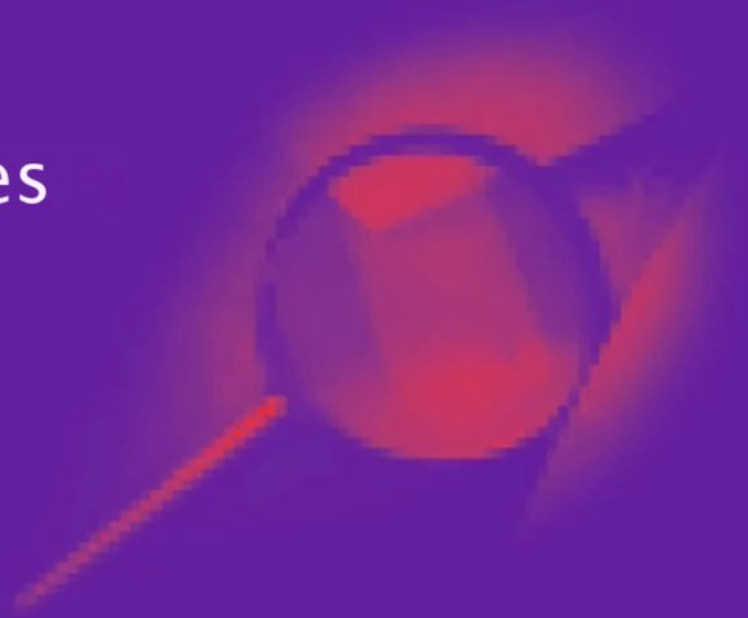
Identifying the owners, administrators and developers of web resources



BEDEROV Igor Sergeevich

T.Hunter

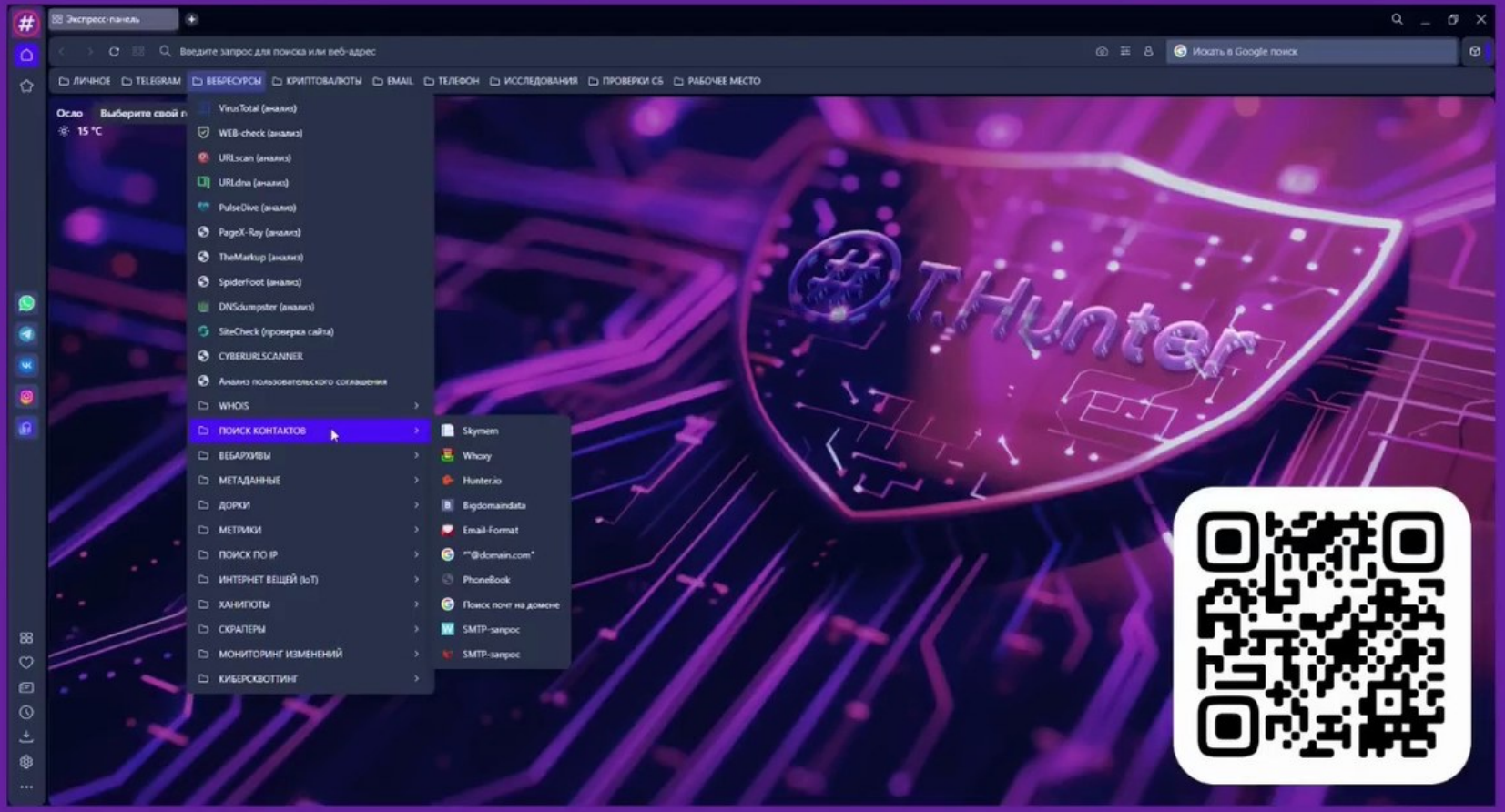
Who are we looking for?

OWNER — the legal entity or individual in whose name the domain name and the hosting are officially registered.

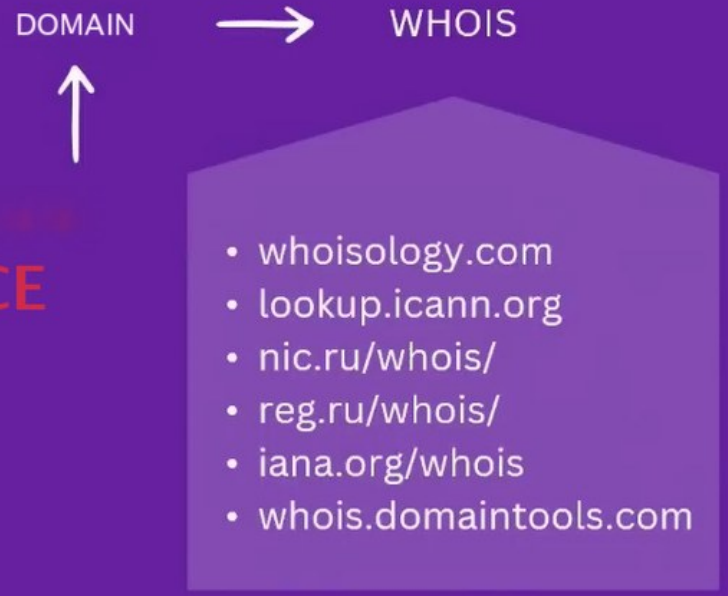
ADMINISTRATOR (or Webmaster) — the specialist or team of specialists responsible for the day-to-day running of the site.

DEVELOPER — the programmer or team of programmers who build and maintain the technical part of the site.




Экспресс-панель
Введите запрос для поиска или веб-адрес
Искать в Google поиск
ЛИЧНОЕ
TELEGRAM
ВЕБРЕСУРСЫ
КРИПТОВАЛЮТЫ
EMAIL
ТЕЛЕФОН
ИССЛЕДОВАНИЯ
ПРОВЕРКИ CS
РАБОЧЕЕ МЕСТО
Осло
15 °C
VirusTotal (анализ)
WEB-check (анализ)
URLscan (анализ)
URLdna (анализ)
PulseDive (анализ)
PageX-Ray (анализ)
TheMarkup (анализ)
SpiderFoot (анализ)
DNSdumpster (анализ)
SiteCheck (проверка сайта)
CYBERURLSCANNER
Анализ пользовательского соглашения
WHOIS
ПОИСК КОНТАКТОВ
ВЕБАРХИВЫ
МЕТАДАННЫЕ
ДОРКИ
МЕТРИКИ
ПОИСК ПО IP
ИНТЕРНЕТ ВЕЩЕЙ (IoT)
ХАНИПОТЫ
СКРАПЕРЫ
МОНИТОРИНГ ИЗМЕНЕНИЙ
КИБЕРСКВОТТИНГ
Skymem
Whoxy
Hunter.io
Bigdomaindata
Email-Format
"*@domain.com"
PhoneBook
Поиск почт на домене
SMTP-запрос
SMTP-запрос
T.Hunter

Domain and WHOIS data



DOMAIN NAME (domain) — a site's unique address on the internet by which users can find the resource.

WHOIS is a public database and network protocol that provides information on the registration of domain names, IP addresses and autonomous systems.

WHOIS archive

DOMAIN → WHOIS → WHOIS ARCHIVE

WEB RESOURCE

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

Historical information on domain names and IP addresses held by dedicated services that track changes in the data on owners, registrars, registration periods and other domain characteristics since their first registration.

Recent news on domains...

WEB RESOURCE

DOMAIN

- intelx.io
- haveibeenpwned.com

- dnstwister.report
- dnstwist.it
- haveibeensquatted.com

The Supreme Court of Russia ruled that companies must themselves detect and block fraudulent mirror sites!

TYPOSQUATTING is a form of cybersquatting in which domain names similar to the addresses of popular sites are registered in order to intercept users who mistype an address in the browser.

Hosting

HOSTING is a service for placing a site on a server that is permanently connected to the internet. In effect, hosting is the rental of space on a server where all the site's data is stored: texts, images, code and so on. Hosting provides permanent access to the site over the internet, letting users visit the site at any time.

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

- "cmd" + "ping example.com"

HOSTING



WEB RESOURCE

Bypassing CloudFlare protection

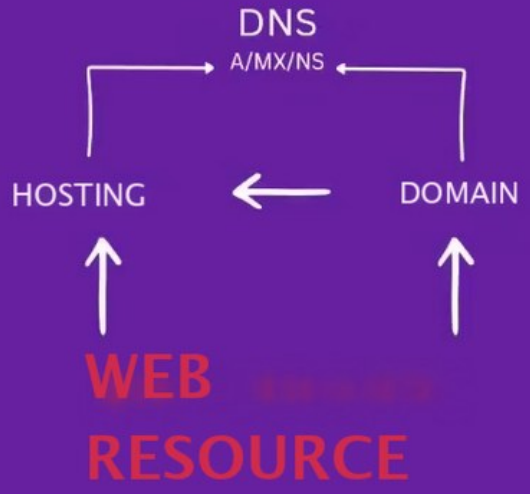
Cloudflare is an American company and a global server network providing services to protect, accelerate and optimize the operation of internet resources.

- urlscan.io (if indexed before CloudFlare was enabled)
- virustotal.com (see the "relations" tab)
- webresolver.nl and skypeipresolver.net (CloudFlare database leaks)
- dnsdumpster.com and pulsedive.com (viewing DNS records)
- SSL certificate analysis and favicon hash



DNS records

- dnsdumpster.com
- ru.hostadvice.com/tools/whois/
- hackertarget.com/dns-lookup/

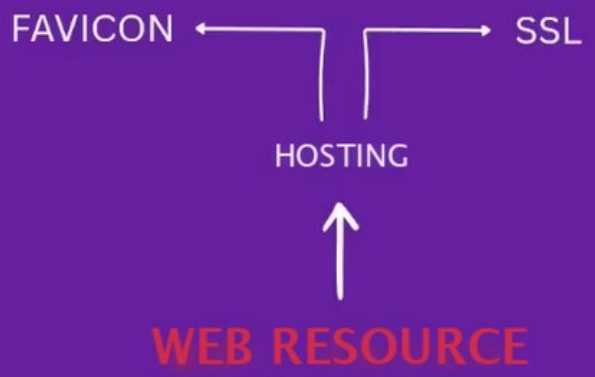


Domain Name System — the system of domain names.

NS record — the main type, defining the addresses of the DNS servers that serve the domain.
A record — binds a domain name to a single IPv4 address (AAAA — for IPv6)
CNAME — indicates that this domain acts as an alias of another domain.
MX record — specifies the name of the mail server.
TXT record — used to store arbitrary information in DNS.
SOA record — contains other information.

SSL and Favicon

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



SSL CERTIFICATE (Secure Sockets Layer) — a digital certificate that provides an encrypted connection between a site and a browser using the SSL protocol.

FAVICON — the icon of a website or of a separate page. The name comes from the English words favorite icon, literally “an icon from favorites”.

Related contacts

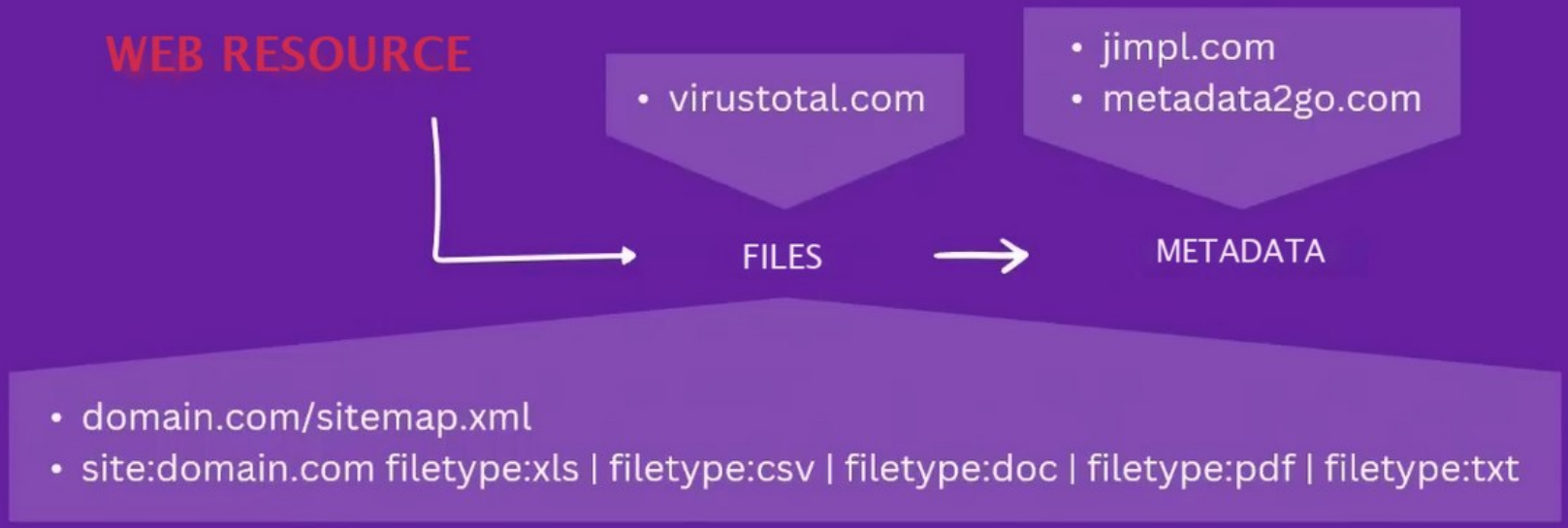


WEB RESOURCE

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

Contacts can also be identified by simple GUESSING of typical usernames (office, contact, admin, support, info, hr, pr) with the domain name under study, followed by a check via an SMTP request to the mail server.

Files and their metadata



FILE METADATA is additional information that describes the content of a file, its technical characteristics, creation history, authorship, access terms and other attributes, making it easier for people and software systems to find and understand it.

Hyperlinks (URL)

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

HYPERLINKS

INTERNAL (HIDDEN SECTIONS)

EXTERNAL (SOCIAL MEDIA, STORAGE)

WEB RESOURCE

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

INTERNAL hyperlinks can point to hidden sections of the web resource that are of particular interest for the investigation. EXTERNAL ones lead to linked social networks and blogs, as well as to file-sharing services.

Embedded technologies

- metrika.yandex.ru/dashboard?id=
- top100.rambler.ru/search?query=
- top.mail.ru/visits?id=

- yandex.ru/support/metrica/

- osint.sh/analytics/ (UA)
- publicwww.com (UA)

WEB RESOURCE

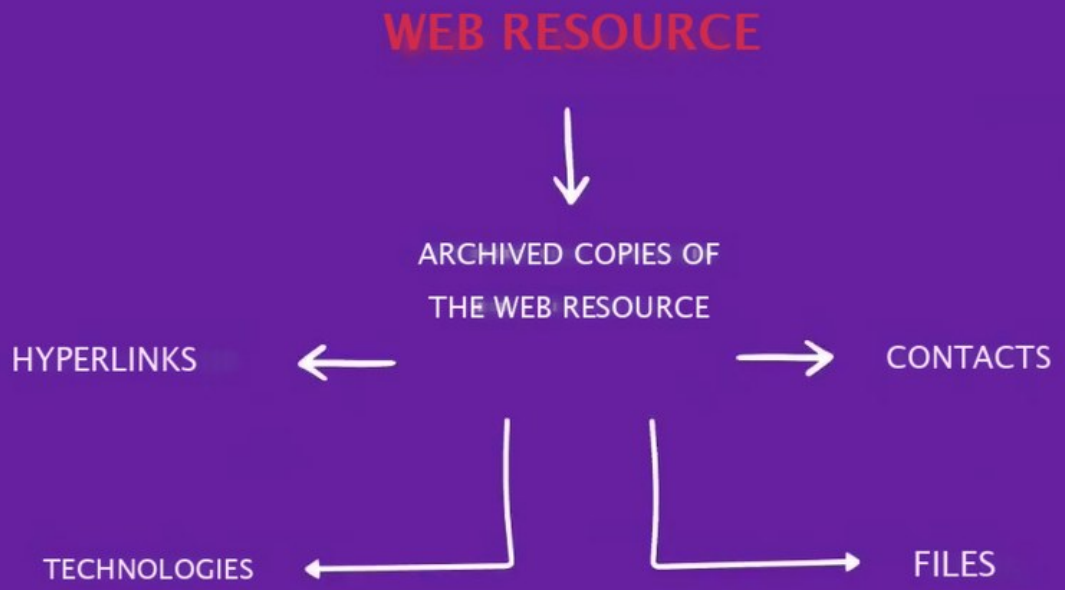


TECHNOLOGIES

ADVERTISING IDENTIFIERS
ANALYTICS, EMBEDDED CHATS
BANK ACQUIRING SERVICES
CODE ELEMENTS

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

Archived copies of a web resource



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

External traffic

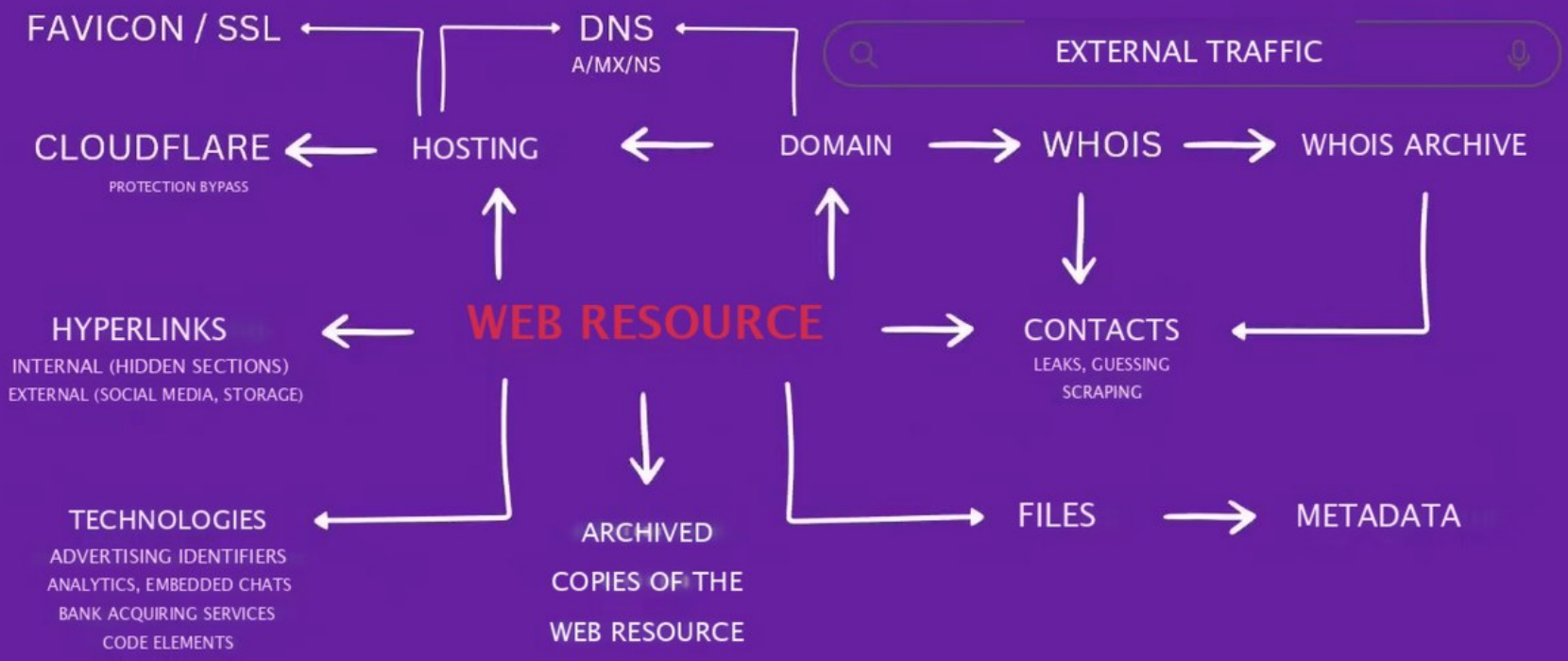
- ya.ru
- google.com
- kribrum.io
- telemetr.me
- vk.com



External traffic to a web resource can often be linked to SMM (social media promotion). This makes it possible to move on in the investigation to studying the specific profiles and social communities that “advertised” the web resource.

The method has become especially relevant when investigating the posting and subsequent promotion of fake petitions through portals such as CHANGE.ORG.

Summing up the investigation plan...



Useful tools

ANALYTICAL SERVICES:

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

WHOIS / DNS:

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

MENTIONS:

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

WEB ARCHIVES:

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

CONTACT SEARCH:

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

OTHER:

- metadata2go.com

ADVANCED GOOGLE SEARCH OPERATORS:

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