УГРОЗА ДОСТУПА К ЛОКАЛЬНЫМ ФАЙЛАМ СЕРВЕРА ПРИ ПОМОЩИ URL

ПОДГОТОВИЛА СТУДЕНТКА ГРУППЫ 15.11Д-МОСИП12/21Б
ГАИТОВА АЗЭЛЬ

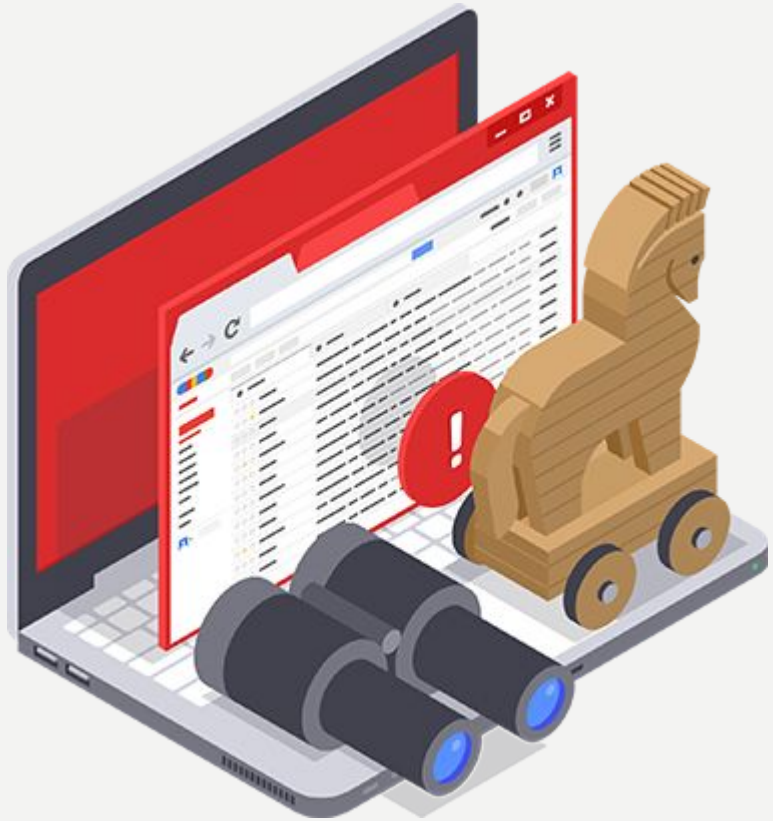
СОДЕРЖАНИЕ

- Введение
- Угроза доступа к локальным файлам сервера при помощи URL
- Вредоносное ПО
- Схема
- Жизненный цикл
- Антивирусное средство и его функции
- Заключение

ВВЕДЕНИЕ

Современный мир насыщен цифровыми технологиями, которые стали неотъемлемой частью нашей повседневной жизни. Однако, с появлением новых возможностей, появляются и новые угрозы, связанные с безопасностью данных.

Одной из таких угроз является доступ к локальным файлам сервера при помощи URL.



УБИ.016 УГРОЗА ДОСТУПА К ЛОКАЛЬНЫМ ФАЙЛАМ СЕРВЕРА ПРИ ПОМОЩИ URL

Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю.

Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами.

Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе.

ВРЕДОНОСНОЕ ПО

Web-шелл (web shell) - это программа, которая позволяет злоумышленнику получить удаленный доступ к серверу. Она может быть загружена на сервер через уязвимости в веб-приложениях или через украденные учетные данные.

Web-шелл может использоваться для выполнения различных действий на сервере, таких как чтение, запись и удаление файлов, запуск команд на сервере и т.д. Это делает его очень опасным инструментом для злоумышленников, которые могут использовать его для получения доступа к конфиденциальной информации, установки вредоносных программ и т.д.

СХЕМА

Для защиты от угрозы web-шелла необходимо следить за безопасностью сервера и регулярно обновлять его программное обеспечение. Также необходимо использовать сильные пароли и двухфакторную аутентификацию для защиты учетных данных. Кроме того, необходимо регулярно проверять сервер на наличие web-шеллов и удалять их при обнаружении.

Уязвимость web-шелла заключается в том, что он позволяет злоумышленнику получить удаленный доступ к серверу и выполнить различные действия на нем. Это может привести к утечке конфиденциальной информации, установке вредоносных программ, изменению или удалению файлов и т.д.

Риск от web-шелла заключается в том, что злоумышленник может получить полный контроль над сервером и использовать его для своих целей. Это может привести к серьезным последствиям для организации, таким как потеря данных, штрафы за нарушение законодательства о защите данных и репутационный ущерб.

Ущерб от web-шелла может быть значительным для организации, так как это может привести к потере конфиденциальной информации, нарушению работоспособности сервера и серьезным финансовым потерям. Кроме того, уязвимость web-шелла может привести к угрозам безопасности для клиентов и пользователей организации.

ЖИЗНЕННЫЙ ЦИКЛ

- Подготовка к проникновению включает в себя поиск уязвимостей и создание web-шелла, который может быть использован для получения удаленного доступа к серверу.
- Поиск объектов воздействия включает в себя исследование сервера и его приложений для определения того, какие файлы и директории могут быть скомпрометированы.
- Реализация web-шелла включает в себя загрузку его на сервер и выполнение необходимых действий для получения удаленного доступа.
- Завершение жизненного цикла web-шелла может произойти по нескольким причинам, таким как обнаружение уязвимости и ее исправление, удаление web-шелла администратором системы или его автоматическое удаление при перезагрузке сервера.

АНТИВИРУСНОЕ СРЕДСТВО И ЕГО ФУНКЦИИ

Антивирусное средство против web shell - это программа, которая предназначена для обнаружения и удаления вредоносных web shell скриптов, которые могут использоваться злоумышленниками для получения несанкционированного доступа к веб-сайту и серверу. Для борьбы с web shell Kaspersky Anti-virus.
Функции антивирусного средства против web shell могут включать:

1. Обнаружение и удаление вредоносных файлов и скриптов, связанных с web shell.
2. Мониторинг системы на наличие подозрительной активности, связанной с web shell, такой как попытки изменить файлы, создать новые файлы или отправить данные на удаленный сервер.
3. Оповещение администратора системы о подозрительной активности и действиях, которые необходимо предпринять для защиты системы.
4. Автоматическое обновление базы данных вирусов и уязвимостей, чтобы обеспечить максимальную защиту от новых угроз.
5. Ограничение доступа к файлам и папкам на сервере, чтобы предотвратить возможность загрузки и выполнения вредоносных скриптов.
6. Проверка кода на наличие уязвимостей и ошибок, которые могут быть использованы злоумышленниками для внедрения web shell.
7. Отчетность и журналирование для анализа подозрительной активности и выявления уязвимостей в системе.

ЗАКЛЮЧЕНИЕ

Угроза доступа к локальным файлам сервера при помощи URL – это серьезная проблема, которая может привести к утечке конфиденциальной информации и нарушению работы организации.

В данной работе был рассмотрено такое вредоносное ПО, как web shell. Был изучен его жизненный цикл, составлена схема и изучено антивирусное средство против данного типа вирусов.

СПАСИБО ЗА ВНИМАНИЕ!