WEBTOTEM

Сервис для мониторинга и защиты веб-сайтов.

WEBTOTEM

сервис для мониторинга и защиты веб-сайтов.

- Владельцы/разработчики веб-сайтов
- Регистраторы доменов / хостинги
- Корпорации
- Регуляторы

Защита от уязвимостей для владельцев

Поиск вредоносных для регулятора

«WebTotem Security»
Плагины и расширения

Внешнее сканирование

Ключевые модули

Домен:

- DNS
- Whols
- Даты
- IP
- Расположение
- Наличие защиты (Cloudflare и др.)

Доступность

Scoring

Технологии и CVE

SSL

Открытые пути

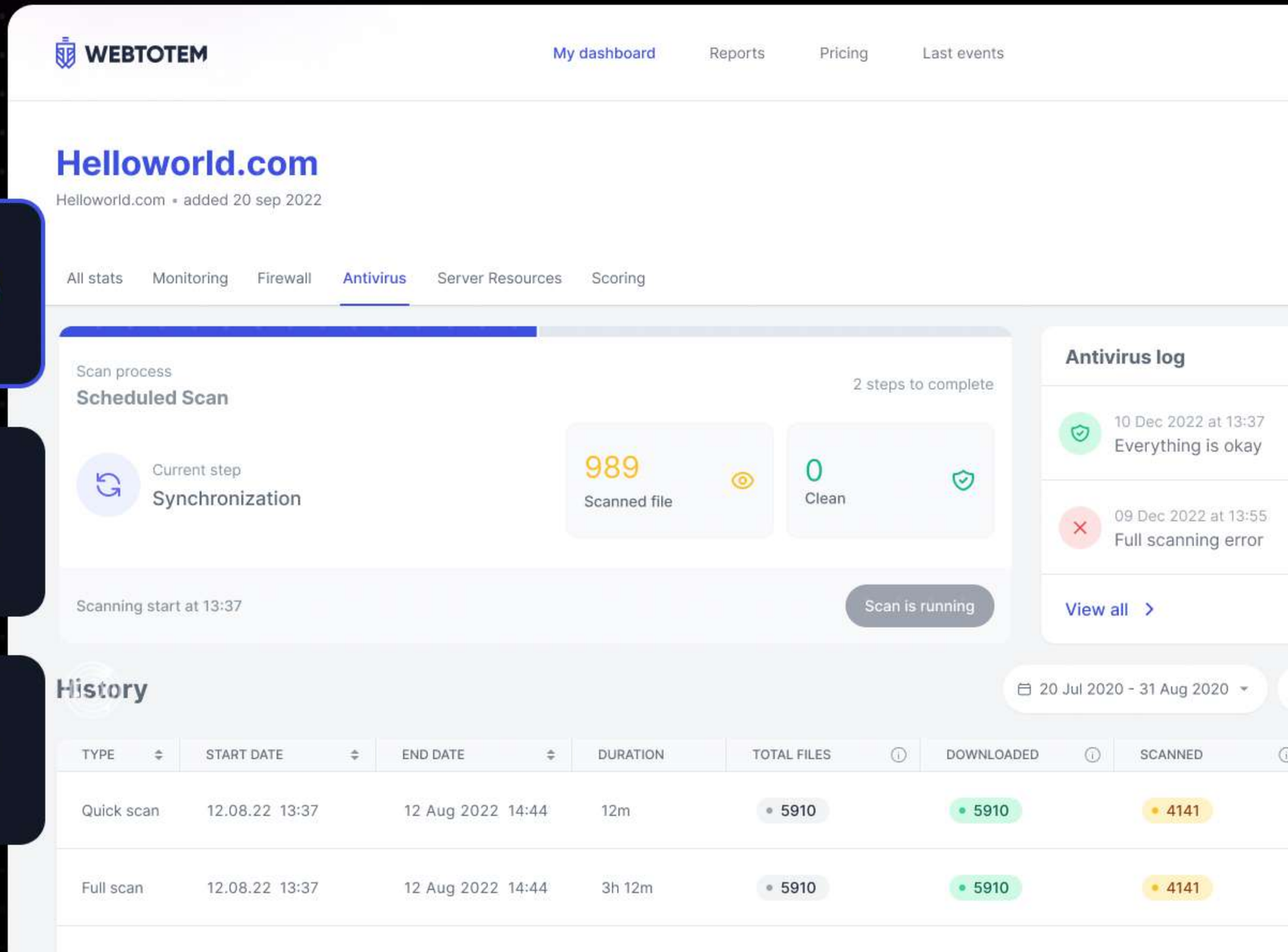
Открытые порты

Anti-phishing

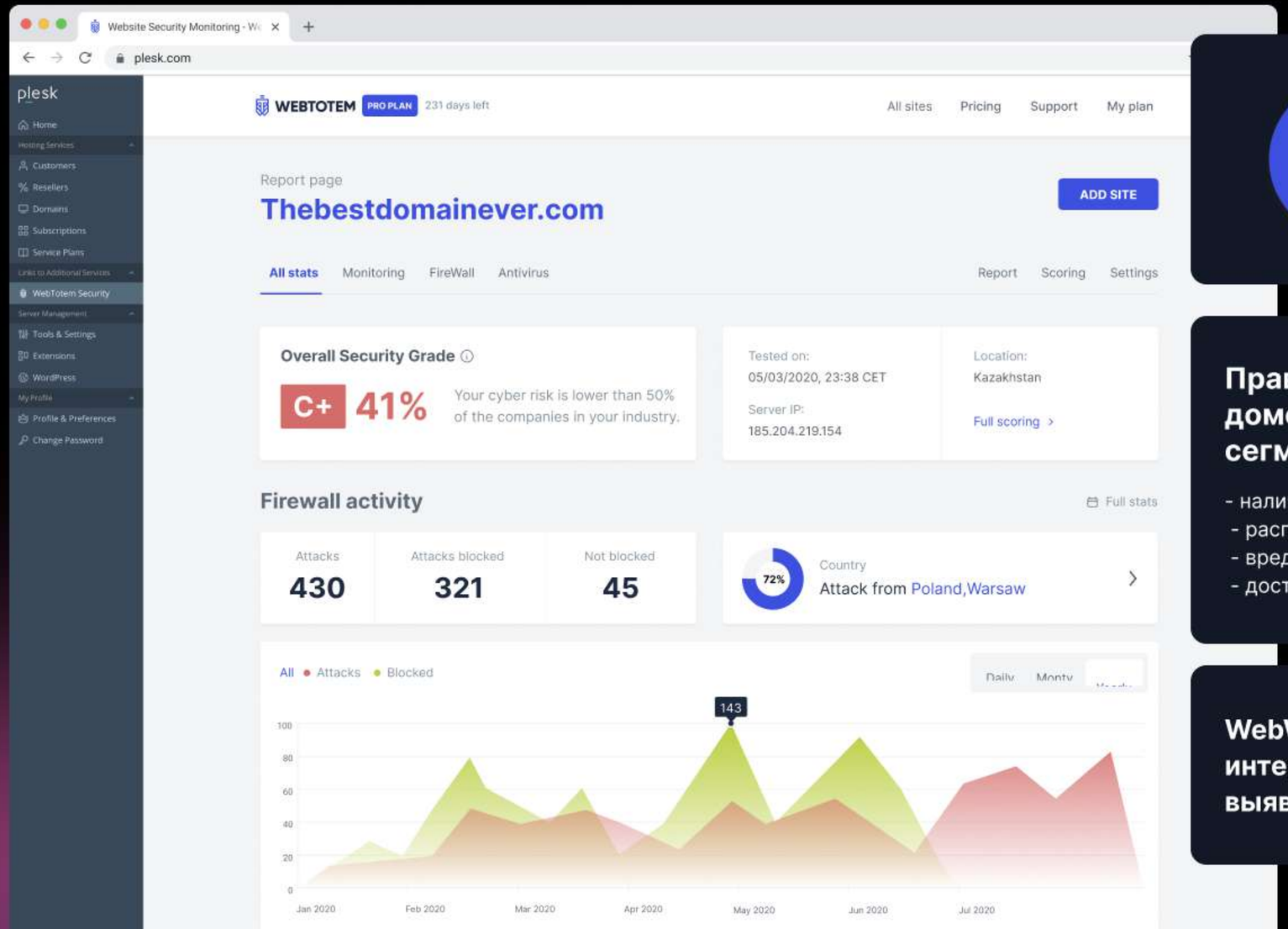
Внутреннее сканирование

Ключевые модули

- **Антивирус**
- **Ресурсы сервера**
- **Web application firewall, WAF**



Казахстанская доменная зона .kz



~190 тыс доменных имен.

WebTotem мониторит казахстанскую доменную зону

Правила регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета

- наличие сертификата безопасности
- расположение сервера вне РК
- вредоносное ПО
- достоверные данные о регистранте

WebWebTotem сканирует интернет-ресурсы для выявления:

- Сайты с уязвимостями
- Зловредные сайты

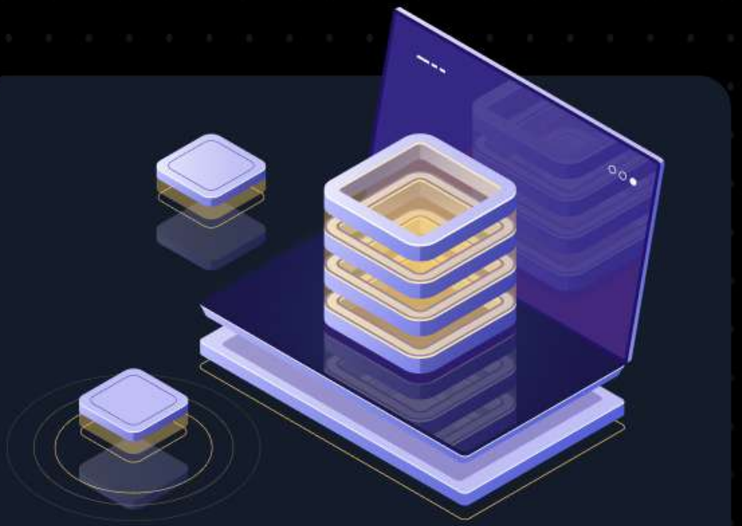
Сканирование DNS

Высокий:

- Обнаружение захвата поддоменов Azure (azure-takeover-detection.yaml
- Обнаружение захвата поддоменов на Amazon Elastic Beanstalk (elasticbeanstalk-takeover.yaml
- Обнаружение "свисающих" CNAME-записей (detect-dangling-cname.yaml)
- **~ 400** Обнаружение уязвимостей DNS Rebinding (dns-rebinding.yaml)
- **~90** Обнаружение

Средний:

- **~12K** Наличие и проверка DMARC-записей (защита электронной почты) (dmarc-detect.yaml)
- **~ 80** Наличие и проверка DNSSEC (расширения безопасности DNS) (dnssec-detection.yaml)
- **~20K** Обнаружение и проверка SPF-записей (spf-record-detect.yaml)
- **~8K** Использование WAF (Web Application Firewall) на уровне DNS (dns-waf-detect.yaml)



Низкий:

- **~31K** Обнаружение хостов с отказом в обслуживании (SERVFAIL/REFUSED) (servfail-refused-hosts.yaml)

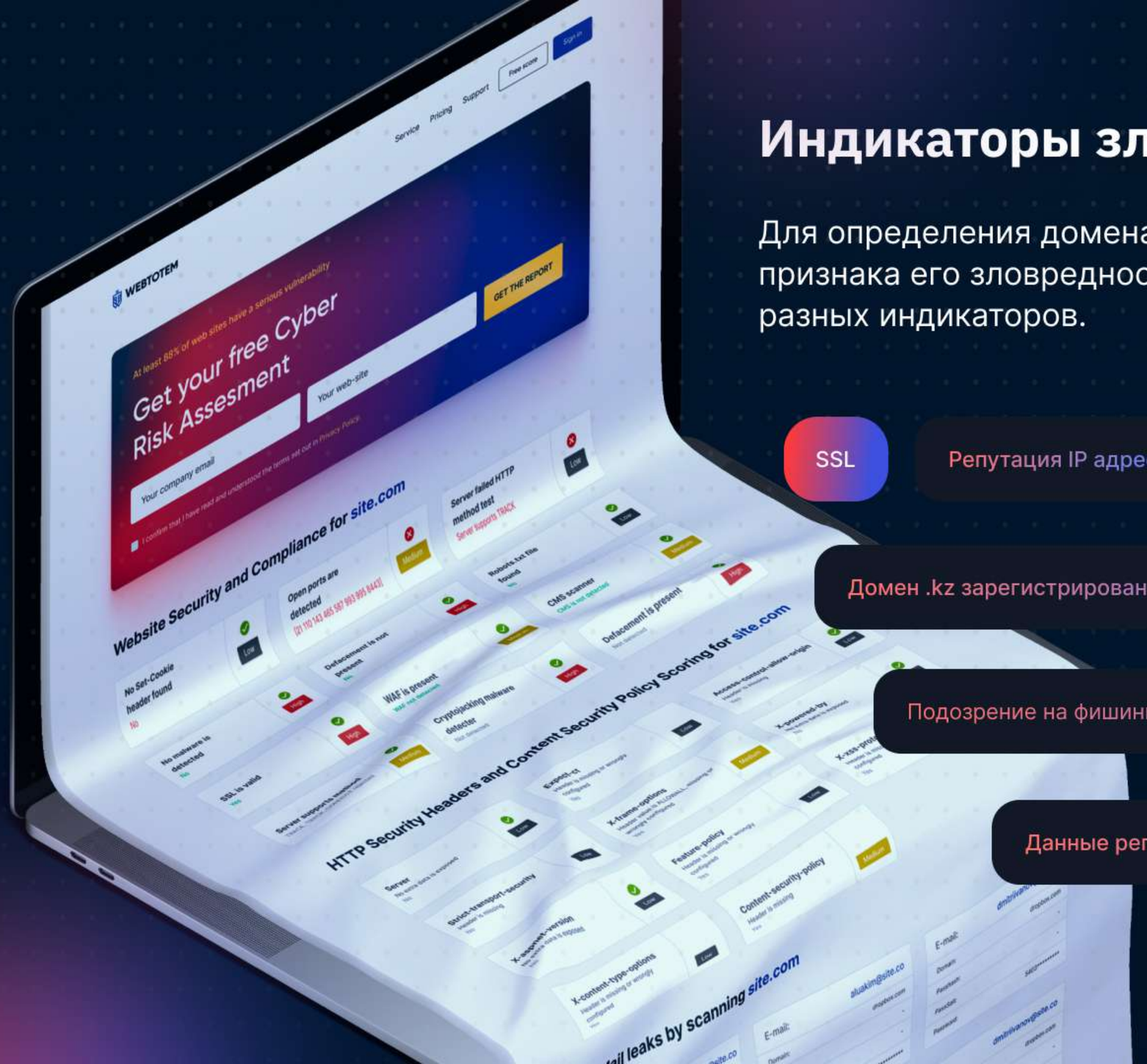
Сканирование DNS

Информативный

- ~20K Анализ CAA-записей (сертификаты безопасности) (caa-fingerprint.yaml)
- Обнаружение записей BIMI (логотипы в электронной почте) (bimi-detect.yaml)
- Обнаружение SOA-записей (начальные записи авторизации) (soa-detect.yaml)
- Обнаружение SaaS-сервисов через DNS (dns-saas-service-detection.yaml)
- Определение NS-серверов (серверов имён) (nameserver-fingerprint.yaml)
- Обнаружение почтовых сервисов по MX-записям (mx-service-detector.yaml)
- Обнаружение почтовых сервисов по MX-записям (mx-service-detector.yaml)
- Обнаружение сервисов на Amazon EC2 (ec2-detection.yaml)
- Анализ MX-записей (почтовые серверы) (mx-fingerprint.yaml)
- Определение NS-серверов (серверов имён) (nameserver-fingerprint.yaml)
- Анализ PTR-записей (обратные DNS-записи) (ptr-fingerprint.yaml)
- Анализ TXT-записей (дополнительная информация в DNS) (txt-fingerprint.yaml)
- Обнаружение сервисов через TXT-записи (txt-service-detect.yaml)
- Обнаружение рабочих сайтов (веб-ресурсов) (worksites-detection.yaml)

Наиболее распространенный
WAF на уровне DNS

Cloudflare – Около
6K веб-сайтов



Индикаторы зловредности домена

Для определения домена как зловредного, не имея явного признака его зловредности, мы рассматриваем комбинации разных индикаторов.

SSL

Репутация IP адреса

Дата регистрации домена

Домен .kz зарегистрирован на иностранца

Сканирование DNS записей

Подозрение на фишинг в результате сканирования

Наличие редиректа

Данные регистранта совпадают с данными домена из серого списка

Domain

Отдельное внимание уделяется противодействию фишинговым сайтам

- Дата регистрации домена
- Наличие или отсутствие SSL сертификата
- Phishing campaign - Сайт проверяется по ряду причин на фишинг.
- Определение редиректа на другие домены
- Результаты сканирования сторонних антивирусов.
- DNS-атака, при которой мошенник подменяет значения DNS-сервера и перенаправляет запросы на зловредный сайт.

При обнаружении комбинаций индикаторов потенциально зловредных доменов, данные интернет-ресурсы проходят дополнительные проверки

- Typo squatting
- Subdomain check
- Контент сайта
- Анализ скачиваемых файлов (антивирус)
- Сканирование линков, куда они ведут и что за ними стоит
- Проверка на вредоносные технологии, например, скрипты криптоджекинга.

Спасибо за внимание!

email: truslan@wtotem.com

телефон: +7 (707) 849 - 80 - 55

веб-сайт: www.wtotem.com

Перейдите по QR-коду, чтобы связаться с нами в Telegram.