



**АКАДЕМИЯ  
КОДЕБАЙ**

ПРОФЕССИЯ ПЕНТЕСТЕР

Netcraft — это компания по предоставлению интернет-услуг, базирующаяся в Англии, предлагающая бесплатный веб-портал, который выполняет различные функции по сбору информации. Использование услуг, подобных тем, которые предлагает Netcraft, считается пассивной техникой, поскольку мы никогда не взаимодействуем с целью напрямую.

Давайте рассмотрим некоторые возможности Netcraft. Например, мы можем использовать страницу DNS-поиска Netcraft (<https://searchdns.netcraft.com>) для сбора информации о домене [megacorpone.com](https://megacorpone.com):

Hostnames matching *.megacorpone.com					
▶ 🔍 Search with another pattern?					
3 results					
Rank	Site	First seen	Netblock	OS	Site Report
58782	<a href="http://www.megacorpone.com">www.megacorpone.com</a> 🔗	March 2013	OVH Hosting, Inc.	Linux - Debian	📄
1089112	<a href="http://intranet.megacorpone.com">intranet.megacorpone.com</a> 🔗		OVH Hosting, Inc.	unknown	📄
1363471	<a href="http://vpn.megacorpone.com">vpn.megacorpone.com</a> 🔗	November 2016	OVH Hosting, Inc.	unknown	📄

Для каждого найденного сервера мы можем просмотреть отчет, который предоставляет дополнительную информацию о сервере, нажав на значок файла рядом с URL каждого сайта:

Background			
Site title	MegaCorp One - Nanotechnology is the Future	Date first seen	March 2013
Site rank	61139	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English
Network			
Site	<a href="http://www.megacorpone.com">http://www.megacorpone.com</a> 🔗	Domain	<a href="https://megacorpone.com">megacorpone.com</a>
Netblock Owner	OVH Hosting, Inc.	Nameserver	ns1.megacorpone.com
Hosting company	OVH	Domain registrar	gandi.net
Hosting country	🇨🇦 CA 🔗	Nameserver organisation	whois.gandi.net
IPv4 address	149.56.244.87 (VirusTotal 🔗)	Organisation	MegaCorpOne, Rachel, 89001, United States
IPv4 autonomous systems	AS16276 🔗	DNS admin	admin@megacorpone.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	<a href="http://www.megacorpone.com">www.megacorpone.com</a>		

В начале отчета представлена информация о регистрации. Однако, если мы прокрутим вниз, то обнаружим различные записи "Site Technology":

<b>Site Technology</b> (fetched 20 days ago)		
<b>Application Servers</b>		
An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.		
Technology	Description	Popular sites using this technology
Apache <a href="#">↗</a>	Web server software	<a href="http://www.fedex.com">www.fedex.com</a> , <a href="http://www.victoriaweather.ca">www.victoriaweather.ca</a> , <a href="http://www.majorgeeks.com">www.majorgeeks.com</a>
Debian <a href="#">↗</a>	No description	<a href="http://www.smtpcorp.com">www.smtpcorp.com</a> , <a href="http://new.adblockplus.org">new.adblockplus.org</a> , <a href="http://crm.aviasg.com">crm.aviasg.com</a>
<b>Server-Side</b>		
Includes all the main technologies that Netcraft detects as running on the server such as PHP.		
Technology	Description	Popular sites using this technology
SSL <a href="#">↗</a>	A cryptographic protocol providing communication security over the Internet	
<b>Client-Side</b>		
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).		
Technology	Description	Popular sites using this technology
JavaScript <a href="#">↗</a>	Widely-supported programming language commonly used to power client-side dynamic content on websites	<a href="http://www.google.com">www.google.com</a> , <a href="http://mail.google.com">mail.google.com</a> , <a href="http://en.wikipedia.org">en.wikipedia.org</a>

Список полученных поддоменов и технологий, используемых на сайте, окажется полезным, когда мы перейдем к эксплуатации информации. Пока же мы добавим его в наши заметки.