Научная статья
Original article
УДК 004.424

ВЕБ-ОБОЛОЧКА

WEB SHELL

Казарян Каторина Камоевна студент специалитета, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kazaryan_katorina@mail.ru

Белан Виктория Вадимовна магистрант, Донской государственный технический университет, г. Ростов-на-Дону, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), viktoriyabelan2018@gmail.com

Kazaryan Katorina Kamoevna specialty student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kazaryan_katorina@mail.ru

Belan Victoria Vadimovna Master student, Don State Technical University, Rostov-on-Don, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), viktoriyabelan2018@gmail.com

Аннотация: Веб-оболочки - это вредоносные сценарии, которые позволяют злоумышленникам взламывать веб-серверы и запускать дополнительные атаки. Злоумышленники сначала проникают в систему или сеть, а затем устанавливают веб-оболочку. С этого момента они используют его как постоянный бэкдор в целевые веб-приложения и любые подключенные системы. Работа с такими системами описана в данной статье.

Цель работы: Анализ веб-оболочек на уязвимости и борьба с атаками в данной среде

Abstract: Web shells are malicious scripts that allow attackers to compromise web servers and launch additional attacks. Attackers first penetrate the system or network and then install the web shell. From now on, they use it as a permanent backdoor to targeted web applications and any connected systems. Working with such systems is described in this article.

Ключевые слова: Веб-оболочки, злоумышленники, защита данных, сетевые атаки, сценарии атак

Keywords: Web shells, attackers, data protection, network attacks, attack scenarios

Как злоумышленники используют веб-оболочки?

Злоумышленники используют веб-оболочки для ряда сценариев:

- Извлечение и сбор конфиденциальной информации и учетных данных.
- Загрузка вредоносного ПО, которое потенциально может создать лазейку для дальнейшего заражения и сканирования других жертв.
- Удаление веб-сайтов путем изменения или добавления файлов.

Веб-оболочка может служить точкой ретрансляции для выдачи команд хостам, расположенным внутри сети, без прямого доступа в Интернет. Веб-оболочки также могут участвовать в инфраструктуре управления и контроля - например, веб-оболочка может использоваться для взлома хоста и включения его в ботнет . Злоумышленники могут заразить другие системы в сети с помощью веб-оболочки, чтобы поставить под угрозу дополнительные ресурсы.

Злоумышленники используют широкий спектр уязвимостей и эксплойтов веб-приложений для доставки веб-оболочек, включая внедрение SQL (SQLi) и межсайтовые сценарии (XSS). Злоумышленники также используют уязвимости в службах и приложениях, уязвимости обработки файлов, открытые интерфейсы администратора, а также уязвимости включения локальных файлов (LFI) и удаленного включения файлов (RFI).

Число атак через веб-оболочку растет

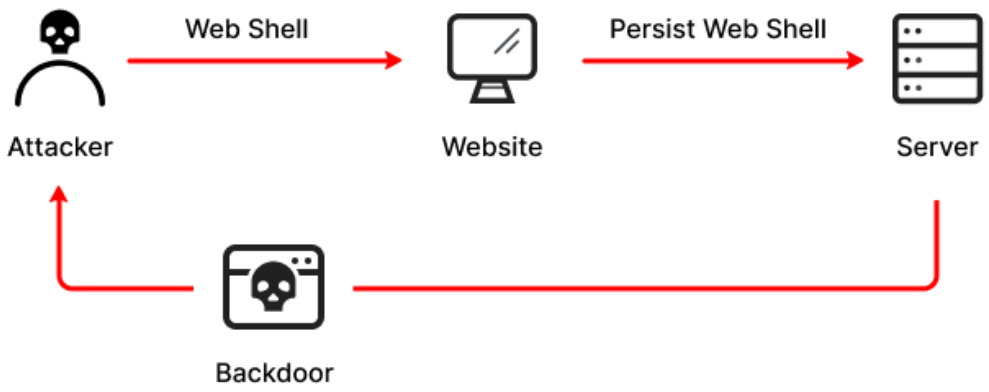
Microsoft выявила рост атак через веб-оболочку со стороны различных групп, затрагивающих как частные, так и государственные организации. К ним относятся группы продвинутых постоянных угроз (APT), использующие веб-оболочки, чтобы закрепиться в целевых сетях.

Одна из таких атак, обнаруженная группой обнаружения и реагирования Microsoft, включала веб-оболочки, установленные в нескольких папках на неправильно настроенном сервере организации, что позволяло злоумышленнику перемещаться по сторонам и устанавливать веб-оболочки в других системах. Бэкдор DLL, зарегистрированный как служба, позволял злоумышленнику оставаться на почтовом сервере, загружать полезные нагрузки вредоносных программ и отправлять команды в форме электронных писем.

Если веб-оболочка успешно имплантируется на веб-сервер, она позволяет удаленному злоумышленнику выполнять вредоносные команды и красть данные. Хакерские группы, которые использовали веб-оболочки в своих атаках, включают группу Gallium и группу Lazarus.

Как работают веб-оболочки

Атаки через веб-оболочку состоят из нескольких этапов: сначала злоумышленник создает на сервере постоянный механизм, обеспечивающий удаленный доступ. Затем они пытаются повысить привилегии и использовать бэкдор для атаки на организацию или использования ее ресурсов для преступной деятельности.



Как работает атака через веб-оболочку

1. Постоянный удаленный доступ

Скрипты веб-оболочки предоставляют бэкдор, позволяющий злоумышленникам получить удаленный доступ к незащищенному серверу. Настойчивым злоумышленникам не нужно использовать новую уязвимость для каждого злонамеренного действия. Некоторые злоумышленники даже исправляют уязвимость, которую они используют, чтобы не дать другим сделать то же самое и избежать обнаружения.

Некоторые веб-оболочки используют такие методы, как аутентификация по паролю, чтобы гарантировать, что только определенные злоумышленники могут получить к ним доступ. Веб-оболочки обычно маскируют себя, включая код, который не позволяет поисковым системам заносить в черный список веб-сайт, на котором установлена оболочка.

2. Повышение привилегий

Веб-оболочки обычно запускаются с правами пользователя, которые могут быть ограничены. Злоумышленники могут повышать привилегии через веб-оболочки, используя уязвимости системы для получения привилегий root. Доступ к учетной записи root позволяет злоумышленникам выполнять практически любые действия - они могут устанавливать программное обеспечение, изменять разрешения, добавлять или удалять пользователей, читать электронную почту, красть пароли и т. Д.

3. Разворот и запуск атак

Злоумышленники могут использовать веб-оболочки для поиска дополнительных целей как в сети, так и за ее пределами. Процесс прослушивания сетевого трафика для идентификации активных хостов, брандмауэров или маршрутизаторов (перечисление) может занять недели, в течение которых злоумышленники будут вести себя сдержанно, чтобы избежать обнаружения.

Злоумышленник, успешно сохраняющийся в сети, будет терпеливо двигаться, возможно, даже используя скомпрометированную систему для атаки других целей. Это позволяет злоумышленнику оставаться анонимным, а переключение между несколькими системами может сделать практически невозможным отследить источник атаки.

4. Бот-стадо

Веб-оболочки могут использоваться для подключения серверов к ботнету (сети систем, контролируемых злоумышленником). Затронутые серверы выполняют команды, отправленные злоумышленниками через сервер управления и контроля, подключенный к веб-оболочке.

Это распространенный метод DDoS-атак , требующих большой пропускной способности. Злоумышленники не нацелены напрямую на систему, в которой они установили веб-оболочку, а просто используют ее ресурсы для атаки более ценных целей.

Защита веб-оболочки

Вот несколько способов защитить вашу организацию от угроз веб-оболочек.

Мониторинг целостности файлов

Решения для мониторинга целостности файлов (FIM) предназначены для блокировки изменений файлов в каталогах, доступных через Интернет. Как только изменение обнаружено, инструменты FIM предупреждают администраторов и сотрудников службы безопасности. Внедрение FIM может помочь обнаруживать проблемы в режиме реального времени, как только

файлы сохраняются в каталоге. Это может помочь сотрудникам службы безопасности быстро найти и удалить веб-оболочки.

Решения для мониторинга целостности можно настроить так, чтобы разрешить определенные изменения файлов и заблокировать другие. Если, например, ваше веб-приложение обычно обрабатывает только файлы в формате переносимых документов (PDF), решение для контроля целостности может блокировать загрузки, которые не заканчиваются расширением «.pdf».

Разрешения веб-приложения

При определении разрешений для веб-приложений важно использовать концепцию наименьших привилегий. Главный принцип, лежащий в основе этой концепции, - предоставить пользователям минимум привилегий, необходимых для выполнения их роли. Цель состоит в том, чтобы гарантировать, что у каждого пользователя нет привилегий, которых он не должен иметь, и что действия скомпрометированных учетных записей ограничены .

Принцип наименьших привилегий может помочь предотвратить загрузку злоумышленниками веб-оболочки в уязвимые приложения. Вы можете установить его, не разрешая веб-приложениям напрямую писать в каталог, доступный через Интернет, или изменять код, доступный через Интернет. Таким образом, сервер блокирует доступ актера к веб-каталогу.

Предотвращение вторжений и брандмауэры веб-приложений

Система предотвращения вторжений (IPS) - это технология сетевой безопасности, предназначенная для защиты ИТ-активов и среды от угроз путем мониторинга потока сетевого трафика. Брандмауэры веб-приложений (WAF) защищают от угроз путем фильтрации, мониторинга и блокировки HTTP-трафика, поступающего к веб-службам и от них.

При реализации предотвращения вторжений организациям следует использовать несколько технологий. При совместном использовании решения IPS и WAF могут отслеживать поток трафика и блокировать известные вредоносные загрузки. В идеале каждое устройство безопасности, вводимое в

экосистему, должно быть адаптировано к конкретным потребностям организации.

Сегментация сети

Сегментация сети - это тип архитектуры, которая разбивает сеть на отдельные подсети. Каждая подсеть считается сегментом, и каждый сегмент имеет собственную защищенную сеть. Архитектура разделения сети предотвращает соединения между несвязанными сегментами. Это разделение может помочь предотвратить распространение веб-оболочки.

Существует широкий спектр методов разделения сети. Изоляция подсети демилитаризованной зоны (DMZ), например, является основным методом, с помощью которого можно изолировать серверы, подключенные к Интернету. Существуют также более продвинутые методы разделения сети, такие как программно-определяемые сети (SDN), которые могут помочь реализовать архитектуру с нулевым доверием.

Нуль доверия архитектура требует явного разрешения , прежде чем разрешить связь между узлами в сети. Этот тип техники может помешать злоумышленникам объединить веб-оболочки в цепочку для более глубокого проникновения в сеть. В этом сценарии веб-оболочки по-прежнему могут влиять на целевой сервер, но злоумышленники не могут продвинуться дальше в сеть.

Обнаружение конечной точки и ответ (EDR)

Определенные решения для обнаружения и отклика конечных точек (EDR) и ведения журналов хоста могут помочь защитить от атак через веб-оболочку. Эти решения отслеживают системные вызовы и аномалии происхождения процессов и используют шаблоны злонамеренного поведения для обнаружения веб-оболочек.

Решения EDR с возможностями защиты веб-оболочки могут отслеживать все процессы на конечных точках, включая вызванные системные вызовы. Когда веб-оболочки вызывают ненормальное поведение в процессе веб-сервера, решение распознает это. Например, большинство веб-серверов

обычно не запускают утилиту ipconfig. Это распространенный метод разведки с помощью веб-оболочки, который можно распознать с помощью поведенческого анализа.

Литература

1. Mark Liberman Phishing - itre.cis.upenn.edu/~myl/languagelog/archives/001477.html (англ.) (22 сентября 2004).
2. Cave Paintings Phishing - historyofscience.com/G2I/timeline/index.php?id=1682 (англ.).
3. Usenet - groups.google.com/group/alt.online-service.america-online (англ.). — 2 января 1996 г.
4. The Phishing Guide - www.webcitation.org/5w9YT7W5q (англ.). Архивировано из первоисточника - www.technicalinfo.net/papers/Phishing.html 31 января 2011.
5. phishing - www.webcitation.org/5w9YTyC3n (англ.) (1 августа 2003). Архивировано из первоисточника - www.wordspy.com/2003/08/phishing.html 31 января 2011.
6. Michael Stutz AOL: A Cracker's Paradise? - wired-vig.wired.com/science/discoveries/news/1998/01/9932 (англ.) (29 января 1998).
7. History of AOL Warez - www.webcitation.org/5w9YV2fuL (англ.). Архивировано из первоисточника - www.rajuabju.com/warezirc/historyofaolwarez.htm 31 января 2011.

References

1. Mark Liberman Phishing - itre.cis.upenn.edu/~myl/languagelog/archives/001477.html (English) (September 22, 2004).
2. Cave Paintings Phishing - historyofscience.com/G2I/timeline/index.php?id=1682.

3. Usenet - groups.google.com/group/alt.online-service.america-online (English). - January 2, 1996
4. The Phishing Guide - www.webcitation.org/5w9YT7W5q (English). Archived from the original - www.technicalinfo.net/papers/Phishing.html January 31, 2011.
5. phishing - www.webcitation.org/5w9YTyC3n (English) (August 1, 2003). Archived from the original - www.wordspy.com/2003/08/phishing.html on January 31, 2011.
6. Michael Stutz AOL: A Cracker's Paradise? - wired-vig.wired.com/science/discoveries/news/1998/01/9932 (January 29, 1998).
7. History of AOL Warez - www.webcitation.org/5w9YV2fuL. Archived from the original - www.rajuabju.com/warezirc/historyofaolwarez.htm on January 31, 2011.

© Казарян К.К., Белан В.В., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Казарян К.К., Белан В.В. ВЕБ-ОБОЛОЧКА// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.