УДК 004.056

УСТАРЕВШЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК УГРОЗА КИБЕРБЕЗОПАСНОСТИ

Белоус А.С. (Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный морской технический университет»)

Научный руководитель – к.т.н., доцент Чернов А.И.
(Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный морской технический университет»)

Введение.
От года к году всё больше компаний и проектов ведут свою деятельность онлайн, потому поднимается важный вопрос о безопасности и приватности их личной информации. Однако устаревшее программное обеспечение является угрозой кибербезопасности, которую часто нельзя игнорировать. Для того, чтобы достичь уровня кибербезопасности, необходимо иметь достоверные сведения, что устаревшие решения находятся в соответствии с указанными стандартами. В работе будет описано, какую угрозу кибербезопасности несут устаревшие программные решения. А также, будет рассмотрен пример использования эксплойта и защиты от подобного рода атаки

Основная часть.
По версии корпорации OWASP, использование устаревшего и/или уязвимого программного обеспечения носит критичный характер и входит в категорию угроз TOP10.
Всё это потому, что за счёт эксплуатации уязвимости в ПО можно получить как прямой доступ к коммерческой, персональной информации организации, так и завладеть полным контролем над частью или всей её инфраструктурой. Всё это может повлечь как только финансовые, репутационные издержки, утечку персональной и корпоративной информации, так и подвергнуть угрозе здоровья граждан, если, к примеру, уязвимое ПО установлено на производственном предприятии.
Наиболее критическим типом уязвимости в ПО является RCE – Remote Code Execution – удаленное исполнение команд, что даёт возможность захвата инфраструктуры жертвы и установления полного контроля над ней.
С учётом вышесказанного, злоумышленник способен превратить инфраструктуру организации в ботнет, как для проведения масштабных DDOS атак, так и для захвата оборудования другой компании, что потенциально будет способствовать распространению вирусной «эпидемии» в геометрической прогрессии.
В работе будет рассмотрен способ эксплуатации актуальной уязвимости при помощи открытого ПО на базе Kali Linux, благодаря уязвимости сервиса, искусственно развернутом на виртуальной машине. Будет использовано программное обеспечение для анализа сервисов и использования эксплойта.
Основным способом противодействия подобному роду атак является своевременное обновление программного обеспечения, отказ от небезопасных программных решений в пользу аналогов, если поддержка и обновление текущего ПО не представляется возможным.
Одним из вариантов защиты является многослойность – разделение внешней и внутренней инфраструктуры организации, что даёт возможность продолжать деятельность, несмотря на заражение внешней инфраструктуры
Более того, рекомендуется соответствующе заботиться о безопасности критичных данных, отслеживать внешние подключения, попытки вторжения и несогласованного сканирования сервисов. А также, рекомендуется периодически проверять актуальность ПО, установленного на инфраструктуре организации. Всё это поможет предотвратить плачевные последствия.

Выводы.
Проведен анализ актуальности проблемы кибербезопасности, связанной с несвоевременным решением задач по обновлению программного обеспечения, содержащего критические ошибки. Рассмотрен сценарий событий при получении несанкционированного доступа к инфраструктуре организации, что впоследствии привело к дальнейшему распространению вирусной «эпидемии» и созданию ботнета. Описан процесс атаки на уязвимый сервис и метод защиты от данного рода атак.

Список использованных источников:

1. OWASP TOP 10 [Электронный ресурс] URL: https://owasp.org/Top10/
2. Кибербезопасность 2022-2023. Тренды и прогнозы [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/

Белоус А.С. (автор) Подпись

Чернов А.И. (научный руководитель) Подпись