www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Политика ответственного сканирования

1. Введение

Одно из главных направлений деятельности Акционерного общества «Сайбер ОК» (далее — Компания, мы) заключается в поиске уязвимостей в инфраструктурах, системах и программном обеспечении. В ходе нашей работы мы можем обнаружить уязвимости разных оценок опасности, в том числе и критические уязвимости.

В нашей работе мы руководствуемся следующими принципами:

- заботимся об информационной безопасности и не используем полученную нами информацию об уязвимостях каким-либо противоправным образом;
- прикладываем много усилий для того, чтобы сделать безопаснее цифровую часть нашего общества, обеспечивая прозрачность и доступность информации об открытых и потенциально уязвимых ресурсах;
- придерживаемся политики ответственного разглашения и всегда безвозмездно сообщаем о найденных уязвимостях вендорам.

Все наши действия по сканированию устройств в Интернете регулируются данным документом, который поясняет, как и зачем мы проводим сканирование.

2. Методология сканирования

2.1. При сканировании мы используем инструменты, которые определяют:
- устройства, подключенные к сети Интернет, их типы и характеристики (например, используемые порты и версии программного обеспечения);
- сертификаты SSL и их связи с определенными IP-адресами или доменами.

2.2. Частота сканирования: сканирование IP-адресов и доменов проводится не чаще одного раза в сутки.

2.3. Цели сканирования: определение открытых портов, устаревшего или уязвимого программного обеспечения, и других потенциальных угроз безопасности.

2.4. IP-адреса, с которых осуществляется сканирование, имеют DNS имена вида scan-[dd].skipa.cyberok.ru, где dd — от 00 до 300. Проверить их принадлежность можно с помощью обратного DNS запроса ping -a [IP], host [IP] или dig [IP]. На данный момент все используемые IP-адреса принадлежат сети 85.142.100.0/24.

2.5. При проведении сканирования мы также используем программное обеспечение СКИПА — Система Контроля и Информирования о Поверхности Атак (далее — СКИПА), нашей собственной разработки. СКИПА относится к классу программного обеспечения «Средства обнаружения угроз и расследования сетевых инцидентов», является системой контроля поверхности атак (attack surface management, ASM) и включает в себя механизмы контроля и анализа защищенности сети. Функционирование подобного программного обеспечения может вызывать срабатывание средств защиты, однако при этом такое программное обеспечение не является вредоносным программным обеспечением.

То, что СКИПА не является вредоносным программным обеспечением, также подтверждает тот факт, что программное обеспечение СКИПА:

- 05 сентября 2023 года зарегистрировано в Едином реестре российских программ для электронных вычислительных машин и баз данных (далее — Реестр) за регистрационным номером 18867. При регистрации каждый экземпляр программного обеспечения проходит всестороннюю проверку экспертами Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Ознакомиться с информацией из

Реестра о СКИПА можно здесь — https://reestr.digital.gov.ru/reestr/1765596/?sphrase_id=4356720.

- 10 мая 2023 года зарегистрировано в реестре программ для ЭВМ Федеральной службой по интеллектуальной собственности, патентам и товарным знакам, в подтверждении чего выдано свидетельство о государственной регистрации программы для ЭВМ № 2023619366.

3. Исключения из списка сканирования

Если вы желаете исключить свои ресурсы из нашего списка сканирования, то вы можете:

- самостоятельно запретить доступ с IP-адресов, с которых мы проводим сканирование;
- написать нам на abuse@cyberok.ru, указав соответствующие IP-адреса или домены.

4. Процедура ответа на инциденты

В случае обнаружения активности со стороны Компании, которая вызывает опасения, просим немедленно связаться с нами по адресу: abuse@cyberok.ru. Мы гарантируем оперативное рассмотрение всех обращений и принятие необходимых мер.

5. Контакты

Для общих вопросов, пожалуйста, свяжитесь с нами по адресу info@cyberok.ru.

6. Гарантии конфиденциальности

Обнаруженная информация используется исключительно в исследовательских и аналитических целях.

Никакие персональные данные или конфиденциальная информация не обрабатываются и не передаются третьим лицам. Если в процессе сканирования мы случайно получим доступ к персональным данным, они будут немедленно удалены.

Данные, полученные в результате сканирования, хранятся в зашифрованном виде, и доступ к ним разграничен по ролям — то есть доступ к ним имеют только авторизованные сотрудники.

7. Заключение

Основываясь на этой политике, мы прилагаем все усилия для того, чтобы обеспечивать безопасность и надежность интернет-пространства, взаимодействуя с сообществом на принципах открытости и прозрачности.