

Установление владельцев, администраторов и разработчиков веб-ресурсов

БЕДЕРОВ Игорь Сергеевич

T.Hunter

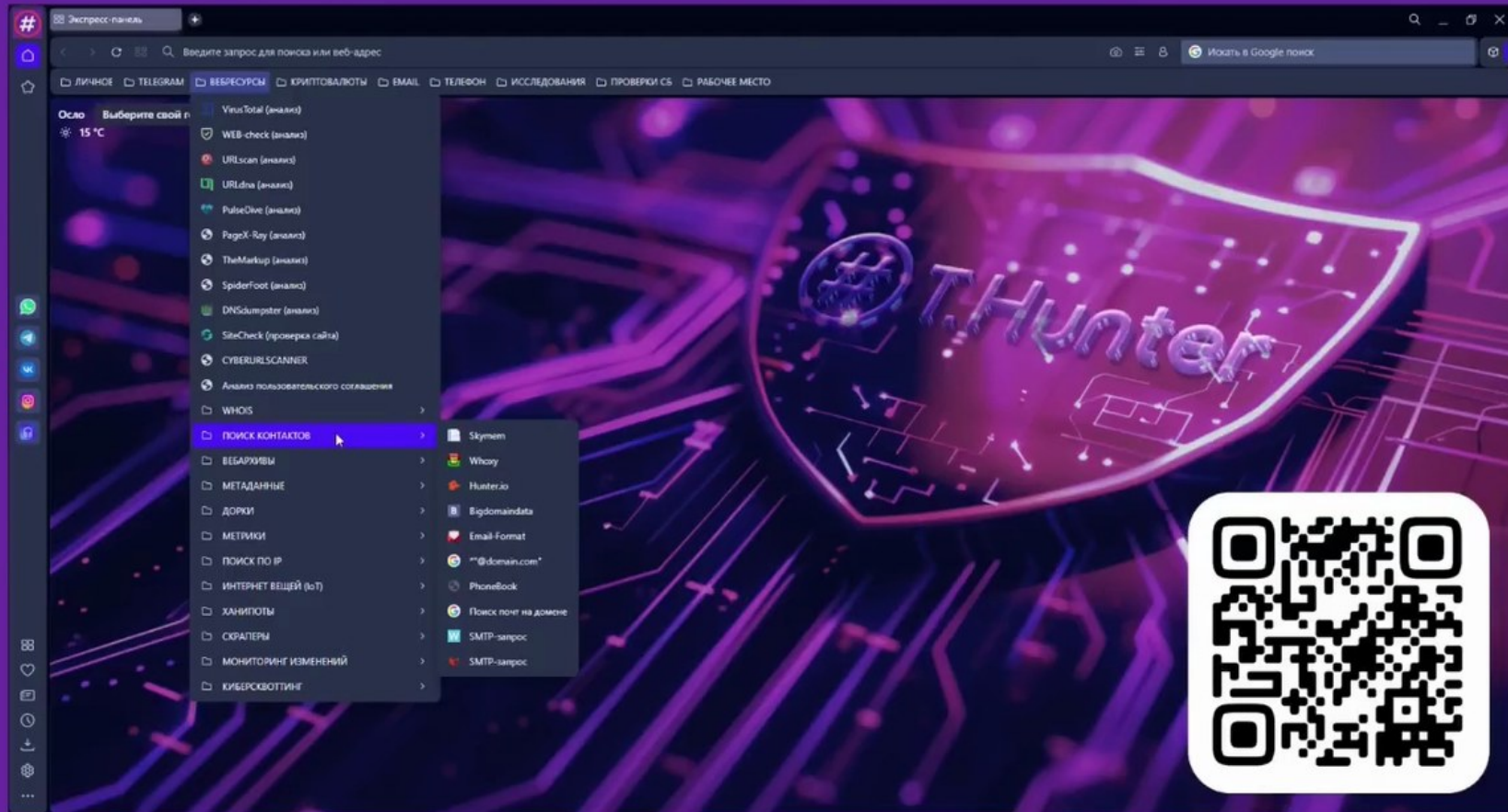


Кого мы ищем?



- # **ВЛАДЕЛЕЦ** (Owner) — юридическое или физическое лицо, на которое официально зарегистрированы доменное имя и хостинг.
- # **АДМИНИСТРАТОР** (Administrator или Webmaster) — специалист или группа специалистов, отвечающие за ежедневную работу сайта.
- # **РАЗРАБОТЧИК** (Developer) — программист или команда программистов, создающие и дорабатывающие техническую часть сайта.







Домен и данные WHOIS



ДОМЕННОЕ ИМЯ (домен) — уникальный адрес сайта в интернете, по которому пользователи могут найти ресурс.

WHOIS — это общедоступная БД и сетевой протокол, который предоставляет информацию о регистрации доменных имен, IP-адресов и автономных систем.



Архив WHOIS



- whoishistory.ru
- whoxy.com
- virustotal.com
- osint.sh/whoishistory/
- drs.whoisxmlapi.com/whois-history
- bigdomaindata.com

Историческая информация о доменных именах и IP-адресах, хранящаяся в специальных сервисах, которые отслеживают изменения в данных о владельцах, регистраторах, сроках регистрации и других характеристиках доменов с момента их первой регистрации.



Из актуального про домены...



ВЕБ-РЕСУРС



ДОМЕН

- intelx.io
- haveibeenpwned.com

- dnstwister.report
- dnstwist.it
- haveibeenquatted.com

ВС РФ постановил, что компании обязаны самостоятельно отслеживать и блокировать мошеннические сайты-зеркала!

ТАЙПСКВОТТИНГ — это вид киберсквоттинга, при котором регистрируются доменные имена, похожие на адреса популярных сайтов, чтобы перехватить пользователей, допустивших ошибку при вводе адреса в браузере.



Хостинг



ХОСТИНГ — услуга по размещению сайта на сервере, который постоянно подключён к интернету.

Фактически, хостинг — это аренда пространства на сервере, где хранятся все данные сайта: тексты, изображения, коды и т.д. Хостинг обеспечивает постоянный доступ к сайту через интернет, позволяя пользователям заходить на сайт в любое время.

- urlscan.io
- web-check.xyz
- pulsedive.com
- virustotal.com

- `"cmd" + "ping example.com"`

ХОСТИНГ



ВЕБ-РЕСУРС



Обход защиты CloudFlare



Cloudflare — это американская компания и глобальная сеть серверов, предоставляющая услуги для защиты, ускорения и оптимизации работы интернет-ресурсов.

- urlscan.io (в случае индексации до включения CloudFlare)
- virustotal.com (см. вкладку "relations")
- webresolver.nl и skypeipresolver.net (утечки баз данных CloudFlare)
- dnsdumpster.com и pulsedive.com (просмотр записей DNS)
- анализ SSL-сертификата и хэш favicon

CLOUDFLARE ← ХОСТИНГ
ОБХОД ЗАЩИТЫ



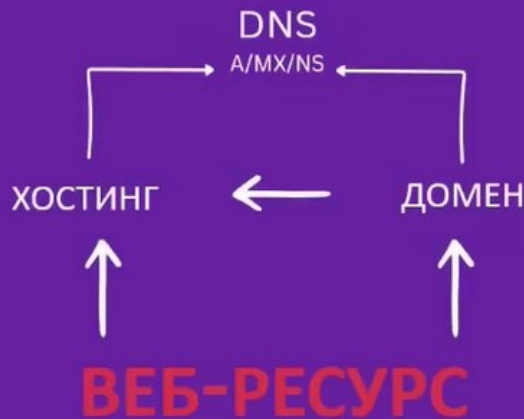
ВЕБ-РЕСУРС



DNS-записи



- [dnsdumpster.com](https://dnstool.net/dnsdumpster.com)
- ru.hostadvice.com/tools/whois/
- hackertarget.com/dns-lookup/



Domain Name System — система доменных имен.

NS-запись — главный тип, определяющий адреса DNS-серверов, обслуживающих домен.

A-запись — привязывает доменное имя на один адрес **IPv4** (**AAAA** — для **IPv6**)

CNAME — указывает, что данный домен выполняет функции псевдонима (алиаса) другого домена.

MX-запись — указывает имя почтового сервера.

TXT-запись — используется для хранения произвольной информации в DNS.

SOA-запись — содержит прочую информацию.



SSL и Favicon



- shodan.io
- zoomeye.hk
- search.censys.io
- greynoise.io
- fofa.info



SSL-СЕРТИФИКАТ (Secure Sockets Layer) — цифровой сертификат, который обеспечивает шифрованное соединение между сайтом и браузером с помощью SSL-протокола.

ФАВИКОН (Favicon) — это иконка веб-сайта или отдельной страницы. Название образовано от английских слов favorite icon, что дословно переводится как «иконка из избранного».



Связанные контакты



- hunter.io
- email-format.com
- skymem.info
- findemail.io
- bigdomaindata.com
- whoxy.com

В качестве метода выявления контактов может быть использован и простой **ПОДБОР** типичных никнеймов (office, contact, admin, support, info, hr, pr) с исследуемым доменным именем и последующей проверкой при помощи SMTP-запроса к почтовому серверу.



Файлы и их метаданные



ВЕБ-РЕСУРС

- virustotal.com

- jimpl.com
- metadata2go.com



ФАЙЛЫ



МЕТАДАННЫЕ

- domain.com/sitemap.xml
- site:domain.com filetype:xls | filetype:csv | filetype:doc | filetype:pdf | filetype:txt

МЕТАДАННЫЕ ФАЙЛА — это дополнительная информация, которая описывает содержание файла, его технические характеристики, историю создания, авторство, условия доступа и другие атрибуты, облегчая его поиск и понимание для людей и для программных систем.



Гиперссылки (URL)



- domain.com/robots.txt
- domain.com/sitemap.xml

ГИПЕРССЫЛКИ

ВНУТРЕННИЕ (СКРЫТЫЕ РАЗДЕЛЫ)
ВНЕШНИЕ (СОЦСЕТИ, ХРАНИЛИЩА)



ВЕБ-РЕСУРС

- urlscan.io
- web-check.xyz
- virustotal.com

ВНУТРЕННИЕ гиперссылки могут указывать на скрытые разделы веб-ресурса, представляющие определенный интерес для исследования. **ВНЕШНИЕ** — вести на связанные социальные сети, блоги, а также файлообменники.



Встроенные технологии



- metrika.yandex.ru/dashboard?id=
- top100.rambler.ru/search?query=
- top.mail.ru/visits?id=
- yandex.ru/support/metrika/
- osint.sh/analytics/ (UA)
- publicwww.com (UA)

ТЕХНОЛОГИИ

РЕКЛАМНЫЕ ИДЕНТИФИКАТОРЫ
МЕТРИКИ, ВСТРЕННЫЕ ЧАТЫ
БАНКОВСКИЕ ЭКВАЙРИНГИ
ЭЛЕМЕНТЫ КОДА

- urlscan.io
- web-check.xyz
- virustotal.com

ВЕБ-РЕСУРС





Архивные копии веб-ресурса



ВЕБ-РЕСУРС



АРХИВНЫЕ КОПИИ ВЕБ-РЕСУРСА

- archive.org
- archive.md
- web-arhive.ru

ГИПЕРССЫЛКИ



КОНТАКТЫ



ТЕХНОЛОГИИ



ФАЙЛЫ





Внешний трафик



- ya.ru
- google.com
- kribrum.io
- telemetr.me
- vk.com

ВЕБ-РЕСУРС



ВНЕШНИЙ ТРАФИК



Внешний трафик на веб-ресурс часто может быть связан с SMM (раскруткой в социальных медиа). Это позволяет переходить в своем исследовании к изучению конкретных профилей и социальных сообществ, которые “рекламировали” веб-ресурс.

Особенную актуальность метод приобрел при исследовании размещения и последующей раскрутки фейковых петиций через такие порталы, как **CHANGE.ORG**.



Обобщим план исследования...





Полезные инструменты



АНАЛИТИЧЕСКИЕ СЕРВИСЫ:

- urlscan.io
- web-check.xyz
- pulsedive.com
- virustotal.com

УПОМИНАНИЯ:

- google.com
- kribrum.io
- telemetr.me
- vk.com

ПОИСК КОНТАКТОВ:

- hunter.io
- skymem.info
- findemail.io
- bigdomaindata.com

WHOIS / DNS:

- whois.domaintools.com
- reg.ru/whois/
- dnscumster.com

ВЕБАРХИВЫ:

- archive.org
- archive.md
- web-arhive.ru

ПРОЧЕЕ:

- metadata2go.com

РАСШИРЕННЫЕ ОПЕРАТОРЫ ПОИСКА GOOGLE:

- domain.com/robots.txt / domain.com/sitemap.xml
- site:domain.com filetype:xls (csv, doc, pdf, txt, ppt, log)