



Поиск владельцев веб-сайтов

Докладчик: @osinterka

Что ищем?

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



Электронную почту



Телефон



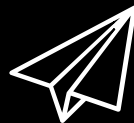
Ключевые слова



Метаданные



Страницы/группы в
социальных сетях



Telegram аккаунты и
возможные юзернеймы



ФИО / др. контактная
информация



WHOIS



Веб-архив



Дорки



Анализ
веб-сайта

- ФИО
- Электронная почта
- Номер телефона
- Организация
- Дополнительные ресурсы
- Метаданные



who is — кто это

позволяет узнать основные сведения о доменном имени и его владельце

- person - ФИО
- e-mail - электронная почта
- phone - номер телефона
- org – организация
- city, street – адрес
- created – дата создания доменного имени
- admin-contact – связь с администратором
- ip - IP-адрес сервера

```
domain: TS [REDACTED] IP.SU
nserver: ns1.reg.ru.
nserver: ns2.reg.ru.
state: REGISTERED, DELEGATED
person: Private Person
e-mail: ale [REDACTED]@mail.ru
registrar: REGRU-SU
created: 2021-08-18T09:02:41Z
paid-till: 2023-08-18T09:02:41Z
free-date: 2023-09-20
source: TCI
```

пример данных whois

Инструменты #1. WHOIS сервисы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



2



2IP – 2ip.ru/whois (+поиск доменов владельца)



Domain Tools – whois.domaintools.com (+информация об изменениях на домене)



BULK SEO TOOLS – bulkseotools.com/bulk-whois-lookup.php (+массовый поиск до 500 доменов)



WhoisHistory – whoishistory.ru , backorder.ru (+история whois)





Reversewhois.io – Обратный поиск Whois по почте/имени

Инструменты #1. WHOIS сервисы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



Domain Tools - whois.domaintools.com

Статус регистратора	ЗАРЕГИСТРИРОВАН,		
Даты	5 дней		↗
	Создано 16.07.2023		
	Истекает 16.07.2024		
Серверы имен	ЯНТАРЬ.NS.CLOUDFLARE.COM. (имеет 25 482 936 доменов) RANDY.NS.CLOUDFLARE.COM. (имеет 25 482 936 доменов)		↗
Айпи адрес	104.	251 – 782 других сайта, размещенных на этом сервере.	↗
IP-адрес	 - Калифорния - Сан-Хосе - Cloudflare Inc.		
ASN	 AS13335 CLOUDFLARENET, США (зарегистрирован 14 июля 2010 г.)		
История IP	2 изменения на 2 уникальных IP-адреса за 0 лет		↗
История хостинга	5 изменений на 3 уникальных серверах имён за 1 год		↗

Инструменты #1. WHOIS сервисы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



BULK SEO TOOLS – bulkseotools.com/bulk-whois-lookup.php

Domain Name	Registrar	Date Created	Date Expires	Owner Name	Owner Address	Owner Email	Owner Phone	Nameserver
healt[redacted]u	RUCENTER-REG-RIPN	2020-11-20	2023-11-20	null		anton[redacted].ru;	+7[redacted];;	null
group[redacted].su	RUCENTER-REG-RIPN	2021-08-18	2023-08-18	null		[redacted]7ck@mail.ru;	+7[redacted]80;;	ns1.reg.ru; ns2.reg.ru;
c[redacted]ver.ru	RUCENTER-REG-RIPN	2023-07-19	2024-07-19	null	null		;	ns1.gohost.ru; ns2.gohost.ru;
creativ[redacted]irs.ru	RUCENTER-REG-RIPN	2023-07-19	2024-07-19	null	null		;	ns5.hosting.reg.ru; ; ns6.hosting.reg.ru; ;
c[redacted]stylist.ru	RUCENTER-REG-RIPN	2023-07-19	2024-07-19	null	null		;	ns1.beget.com; ns1.beget.pro; ns2.beget.com; ns2.beget.pro;

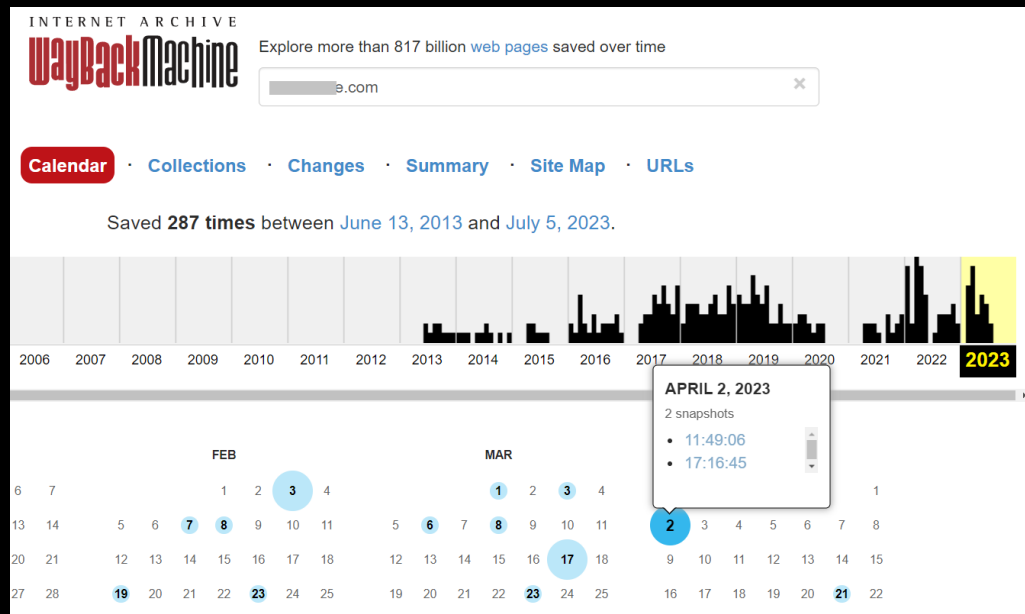


История whois - whoishistory.ru , backorder.ru

	person:	Private Person
	registrar:	REGRU-RU
	admin-contact:	http://www.reg.ru/whois/admin_contact
	created:	2021-11-02 10:59:37
	paid-till:	2022-11-02 10:59:37
	free-date:	2022-12-03
	source:	TCI
	org:	JSC
	inn:	7716
	org-ru:	AO C пов
с 2021-11-02 11:01:30 по 2021-11-02 11:16:31		
	domain:	osa u
	nserver:	ns1.hosting.reg.ru.
	nserver:	ns2.hosting.reg.ru.
	state:	REGISTERED, DELEGATED, UNVERIFIED
	org:	JSC Sy rs
	registrar:	REGRU-RU
	admin-contact:	http://www.reg.ru/whois/admin_contact
	created:	2021-11-02 10:59:37
	paid-till:	2022-11-02 10:59:37
	free-date:	2022-12-03
	source:	TCI
	inn:	771
	org-ru:	AO тров
УСЛОВНЫЕ ОБОЗНАЧЕНИЯ		
Измененные поля		
Добавленные поля		
Удаленные поля		

Инструменты #1. Веб-архивы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



	Captures	URLs	New URLs
text/html	14 939	4 092	2 124
image/jpeg	1 967	1 175	801
image/png	1 273	511	201
text/css	733	310	228
application/javascript			
image/gif			
application/pdf			
image/svg+xml			
image/vnd.microsoft.icon			
video/mp4			

URL ↑
http://y.com:80/
https://ify.com/.well-known/assetlinks.json
https://ify.com/.well-known/gpc.json
https://ify.com/.well-known/shopify/monorail/unstable
https://ify.com/26800947253/checkouts/cc2d9a74ae6906ee
https://ify.com/26800947253/digital_wallets/dialog
https://ify.com/account
https://ify.com/account/login
https://ify.com/account/login?return_url=%2Faccount

● archive.org/web

● archive.ph

● timetravel.mementoweb.org

● web-arhive.ru

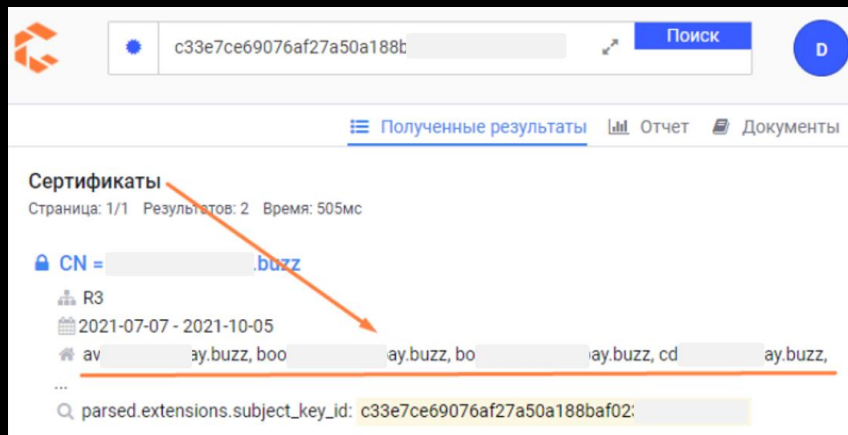
● Яндекс кэш

● Кэш Google - cache:domain.com

Инструменты #1. Анализ веб-сайта

Поиск поддоменов сайта

- <https://osint.sh/subdomain/>
- <https://otx.alienvault.com/indicator/>
- <https://www.virustotal.com/gui/home/search>
- Дорки. site:domain.com
- Поиск по сертификату



Search results for certificate ID: c33e7ce69076af27a50a188b

Сертификаты

Страница: 1/1 Результаты: 2 Время: 505мс

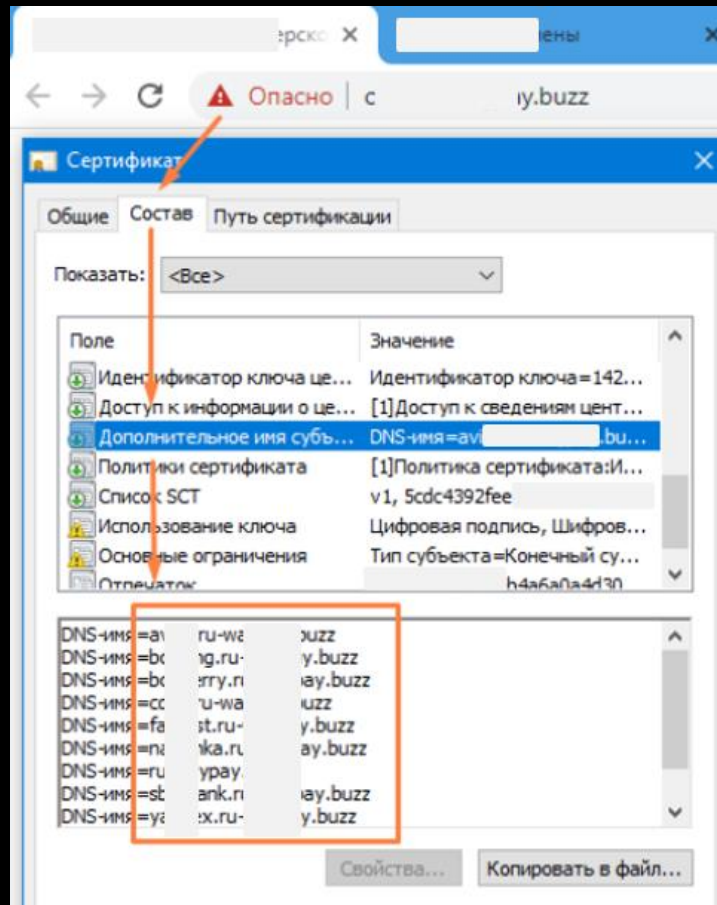
🔒 CN = ay.buzz

R3

2021-07-07 - 2021-10-05

ay.buzz, boo ay.buzz, bo ay.buzz, cd ay.buzz,

parsed.extensions.subject_key_id: c33e7ce69076af27a50a188baf02:



Опасно | ay.buzz

Сертификат

Общие Состав Путь сертификации

Показать: <Все>

Поле	Значение
Идентификатор ключа це...	Идентификатор ключа=142...
Доступ к информации о це...	[1]Доступ к сведениям цент...
Дополнительное имя субь...	DNS-имя=ay.buzz
Политики сертификата	[1]Политика сертификата:И...
Список SCT	v1, 5cdc4392fee
Использование ключа	Цифровая подпись, Шифров...
Основные ограничения	Тип субъекта=Конечный су...
Отпечаток	h4a6a0a4d30

DNS-имя	ru-wa	uzz
DNS-имя=bx	rg.ru-	y.buzz
DNS-имя=bx	rg.ru-	ay.buzz
DNS-имя=cc	'u-wa	uzz
DNS-имя=fa	st.ru-	y.buzz
DNS-имя=fx	ika.ru	ay.buzz
DNS-имя=ru	ypay.	ay.buzz
DNS-имя=st	ank.n	ay.buzz
DNS-имя=yi	ix.ru-	y.buzz

Свойства... Копировать в файл...



Инструменты #1. Анализ веб-сайта



- **Анализ HTML-кода** - поиск дополнительных страниц и закомментированных строк
 - **<https://letsearch.ru/>** - поиск русскоязычных сайтов по заголовку, описанию, ключевым словам и html-коду
 - **Поиск по картинке** в поисковых системах
-

используем дорки

получаем

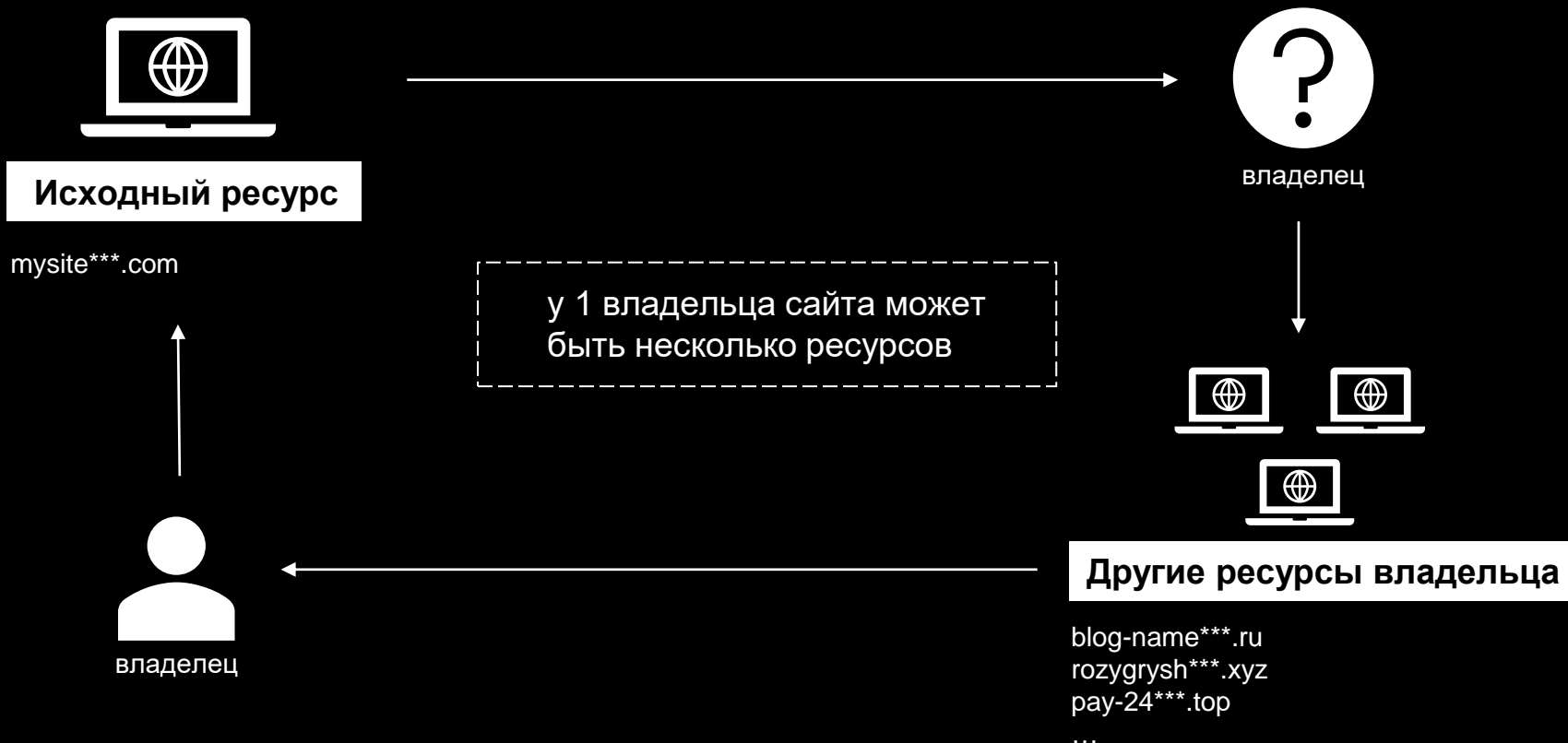
- `site:domain.com` → URL-страницы ресурса и поддомены
- кавычки ("`domain.com`") → упоминания на форумах и в соц.сетях
- ключевые слова и фразы со страницы → новые доменные имена



**Но что делать
когда данных для анализа недостаточно?**

Поиск других ресурсов владельца

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka

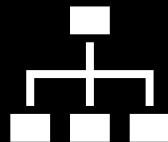


Поиск других ресурсов владельца

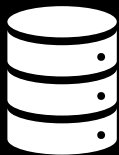
Инструменты #2



Доменные имена



IP-адреса



Системные файлы
и идентификаторы



Социальная
инженерия

Цели создания новых ресурсов:

- мошенническая деятельность
- разные виды проектов
- продвижение ресурсов
- сокрытие негативных отзывов о проекте

Инструменты #2. Доменные имена

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



Проверка по всем доменным зонам

<https://osint.sh/domain/>

No	Domain	Registrar	Created	Owner	Address	Email	Phone
1	lhabrahabr.top	Alpnames Limited	2016-01-14	Wolf	Krasn 29	ppaccx@y	... 7968 4
2	lhabrahabr.mobi	EvoPlus Ltd.	2016-11-03	WhoisProtectSe...	Agios Fylaxeos 6...	habrahabr	i... +357 35
3	lhabrahabr.org	!#No1Registrar, ...	2016-12-22	Domain Manager	Flat No. 48 Cunn...	samirnet2	а... +91.8 40
4	lhabrahabr.tech	Regional Networ...	2018-01-31	JSC "Habrahabr"	Spartakovsky la...	info@tmtr	+7.49 61
5	lhabrahabr.info	Beartrapdomain...	2021-05-14	REDACTED FOR ...	REDACTED FOR ...	please que	... REDA OR ...
6	lhabrahabra.com	NameKing.com I...	2011-10-04	DOMAIN MAY B...	Ramon Arias Av...	admin@w	... +507 9

Инструменты #2. Доменные имена

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



Поиск схожих доменных имен

<https://suip.biz/ru/?act=urlcrazy>

Type	Type	Typo	Pop	DNS-A	CC-A	DNS-MX	Extn
Character Omission		facbook.com		157.240.205.1	US,UNITED STATES		com
Character Omission		facebok.com		157.240.205.1	US,UNITED STATES		com
Character Omission		faceboo.com		157.240.205.1	US,UNITED STATES		com
Character Omission		facebook.cm		103.224.182.239		park-mx.above.com	cm
Character Omission		faceook.com		157.240.205.1	US,UNITED STATES		com
Character Omission		faebook.com		157.240.205.1	US,UNITED STATES		com
Character Omission		fcebook.com		157.240.205.1	US,UNITED STATES		com
Character Repeat		faacebook.com		157.240.205.1	US,UNITED STATES		com
Character Repeat		facecebook.com		157.240.205.1	US,UNITED STATES		com
Character Repeat		facebbbook.com		157.240.205.1	US,UNITED STATES		com
Character Repeat		facebookk.com			?		com
Character Repeat		faceboook.com		157.240.205.1	US,UNITED STATES		com
Character Repeat		faceebook.com		157.240.205.1	US,UNITED STATES		com
Character Repeat		ffacebook.com		157.240.205.1	US,UNITED STATES		com
Character Swap		afcebook.com			?		com
Character Swap		facbeook.com			?		com
Character Swap		faceboko.com		199.59.243.224			com
Character Swap		faceobok.com		157.240.205.1	US,UNITED STATES		com
Character Swap		faecbook.com			?		com

Инструменты #2. Доменные имена

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



Поиск схожих доменных имен и анализ их даты регистрации

Домены RU, зарегистрированные 20 июля 2023 - 21 июля 2023

Всего найдено 4340 доменов, показаны 1 - 100

	Домен
74)	7DOMIKOV.ru
75)	833CARGO.ru
76)	9645793387.ru
77)	9645793396.ru
78)	9645793410.ru
79)	9645793416.ru
80)	9645793419.ru
81)	9645793422.ru
82)	9645793445.ru
83)	9645793446.ru
84)	9645793447.ru
85)	9645793448.ru
86)	9645793453.ru
87)	9645793458.ru
88)	9645793460.ru
89)	9645793463.ru
90)	9819981.ru
91)	989CARGO.ru

<https://domains.ihead.ru/domains/>
поиск доменов по зонам RU, SU, РФ

2IP – ресурсы одного владельца поиск по домену или эл.почте

Все домены одного владельца

Хотите узнать, какие и сколько доменов принадлежит одному человеку? Теперь это не сложно. Введите в поле ниже один из доменов, принадлежащих человеку или его email адрес и вы получите желаемое.

На данный момент сервис знает только домены в зоне *.ru и *.rf

Е-mail или
домен:

Поиск

<https://2ip.ru/domain-list-by-email/>
поиск по зонам RU и РФ

Инструменты #2. IP-адреса

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



Анализ IP-адреса

SecurityTrails	
A Recorded Future Company	
87.236.16.254	
Domain	Hosting Provider
nexplorer.ru	Beget LLC
tele-taxi.ru	Beget LLC
inna-pro-style.com	Beget LLC
cardioneurology.ru	Beget LLC
zealstep.ru	Beget LLC
unescospb.ru	Beget LLC
fckuban.com	Beget LLC

<https://securitytrails.com/>

Ресурсы поблизости

sites on IP-addresses nearby:

87.236.16.121	0-	u.w
87.236.16.127	ad	l.ru w
87.236.16.129	m	ink.com w
87.236.16.135	b2	i.w, readme.ru w
87.236.16.137	fu	.ru w
87.236.16.148	w	ap-com.ru w
87.236.16.151	et	ty.ru w
87.236.16.167	m	l-res.ru w
87.236.16.169	m	ell.com w
87.236.16.193	is	a.pro w
87.236.16.204	ss	ock.beget.com w, m, on.su w
87.236.16.207	w	edia.tj w
87.236.16.214	te	.com w
87.236.16.217	pc	a-platit.site w
87.236.16.228	tg	.me w
87.236.16.230	ku	x.ru w
87.236.16.233	as	urm.tj w

<https://atsameip.intercode.ca/>

Инструменты #2.

Системные файлы и идентификаторы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



<https://urlscan.io/>

117 HTTP transactions

1 data transactions

Everything HTML Script AJAX CSS Image Expand all

Method	Resource	Size	Time	Type	IP
Protocol	Status Path	x-fer	Latency	MIME-Type	Location
GET H2	200 Primary Request / waa...up.com/	76 KB 14 KB	978ms 581ms	Document text/html	68.65.123.184 NAMECHEAP-NET
GET H2	200 style.min.css waa...up.com/wp-includes/css/dist/block-library/	95 KB 12 KB	188ms 185ms	Stylesheet text/css	68.65.123.184 NAMECHEAP-NET
GET H2	200 classic-themes.min.css waa...up.com/wp-includes/css/	291 B 490 B	192ms 187ms	Stylesheet text/css	68.65.123.184 NAMECHEAP-NET
GET H2	200 styles.css waa...up.com/wp-content/plugins/contact-form-7/includes/css/	3 KB 1 KB	372ms 368ms	Stylesheet text/css	68.65.123.184 NAMECHEAP-NET
GET H2	200 sfsi-style.css waa...up.com/wp-content/plugins/ultimate-social-media-icons/css/	73 KB 11 KB	373ms 369ms	Stylesheet text/css	68.65.123.184 NAMECHEAP-NET
GET H2	200 style.css waa...up.com/wp-content/themes/greennature/	114 KB 17 KB	373ms 370ms	Stylesheet text/css	68.65.123.184 NAMECHEAP-NET

Инструменты #2.

Системные файлы и идентификаторы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



<https://analyzeid.com/>

Find websites owned by inna style.com

Search table

Export

Columns

Send feedback

Confidence↕	Domain↕	Adsense↕	Google Analytics↕	Ip↕	Nameserver↕	Registrar↕
	<input type="text" value="Search column"/>	<input type="text" value="Search column"/>	<input type="text" value="Search column"/>	<input type="text" value="Search column"/>	<input type="text" value="Search column"/>	<input type="text" value="Search column"/>
132%	inna style.com			87.236.16.254		
12%	hay.ru	ca-pub-9058932478815599 ca-pub-5752527393443410	UA-141797423	87.236.16.91 87.236.16.254 172.67.163.122		
12%	game-.ru	ca-pub-9058932478815599 ca-pub-5484094047076379	UA-141797423 UA-106746416	87.236.16.91 87.236.16.254		

Инструменты #2.

Системные файлы и идентификаторы



Ресурсы для разработчиков



GitHub – поиск на сайте + дорки



Pastebin – через дорки



Postman – через дорки

Инструменты #2.

Системные файлы и идентификаторы

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



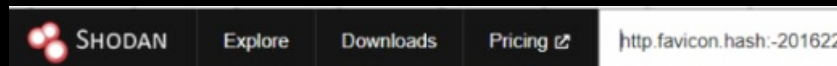
Поиск по favicon - значок веб-сайта, который отображается во вкладке перед названием страницы



Поисковики



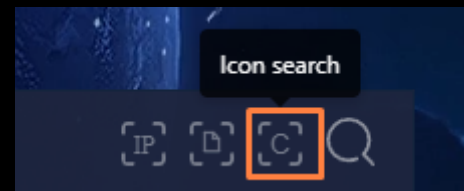
shodan.io



Пример: `http.favicon.hash:-201622***`



zoomeye.org



Поиск по картинке

Инструменты #2. Социальная инженерия



Связаться с администратором ресурса – через регистратора/хостера (WHOIS)

- admin-contact – если хотим связаться с админом (через форму у регистратора)
- почта abuse@ – когда пишем регулятору и просим передать наше обращение

Сделать попытку платежа (без дальнейшей оплаты)

- при наличии: проверить наименование мерчанта / адрес площадки в СМС

Canary Tokens – для получения новых идентификаторов или проверки взаимосвязи

Заблокировать ресурс (если фишинг)

- направить запрос в компетентную организацию (<https://cctld.ru/help/safety/competent/>)

Поиск владельцев веб-сайтов.

Подтверждаем догадки

OSINT mindset meetup #11
Поиск владельцев веб-сайтов
@osinterka



@telesint_bot (https://t.me/telesint_bot)

позволяет найти группы Telegram
в которых состоит пользователь

Открытые группы:

[@gmbing](#) Арбитраж Беттинга и Гэмблинга
[@gamblingaff](#) Gambling Affiliates SEO Chat
[@d_conf](#) d-conf
[@seo_burzh_chat](#) SEO БУРЖ chat
[@a_parser](#) A-Parser - парсер для SEO,
маркетологов, арбитражников и SaaS систем
[@betting_gambling](#) Betting & Gambling
[@wmsnchat](#) wmsn чат

Открытые группы [17]:

[@chat_drop](#) Поиск товара Дроп | Опт
Поставщики
[@prlike1](#) Бесплатная реклама и пиар каналов
[@topcasino119](#) Кракен казино
[@javaprogrammingchat](#) Java Programming Chat
[@zarabotoka](#) заработок онлайн чат
[@chechen_chat](#) Вай чат
[@dealersmafia](#) Facebook from AD
[@advertiseru](#) Advertise | Ru
[@tong_shop](#) tongShop | Padarka Sovgalar
Podarkalar Aksiya SEVISHGANLAR 8 MART UCHUN
PODARKA
[@sukalosina](#) Подвал чечни Chat
[@moneymakers_bets_chat](#) Ставки манимейкера
[@fathers_of_traffic](#) Отцы Трафика - Арбитраж
[@protrafficcom](#) Чат ProTraffic - Арбитраж
трафика
[@negrochat](#) NEGROCHAT OFFICIAL
[@sim_sim_sim_sim_sim](#) НА СВЯЗИ
[@piar_kanal](#) Пиар канал

The End

СПАСИБО. ВОПРОСЫ?



<https://t.me/osinterka>



https://t.me/osint_mindset



<https://t.me/+smhN69qD2mkxMTEy>