

Hipertec Sistemas						
Sites encontrados:	hipertec.com.br	hiperdoctor.com	hipergestor.com.br	ecoreport.com.br	hiperlotes.com.br	hipertecsistemas.com.br
Servidores DNS:	dns1.kinghost.com.br dns2.kinghost.com.br dns3.kinghost.com.br dns4.kinghost.com.br dns5.kinghost.com.br dns6.kinghost.com.br	d.sec.dns.br f.sec.dns.br	d.sec.dns.br f.sec.dns.br	d.sec.dns.br f.sec.dns.br	d.sec.dns.br f.sec.dns.br	d.sec.dns.br f.sec.dns.br
Endereço IPV4:	177.12.171.167	216.172.172.187	186.202.116.108	186.202.116.108	186.202.116.108	186.202.116.108
SO:	Linux	Linux	Windows Server 2008	Windows Server 2008	Windows Server 2008	Windows Server 2008
Web server:	Apache	Apache	Microsoft-IIS/7.5	Microsoft-IIS/7.5	Microsoft-IIS/7.5	Microsoft-IIS/7.5
Engenharia social:	Dono: Alexandre Sotis Labaki	Tel.(17) 3224-9009 Cel. (17) 98105-4500 Cel.(17) 98129-9850	contato@hipertec.com.br			
Informações úteis:	Usa o chatbot LiveZilla	Site de login (hipertecsistemas.com.br) muito simples e provavelmente facil de quebrar (onclick="document.forms[0].submit();return false;")		Site: Apache Tomcat/8.5.30		

Banco do Brasil

Informações úteis:	Tem robots.txt (bb.com.br/robots.txt)	Contem alguns arquivos pdf "expostos" (https://www.bb.com.br/docs/...)	JavaScript e HTML5	Enderecos de email: mailer01.bb.com.br mailer02.bb.com.br o365edge.bancobrasil.com.br	
Sites encontrados:	bb.com.br	bancobrasil.com.br			
Servidores DNS:	dns1.bb.com.br dns2.bb.com.br dns3.bb.com.br dns4.bb.com.br	170.66.3.2 170.66.3.3 170.66.205.1 170.66.205.2			
Endereço IPV4:	170.66.11.10	170.66.2.59			
SO:	Citrix Netscaler	Citrix Netscaler, Windows Server 2003 e OS/390			
Web server:	unknown	unknown e IBM HTTP Server/V5R3M0			
Engenharia social:	dined.comunicacao@bb.com.br ditec.redes@bb.com.br postmaster@bb.com.br				

Spotfy							
Informações úteis:	Tem robots.txt (spotify.com/robots.txt)	Tem um txt com os seus ads (spotify.com/ads.txt)	Index of "exposto" (repository-origin.spotify.com/dists/ ou /pool/)	Enderecos de email: alt1.aspmx.l.google.com alt2.aspmx.l.google.com aspmx.l.google.com aspmx2.googlemail.com aspmx3.googlemail.com aspmx4.googlemail.com aspmx5.googlemail.com		Google Compute Engine	JavaScript e HTML5
Sites encontrados:	spotify.com (*.spotify.com)						
Servidores DNS:	dns1.p07.nsone.net dns2.p07.nsone.net dns3.p07.nsone.net dns4.p07.nsone.net ns-cloud-a1.googledomains.com ns-cloud-a2.googledomains.com ns-cloud-a3.googledomains.com ns-cloud-a4.googledomains.com	198.51.44.7 198.51.45.7 198.51.44.71 198.51.45.71 216.239.32.106 216.239.34.106 216.239.36.106 216.239.38.106					
Endereço IPV4:	35.186.224.25						
SO:	Linux						
Web server:	nginx e envoy						
Engenharia social:	office@spotify.com						

OLX

Informações úteis:	Tem robots.txt (https://olx.com.br/robots.txt)	Tem um txt com os seus ads (https://olx.com.br/ads.txt)	Endereços de email: mxd01.olx.com.br mxd02.olx.com.br	Amazon Web Services	JavaScript e HTML5
Sites encontrados:	olx.com.br (*.olx.com.br)				
Servidores DNS:	ns-976.awsdns-58.net ns-1103.awsdns-09.org ns-2004.awsdns-58.co.uk ns-2.awsdns-00.com				
Endereço IPV4:	13.224.69.59				
SO:	Linux				
Web server:	nginx				
Endereços:	108.139.182.129 108.139.182.119 108.139.182.56 108.139.182.115	13.227.126.52 13.227.126.57 13.227.126.16 13.227.126.89			
Engenharia social:	Dono: Schibsted Brasil	infra@olxbr.com			
Ps: Descobri depois de terminar que ela é sediada em outro país.					