Отчет Felix от «Персонального аналитика»
По сайту https://[redacted]
с [redacted].2022 по [redacted].2022

Из журнала Felix

Дополнительные детали по событиям из данного раздела смогут быть созданы по конкретному запросу.

Дата	Категория	Серьезность	Источник	Детали	Рекомендации
15.[redacted].2022	Брутфорс	Низкая	• Клиенты [redacted] из разных ЦОД в ЕС • Клиент [redacted] в РФ	Стандартная атака, без признаков знания вашего сайта	Ничего не надо – Felix отсекает
15.[redacted].2022	DDoS	Средняя	Германия, США	Плохо регулируемые веб-сканеры	Ничего не надо – Felix отсекает
15.[redacted].2022	Спам	Низкая	Польша	Стандартная атака, без признаков знания вашего сайта	Ничего не надо – Felix отсекает
Постоянно	Дизайн сайта	Высокая	Все посетители сайта, санкционированные и не санкционированные	Пока посетитель сидит на любой странице сайта, сайт автоматически отправляет запрос на ссылку https://[redacted] раз в секунду. В течение DDoS-атаки это приведет к усилению загрузки, возможно в несколько раз.	Со своим разработчиком обсудить возможность ограничения использования данной ссылки к авторизованным пользователям и(или) подбору страниц.
16.[redacted].2022	Поиск уязвимостей	Средняя	• Клиент [redacted] (США) • Франция	Стандартная атака, без признаков знания вашего сайта	Ничего не надо – Felix отсекает
17.[redacted].2022	Поиск уязвимостей + DDoS	Средняя	[redacted] (США)	Стандартная атака, но очень упорная.	Ничего не надо – Felix отсекает
17.[redacted].2022	Контент сайта	Средняя	Яндекс	Бот Яндекс посещает ссылку https://[redacted] и получает ошибку 404 (страницы не найдено).	Узнать, должна ли такая страница существует. Если да, то починить проблему на сайте. Если нет, то разобраться, откуда Яндекс получил неверную ссылку.
18.[redacted].2022	Поиск уязвимостей	Средняя	[redacted] (Германия)	Упорная атака по незащищенным ссылкам ночью.	Ничего не надо – Felix отсекает

Дата	Категория	Серьезность	Источник	Детали	Рекомендации
Раз в день-два	Сканирование	Средняя	IP-адреса [redacted] (СПб)	Сканирует все контентные страницы вашего сайта, выполняет функционал «поиск» на сайте. Возможно, конкурент или злоумышленник создает сайт-двойник.	Наблюдать. Если конкурент, то это деловая проблема. А если злоумышленник, то целью может быть кража данных ваших клиентов и партнеров.
19.[redacted].2022	DDoS	Средняя	Германия, США	Плохо регулируемые веб-сканеры	Ничего не надо – Felix отсекает
19.[redacted].2022	Поиск уязвимостей	Средняя	ЕС, США	Стандартная атака, без признаков знания вашего сайта	Ничего не надо – Felix отсекает
20.[redacted].2022	Поиск уязвимостей	Высокая	IP-адреса [redacted] (клиент [redacted], Калининград)	В 17:22 запустил сканнер уязвимости вашего CMS. Такое тоже было в ваших прошлых записях журнала: 05-06.[redacted].2022 и 30.[redacted].2022.	Если это ваш сотрудник, то ничего не надо. Если нет, то немедленно сами запустить сканнер, поправить все найденные уязвимости; обновить ПО CMS до последней версии. Наблюдать.
21.[redacted].2022	Брутфорс	Высокая	Роттердам	Подбор паролей по административной ссылки вашего сайта 06:41	Felix атак отсек, но очень рекомендуем проверить пароль администратора за силу, обновить ПО CMS до последней версии, при возможности запустить двухфакторную аутентификацию.
21.[redacted].2022	Сканирование	Средняя	IP-адреса [redacted] (Краснодар)	Сканирует все контентные страницы вашего сайта, выполняет функционал «поиск» на сайте. Возможно, конкурент или злоумышленник создает сайт-двойник.	Наблюдать. Если конкурент, то это деловая проблема. А если злоумышленник, то целью может быть кража данных ваших клиентов и партнеров.
21.[redacted].2022	Поиск уязвимостей	Средняя	ЕС	Стандартная атака по другому CMS.	Ничего не надо – Felix отсекает
21.[redacted].2022	DDoS	Средняя	Норвегия	Плохо регулируемые веб-сканеры	Ничего не надо – Felix отсекает
22.[redacted].2022	Контент сайта	Средняя	США, СПб, Москва. Один из компании вашего партнера [redacted]	Неоднократное посещение ссылки https://[redacted], которая дает 404 (страницы не найдено).	Узнать, должна ли такая страница существует. Если да, то починить проблему на сайте. Если нет, то разобраться, откуда Яндекс получил неверную ссылку.

Дата	Категория	Серьезность	Источник	Детали	Рекомендации
22.xx.2022	Сертификат-SSL	Высокая	-	Прок вашего текущего сертификата истечет через 5 дней.	Обновить сертификат, чтобы безопасное соединение с сайтом продолжалось без ошибок.

Из других записей, Вами нам предоставленных на анализ

Результаты анализы по данным записям могут быть ограничены, поскольку активность не было обработана Felix и(или) не все данные, необходимые для выяснения проблемы, были предоставлены Вами.

Дата	Категория	Серьезность	Источник	Детали
С xxxxx.2022 по xxxxx.2022	DDoS	Средняя	Невозможно сказать, поскольку Вы были подключены к сервису xxxxxxxxx, все IP-адреса – их.	• Активность нескольких отдельных ботнетов по публичным ссылкам. • Плохо регулируемые веб-сканеры Стандартные атаки.
С xxxxx.2022 по xxxxx.2022	Поиск уязвимостей	Средняя	Невозможно сказать, поскольку Вы были подключены к сервису xxxxxxxxx, все IP-адреса – их.	Активность нескольких отдельных ботнетов
С xxxxx.2022 по xxxxx.2022	Брутфорс	Средняя	Невозможно сказать, поскольку Вы были подключены к сервису xxxxxxxxx, все IP-адреса – их.	Видимо – боты