Kerberoasting

В 20% компаний учётные записи с SPN со слабыми паролями

Атака заключается в подборе пароля учётной записи с SPN (Service Principal Name), с помощью которого был зашифрован TGS билет Kerberos. Для проведения атаки необходимо лишь обладать правами пользователя домена.

Если учётная запись с SPN обладает правами администратора домена, то при успешном подборе пароля атакующий получает учётную запись с максимальными правами в домене Active Directory. В 20% всех анализируемых компаний были обнаружены учётные записи с SPN со слабыми паролями. В 13% всех компаний (17% компаний, в которых были получены права администратора домена) с помощью атаки Kerberoasting были получены права администратора домена.

Рекомендации по защите:

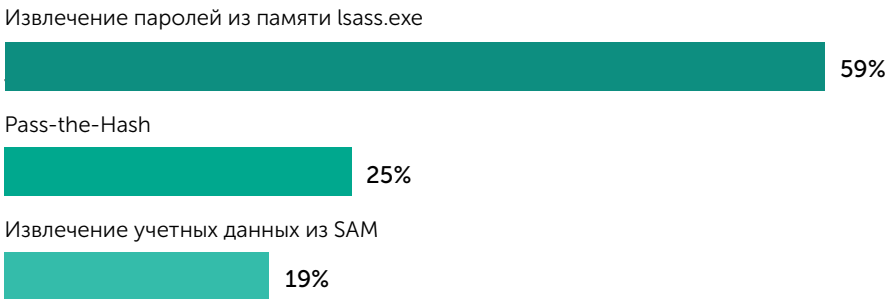
Установить сложный пароль для учётной записи с SPN (не менее 20 символов). Следовать принципу наименьших привилегий для сервисных учётных записей.

Рекомендации по детектированию:

Мониторинг запросов TGS билетов с шифрованием RC4 (событие 4769 с типом 0x17). Большое количество запросов TGS билетов для разных SPN в короткий промежуток времени свидетельствует об атаке.

При проведении тестирований на проникновение специалистами «Лаборатории Касперского» также использовался ряд особенностей работы сетей Windows, которые сами по себе не являются уязвимостями, но предоставляют большое поле для т.н. «горизонтальных перемещений» («lateral movement») и дальнейшего развития атаки. Наиболее активно использовались: извлечение паролей пользователей и хэш-значений из памяти процесса lsass.exe, проведение атаки Pass-the-Hash, извлечение хэш-значений из базы SAM.

Доля векторов, в которых использовалась данная техника



Извлечение паролей в открытом виде из памяти процесса lsass.exe

59%
реализованных векторов

Получение паролей возможно из-за слабости реализации Single Sign-On (SSO) в системах Windows: некоторые подсистемы хранят пароли в памяти ОС с использованием обратимого кодирования. Таким образом, привилегированный пользователь ОС способен получить доступ к паролям всех пользователей, совершивших вход в систему и не завершивших корректно сессию (log out).

Рекомендации по снижению риска:

- Следовать принципу наименьших привилегий во всех системах. Кроме того, по возможности рекомендуется отказаться от использования учётных записей локальных администраторов в доменной среде. Следовать уровневой модели Microsoft для привилегированных учётных записей для снижения рисков компрометации;
- Использовать Credential Guard (данный защитный механизм появился, начиная с Windows 10 / Windows Server 2016);
- Использовать Authentication Policies and Authentication Policy Silos ;
- Запретить сетевой вход для учётных записей локальных администраторов или всех членов группы «Local account and member of Administrators group» (данная группа появилась в Windows 8.1 / Windows Server2012R2, а также в Windows 7/ Windows 8/ Windows Server2008R2 с обновлением KB 2871997);
- Использовать "Restricted Admin RDP" вместо использования обычного RDP. Стоит отметить, что данная мера понижает риск извлечения пароля в открытом виде, но повышает риск несанкционированного RDP-подключения с использованием хэш-значения (атака Pass-the Hash). Использование данной меры рекомендуется только при соблюдении комплексного подхода и принятия мер по защите от атак Pass-the-Hash;
- Использовать группу Protected Users для привилегированных учётных записей, члены которой могут авторизоваться только через протокол Kerberos (перечень всех защитных механизмов данной группы доступен на сайте Microsoft);
- Включить защиту LSA от подключения сторонних модулей;
- Запретить хранение WDigest в памяти или полностью отключить использование метода аутентификации WDigest (применимо к ОС, начиная с Windows 8.1/ Windows Server 2012 R2 или Windows 7/Windows Server 2008 с обновлением безопасности KB2871997);
- Отключить использование привилегии SeDebugPrivilege в настройках доменных политик;
- Отключить функцию Automatic Restart Sign-On (ARSO).
- При использовании привилегированных учётных записей для удаленного доступа (в частности, по RDP) корректно завершать сессию (через выход пользователя из системы).
- Установить в GPO завершение сессий RDP: Computer Configuration\Policies\ Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits. Включить использование SACL для регистрации процессов, пытающихся получить доступ к lsass.exe
- Использовать антивирусное ПО.

Перечень указанных мер не является гарантированным защитным механизмом, но может быть использован для обнаружения атак в сети, а также снижения рисков успешного проведения атаки (в том числе атак проводимых автоматизировано с использованием вредоносного ПО, например, NotPetya/ExPetr).

Рекомендации по детектированию:

Способы обнаружения попыток извлечения паролей из памяти процесса lsass.exe сильно различаются от используемого атакующим подхода и выходит за рамки данной публикации. Подробная информация доступна по ссылке: https://kas.pr/16a7.

Также рекомендуется обратить особое внимание на методы обнаружения извлечения учётных записей с помощью PowerShell (Invoke-Mimikatz).

Атака Pass-the Hash

25%
реализованных
векторов

Атака заключается в использовании NTLM-хэшей, полученных из базы SAM или из памяти процесса lsass.exe для аутентификации на удаленном ресурсе, без использования пароля учётной записи.

Атака успешно применялась в 25% векторов, которые приходятся на 28% анализируемых компаний.

Рекомендации по снижению риска:

Наиболее эффективным методом защиты от данного типа атак является запрет использования в сети протокола NTLM.

Использование LAPS (Local Administrator Password Solution) для управления паролями локальных администраторов.

Запретить сетевой вход для учётных записей локальных администраторов или всех членов группы «Local account and member of Administrators group» (данная группа появилась, в Windows 8.1/ Windows Server 2012R2, а также в Windows 7/ Windows 8/ Windows Server 2008R2 с обновлением KB 2871997).

Следовать принципу наименьших привилегий во всех системах. Следовать уровневой модели Microsoft для привилегированных учётных записей для снижения рисков компрометации.

Рекомендации по детектированию:

Наиболее эффективно данная атака может быть обнаружена в хорошо сегментированной сети, в которой определены строгие правила использования привилегированных учётных записей.

Рекомендуется определить перечень учётных записей, на которые могут быть направлены атаки. В данный перечень должны входить не только высоко привилегированные учётные записи, но и все учётные записи, которые могут быть использованы для доступа к критически важным ресурсам организации.

При построении стратегии детектирования атаки Pass-the Hash стоит учесть нетипичные события сетевого входа, связанные с:

- IP-адресом источника и IP-адресом целевого ресурса;
- Временным моментом аутентификации (рабочее время, даты отпусков);
- Также рекомендуется обратить внимание на нетипичные события, связанные с:
  - Учётными записями (создание учётной записи, изменение настроек учётных записей, попытки использования запрещенных методов аутентификации);
  - Одновременным использованием нескольких учётных записей (попытки аутентификации под разными учётными записями с одного компьютера, использование различных учётных записей для VPN-подключения и учётной записи для доступа к ресурсам);

Многие инструменты, используемые для проведения атаки Pass-the-Hash, генерируют имя рабочей станции случайным образом. Это можно детектировать по событиям 4624, в которых Workstation Name представляет собой случайную комбинацию символов.

Извлечение учётных данных из SAM

19%
реализованных
векторов

NTLM-хэши локальных учётных записей, извлеченные из хранилища SAM ОС Windows, использовались для офлайн-атаки подбора пароля либо проведения атаки Pass-the-Hash.

Рекомендации по детектированию:

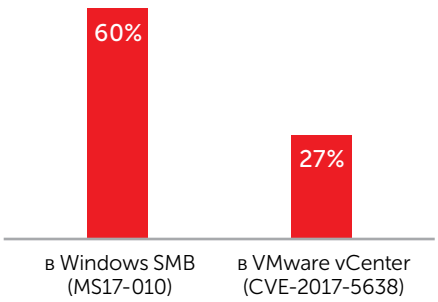
Методы обнаружения попыток извлечения SAM-таблицы зависят от способа, который использует атакующий: прямой доступ к логическому тому, Shadow Copy, reg.exe, удаленный реестр и др.

Подробная информация по обнаружению атак типа «Извлечения учётных данных» доступна по ссылке: https://kas.pr/16a7.

Статистика наиболее распространённых уязвимостей и недостатков защиты

Наиболее распространённые уязвимости и недостатки защиты

* Удалённое выполнение кода:



Недостаточное межсетевое экранирование было выявлено у всех анализируемых компаний. Из пользовательских сегментов были доступны интерфейсы управления (SSH, Telnet, SNMP, интерфейсы управления веб-приложений), а также интерфейсы доступа к СУБД. Использование слабых паролей, а также повторное использование одних и тех же паролей для разных учётных записей упрощало задачу подбора паролей к учётным записям пользователей и интерфейсам управления.

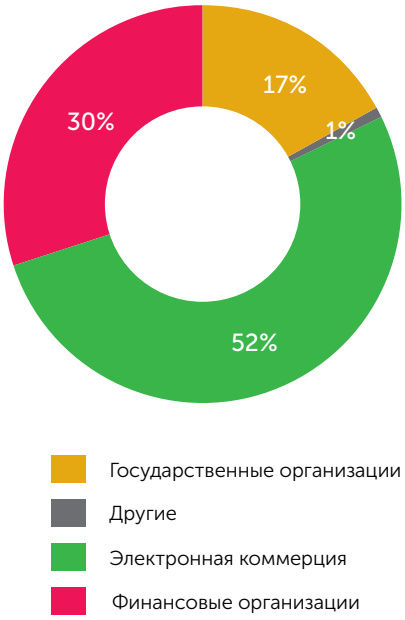
В случае наличия избыточных прав у учётной записи приложения в ОС эксплуатация уязвимостей данного приложения позволяла получить максимальные права на соответствующем узле и это существенно упрощало развитие дальнейшей атаки.

Анализ защищённости веб-приложений

Для расчёта статистики учитывались результаты анализа защищённости для крупных российских и зарубежных компаний. Из всех приложений 52% относится к сфере электронной коммерции.

По данным анализа за 2017 год наиболее уязвимыми являются приложения государственных учреждений, во всех приложениях были найдены уязвимости высокого уровня риска. В приложениях сферы электронной коммерции уязвимости высокого уровня риска занимают наименьшую долю – 26% . В категории «Другие» находится одно приложение, поэтому эта категория не учитывалась в расчете статистики по отраслям.

Доля анализируемых приложений по отраслям



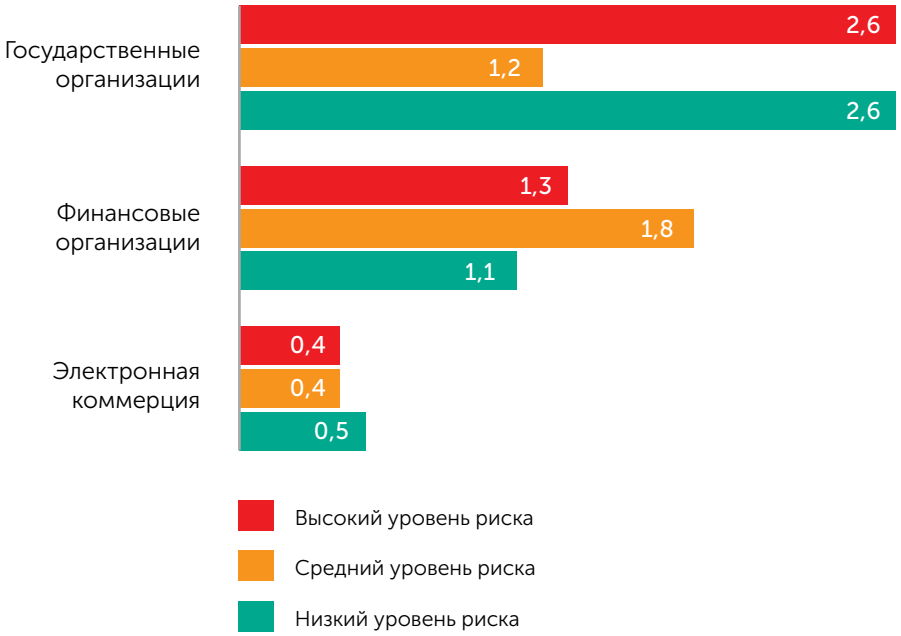
Доля приложений с уязвимостями различного уровня риска

Для каждого приложения был выставлен итоговый уровень риска, исходя из максимального уровня риска уязвимостей, найденных в приложении. Приложения, используемые в сфере электронной коммерции, оказались наиболее защищёнными, только 28% всех приложений содержат уязвимости высокого уровня риска, а для 36% приложений были найдены уязвимости максимум среднего уровня риска.

Доля уязвимых сайтов по максимальному уровню риска

Если сравнивать среднее количество уязвимостей на приложение, то рейтинг отраслей сохраняется: наибольшее среднее количество уязвимостей на приложение было найдено на сайтах государственных организаций, на втором месте финансовые организации и за ними следует отрасль электронной коммерции.

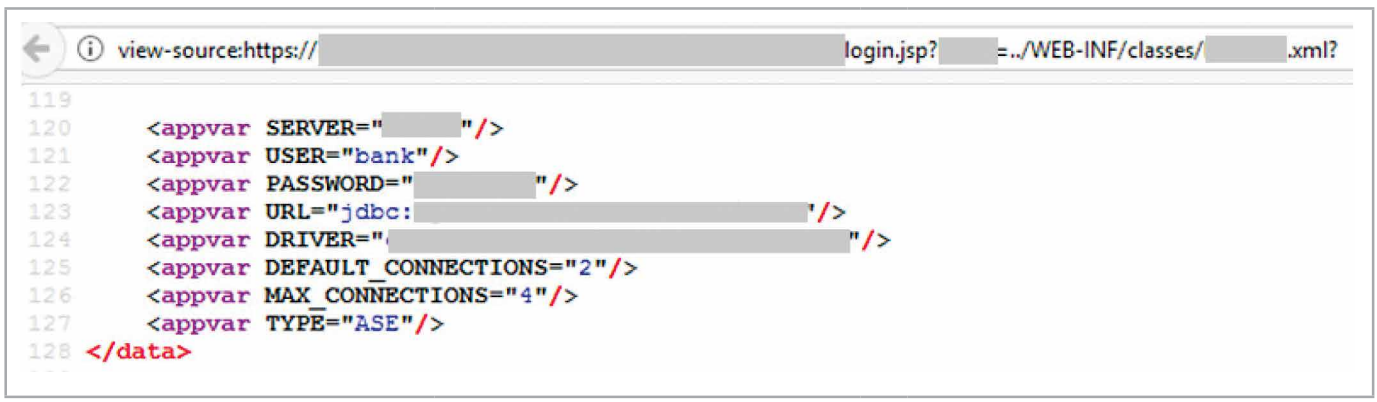
Среднее количество уязвимостей на одно приложение



В 2017 году наибольшее количество приложений было подвержено следующим уязвимостям высокого уровня риска:

- Раскрытие чувствительных данных(Sensitive Data Exposure, по классификации OWASP): исходный код веб-приложения, конфигурационные файлы, файлы журнала событий и др.,

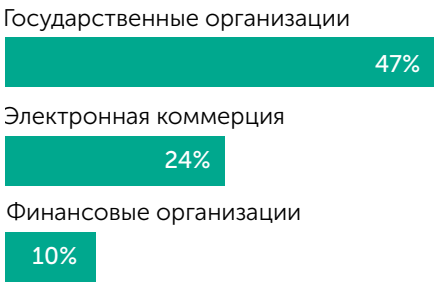
- Непроверенные переадресации и пересылки (Unvalidated Redirects and Forwards, по классификации OWASP). Как правило, данная уязвимость имеет средний уровень риска и используется для проведения фишинговых атак или распространения вредоносного ПО. В 2017 году специалисты «Лаборатории Касперского» сталкивались преимущественно с более опасной версией уязвимости класса Unvalidated Forward. Эта уязвимость присутствовала в Java-приложениях и позволяла выходить за пределы назначенного каталога и читать различные файлы на сервере. В частности, можно было получить детальную информацию о пользователях и пароли в открытом виде.



- Словарные учётные данные пользователя (Broken Authentication, по классификации OWASP): словарные учётные данные обнаруживались при онлайн-атаках подбора пароля, при офлайн-атаках подбора пароля к полученному хэш-значению, при анализе исходного кода веб-приложения.

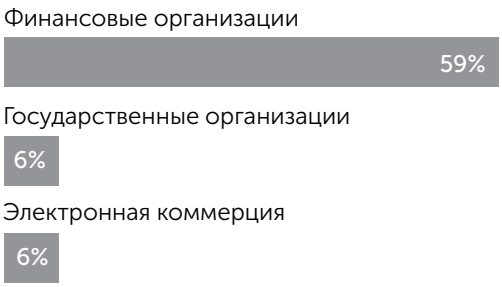
В приложениях всех отраслей было найдено раскрытие чувствительных данных (внутренние IP-адреса и порты для доступа к СУБД, пароли, резервные копии систем и т.д.) **и уязвимость «Словарные учётные данные пользователя»**.

Раскрытие чувствительных данных



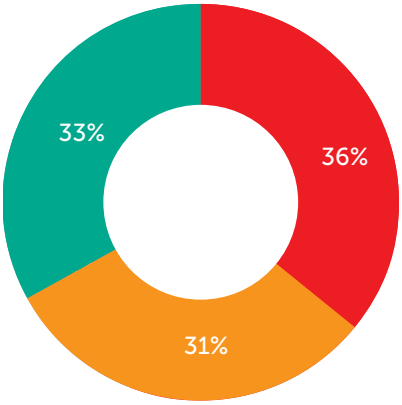
Непроверенные переадресации и пересылки

Словарные учётные данные пользователя



Анализ уязвимостей

Распределение уязвимостей по уровню риска

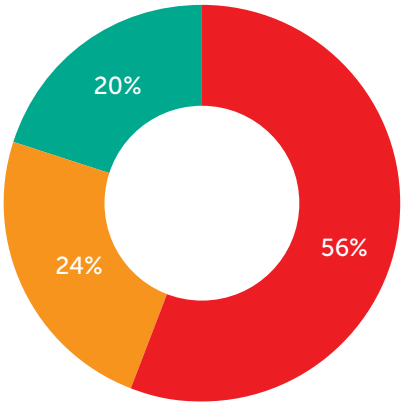


В 2017 году было найдено примерно равное количество уязвимостей высокого, среднего и низкого уровней риска. Однако если рассматривать итоговый уровень риска приложений, то более половины из них (56%) содержат уязвимости высокого уровня риска. Для каждого приложения был выставлен итоговый уровень риска, исходя из максимального уровня риска уязвимостей, найденных в приложении.

Больше половины уязвимостей вызваны ошибками в коде веб-приложений. Среди них наиболее распространена уязвимость «Межсайтовое выполнение сценариев». Недостатки конфигурации стали причиной 44% уязвимостей. Наибольшее количество недостатков конфигурации связано с раскрытием чувствительных данных.

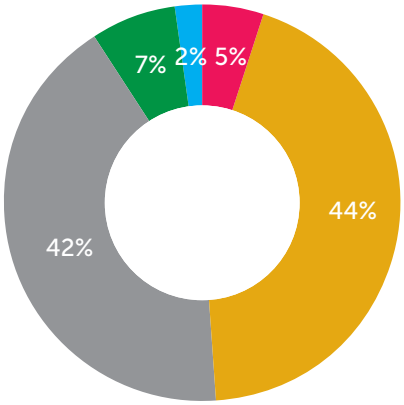
Анализ уязвимостей показал, что большая их часть относится к серверной части приложений. Среди них наиболее распространены «Раскрытие чувствительных данных», «Внедрение операторов SQL» и «Отсутствие контроля доступа на уровне функций». 28% уязвимостей направлены на клиентов приложений, при этом более половины таких уязвимостей – «Межсайтовое выполнение сценариев».

Распределение приложений по уровню риска



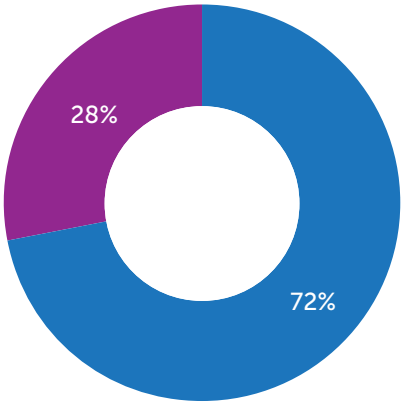
- Высокий уровень риска
- Средний уровень риска
- Низкий уровень риска

Доля уязвимостей разных типов



- Уязвимость в стороннем компоненте ПО (библиотеки, плагины CMS-систем и др.)
- Уязвимость в веб-сервере
- Уязвимость в коде приложения
- Недостаток конфигурации
- Словарный пароль

Доля уязвимостей в серверной и клиентской частях



- Серверная часть
- Клиентская часть

Статистика по общему количеству уязвимостей

В данном разделе приведена общая статистика уязвимостей. Стоит отметить, что в некоторых приложениях было найдено несколько уязвимостей одного типа.

Десять наиболее распространенных уязвимостей

К типу **«Межсайтовое выполнение сценариев»** относятся 20% найденных уязвимостей. Злоумышленник может использовать уязвимость для получения аутентификационных данных пользователей (cookie), фишинга или распространения вредоносного кода.

Уязвимость высокого уровня риска **«Раскрытие чувствительных данных»** находится на втором месте по распространенности. Она позволяет атакующему получить доступ к чувствительным данным приложения или информации пользователей через отладочные сценарии, файлы журналов учёта событий и т.д.

Третьей по распространённости уязвимостью является **«Внедрение операторов SQL»**. Уязвимость заключается в возможности внедрения операторов SQL через данные, вводимые пользователем приложения. При недостаточной проверке данных злоумышленник может изменять логику запросов, отправляемых SQL-серверу, и таким образом получать произвольные данные от SQL-сервера в рамках привилегий веб-приложения.

В ряде приложений отсутствует **Контроль доступа на уровне функций**, таким образом, пользователи могут получать доступ к сценариям приложения и файлам, не предназначенным для назначенной им роли. Например, в одном из приложений любой неавторизованный пользователь имел доступ к странице мониторинга веб-приложения, что могло привести к краже сессий, раскрытию чувствительной информации и нарушению работы сервиса.

Остальные уязвимости приложений одинаково распространены – по 4% от всех найденных уязвимостей:

- **Пользователи используют словарные учётные данные.** Подобрав их, атакующий может получить доступ к уязвимой системе.
- **Непроверенные переадресации и пересылки** позволяют удаленному атакующему перенаправлять пользователей на произвольные веб-сайты и таким образом проводить фишинговые атаки или распространять вредоносное ПО. В некоторых случаях уязвимость может быть использована для получения чувствительной информации (уязвимость класса Unvalidated Forward).
- **Удаленное выполнение произвольного кода** позволяет выполнять любые команды на выбор злоумышленника на целевой системе или в целевом процессе. Как правило, это означает получение полного доступа к исходному коду приложения, конфигурации, доступ к базам данных и возможность дальнейшего развития атаки в сеть.
- При отсутствии надежной защиты от атак **методом перебора** и использовании пользователями словарных учётных данных злоумышленник может получить доступ к системе с правами соответствующего пользователя.
- Многие приложения используют **открытый протокол HTTP** для передачи данных. При успешной реализации атаки типа «человек посередине» злоумышленник может получить чувствительные данные. В частности, если будут перехвачены учётные данные администратора приложения, атакующий получит полный контроль над соответствующими узлами.
- **Раскрытие полного пути** в файловой системе (для веб-каталога или для других объектов системы) упрощает другие атаки, такие как загрузка произвольных файлов, подключение локальных файлов, чтение произвольных файлов.

Статистика по приложениям

В данном разделе приводятся данные о том, насколько распространены уязвимости в приложениях (на диаграмме приведена доля приложений, в которых была выявлена указанная уязвимость).

Доля приложений, в которых были выявлены наиболее распространенные уязвимости

Рекомендации по повышению защищённости веб-приложений

Для снижения уровня рисков, связанных с описанными уязвимостями, рекомендуется реализовать следующие меры:

- Проверять все данные поступающие от пользователей веб-приложения.
- Ограничить доступ к интерфейсам управления, чувствительным данным и директориям.
- Использовать принцип наименьших привилегий и убедиться, что пользователи имеют минимально необходимый набор прав доступа.
- Необходимо установить требования к минимальной длине, сложности и частоте смены пароля. Следует исключить возможность использования словарных комбинаций учётных данных.
- Своевременно устанавливать обновления ПО и используемых компонентов.
- Внедрить средства обнаружения вторжений, рассмотреть возможность использования WAF. Удостовериться, что средства превентивной защиты установлены и функционируют корректно.
- Внедрить процесс безопасной разработки веб-приложений (SSDL).
- Регулярно проводить работы по анализу защищённости ИТ-инфраструктуры, в том числе по анализу защищённости приложений.

Заключение

Итоговый уровень защищённости со стороны внешнего злоумышленника 43% анализируемых компаний был оценен как низкий или крайне низкий: получение привилегированного доступа к важным информационным системам этих организаций возможно за короткое время даже со стороны внешних атакующих, не обладающих высокой квалификацией или какими-либо дополнительными ресурсами помимо публично доступных.

Преодоление внешнего периметра и получение доступа во внутреннюю сеть наиболее часто (73% векторов атак) осуществлялось через эксплуатацию уязвимостей веб-приложений: загрузка произвольных файлов (28%), внедрение операторов SQL (17%) и другие. Другим распространенным вектором преодоления сетевого периметра были различные атаки через общедоступные интерфейсы управления: с использованием учётных записей со слабыми паролями или паролями по умолчанию, либо через эксплуатацию уязвимостей ПО интерфейсов управления. Половину векторов атак можно было предотвратить, ограничив доступ к интерфейсам управления (SSH, RDP, SNMP, веб-интерфейсы администрирования и т.п.).

Уровень защищённости со стороны внутреннего злоумышленника 93% анализируемых компаний был определен как низкий или крайне низкий. Более того, в 64% компаний было выявлено более одного вектора получения наивысших привилегий в ИТ-инфраструктуре: уровень Enterprise Admin в Active Directory, полный контроль над ключевым сетевым оборудованием и важными бизнес-системами. В среднем было обнаружено 2-3 вектора получения максимальных привилегий в каждом проведенном проекте, при этом д**ля получения прав доменного администратора в каждой компании в среднем было достаточно лишь 3 шагов.**

Для развития атаки во внутренней сети использовались как давно известные атаки, такие как NBNS Spoofing и NTLM Relay, так и атаки, связанные с эксплуатацией уязвимостей, обнаруженных в 2017 году: MS17-010 (Windows SMB), CVE-2017-7494 (Samba), CVE-2017-5638 (VMware vCenter). Уязвимость MS17-010, которая активно эксплуатируется не только в рамках отдельных целевых атак, но и в автоматически распространяющемся вредоносном ПО (WannaCry, NotPetya/ExPetr), была обнаружена на узлах внутренней сети в 75% анализируемых компаний, тестирование на проникновение которых проводилось после публикации информации об уязвимости.

В целом, **устаревшее ПО было обнаружено на сетевом периметре в 86% проанализированных компаний**, и во внутренней сети – в 80% компаний.

Отдельно стоит отметить уязвимости удаленного выполнения кода через сервис Java RMI и десериализацию Java в Apache Commons Collections, а также в других библиотеках Java, использующихся во многих готовых продуктах. В 2017 году небезопасная десериализация была включена проектом OWASP в десять наиболее существенных рисков веб-приложений OWASP TOP 10 и заняла восьмое место (A8-Insecure Deserialization). Данная проблема столь масштабна, что компания Oracle рассматривает возможность полностью отказаться в новых версиях Java от встроенной поддержки сериализации/десериализации данных по причине того, что множество уязвимостей связаны с данными операциями[1].

Получение доступа к сетевым устройствам нередко способствовало успешному развитию атаки во внутренней сети. В сетевом оборудовании эксплуатировались такие уязвимости, как:

- **cisco-sa-20170317-cmp** или CVE-2017-3881 (Cisco IOS), позволяющая неавторизованному атакующему получить доступ к коммутатору с максимальными привилегиями через протокол Telnet.
- **cisco-sa-20170629-snmp** (Cisco IOS), позволяющая получить доступ к устройству с максимальным уровнем доступа через протокол SNMP, зная лишь значение строки SNMP Community с правами на чтение, которое зачастую является словарным.
- включенная в коммутаторах по умолчанию функция **Cisco Smart Install**, для использования которой не требуется аутентификация, в результате чего неавторизованный атакующий может получить или заменить конфигурационный файл коммутатора[2].

Анализ защищённости веб-приложений в 2017 году показал, что наиболее уязвимыми являются приложения государственных учреждений (все проанализированные приложения содержали уязвимости высокой степени риска), а наименее уязвимыми - приложения электронной коммерции (28% приложений с уязвимостями высокой степени риска). Наиболее часто в приложениях встречались такие уязвимости как раскрытие чувствительных данных (24%), межсайтовое выполнение сценариев (24%), непроверенные переадресации и пересылки (14%), недостаточная защита от атак методом перебора пароля (14%), словарные учётные данные пользователя (13%).

Для повышения уровня защищённости рекомендуется уделить внимание безопасности веб-приложений, своевременному обновлению уязвимого ПО, парольной защите, правилам межсетевого экранирования, а также регулярно проводить анализ защищённости ИТ-инфраструктуры, в том числе приложений. В связи с тем, что в больших сетях задача полного предотвращения компрометации информационных ресурсов является крайне сложной, а при атаках, основанных на базе уязвимостей нулевого дня – зачастую и невозможной, особенно важно обеспечить как можно более раннее обнаружение инцидентов ИБ. Своевременное обнаружение действий злоумышленников на ранних стадиях атаки и оперативное реагирование могут помочь избежать ущерба от инцидента или значительно его снизить. Для зрелых организаций, где процессы анализа защищённости, управления уязвимостями и обнаружения инцидентов информационной безопасности, уже налажены, стоит рассмотреть возможность проведения тестирований типа Red Teaming. Подобные работы позволяют не только проверить уровень защищённости инфраструктуры от высококвалифицированных атакующих, действующих максимально скрытно, но обеспечить тренировку службы ИБ по выявлению атак и реагированию на инциденты в условиях, приближенных к реальным.

1 https://www.bleepingcomputer.com/news/security/oracle-plans-to-drop-java-serialization-support-the-source-of-most-security-bugs/

2 https://dsec.ru/presentations/cisco-smart-install/

«Лаборатория Касперского»

Решения для крупного бизнеса:
www.kaspersky.ru/enterprise

Аналитика и отчёты о киберугрозах:
www.securelist.ru

#truecybersecurity
#HuMachine

www.kaspersky.ru