****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**0 – Outros Frootprints**

Muitos métodos tradicionais para a obtenção de informações sobre o alvo ainda funcionam hoje, como a análise do lixo, consulta a banco de dados públicos e consulta a mecanismos de busca. No entanto, novos métodos que se valem de tecnologias como aplicações em redes sociais para obter informações estão se tornando cada vez mais comuns.

Do ponto de vista do atacante, é extremamente importante fazer o reconhecimento da forma mais sigilosa possível. Levantando em consideração que a obtenção de informações é uma das primeiras etapas a ser executada pelo invasor, ele deverá tomar o cuidado de não fazer nada que possa alertar o alvo, por isso, devemos obter essas informações sem enviar um único pacote de rede para o alvo.

As informações obtidas durante o reconhecimento sempre terminam ajudando o atacante de alguma forma, mesmo que no momento não esteja claro elas poderão ser úteis. Os atacantes desejam obter o máximo de informações possíveis sobre seu alvo, conhecendo os dados que eles coletam.

**1 – Usando dados de Mídia Sociais**

As mídias sociais estão em todas as partes, e na maioria dos casos, acessível ao público. A maioria das pessoas tem Facebook, LinkedIn, blogs, Twitter ou outras formas de serviços na nuvem.

Estas informações podem ser usadas como meio de inteligência para podermos montar uma engenharia social, seja por telefone ou por spear phishing, das pessoas que trabalham ou trabalhou no alvo.

Podemos identificar ex-funcionários em sites como https://www.lovemondays.com.br/ e http://glassdoor.com, que são mídias sociais onde funcionários e ex-funcionários dão um feedback de como foi trabalhar naquela empresa.

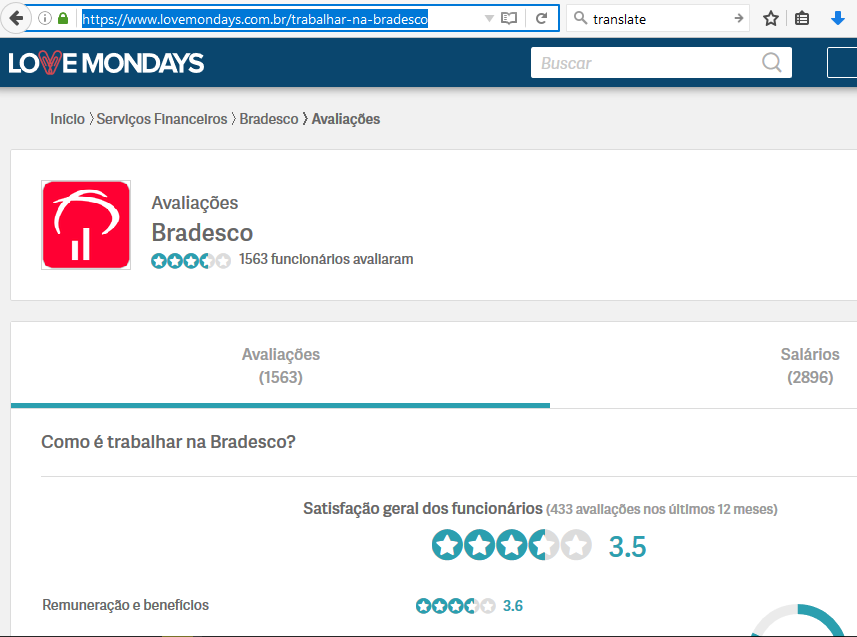


Figura 01 – Site da LoveMondays – Feedback dos Funcionários

Outra forma de buscar dados de pessoas é através do Maltego, que faz buscas na web, mídias sociais, registros públicos, e sites de recrutamento.

A ideia aqui é pesquisar o máximo possível das pessoas que trabalham no alvo, dados esses que podemos utilizar em engenharia social, por exemplo, lugares onde um indivíduo gosta de estar, onde faz negócios, pessoas com quem gosta de estar, interesses pessoais, esporte favorito, entre outros dados que depois de compilado da força para a engenharia social.

**2 – Postagem de Emprego**

Na maioria das publicações de vagas de emprego, os recrutadores costumam colocar uma riqueza de informações sobre o ambiente do alvo.

Os anúncios de emprego costumam fornecer detalhes sobre o tipo de sistemas instalados, quem os administram, nível de habilidade dos candidatos.

Os pessoais de RH são ansiosos para compartilhar informações sobre o ambiente de trabalho, recursos, sistemas, entre outros, que se tornam informações privilegiadas nas mãos certas.

Um exemplo, seria em uma entrevista de emprego, você poderia formular quesitos como: Que sistemas terei que dar suporte, e quais versões? Como funciona a operação, eu ficaria interno ou externo? Pode trabalhar de casa?

Percebeu o tanto de informações em um simples telefonema para um recrutador pode causar ao seu ambiente tecnológico?

**3 – Localização**

Saber a localização do alvo é importante por diversos fatores. Pois observando a localização do alvo pode dizer muito sobre ele.

O investimento em segurança da informação do alvo pode ser determinado com base no investimento em segurança física. Pois um alvo que tem catracas de acesso, guardas armados, localização privada e dedicada, possivelmente tem um maior investimento em segurança da informação do que um alvo que está localizado em um edifício público.

Fontes de mapeamento on-line como o Google Maps pode ajudar a identificar a segurança física, as formas como as pessoas se deslocam de, para e a partir do alvo. Podemos com base na localização encontrar ambientes de descontração como bares, lanchonetes, cafeterias onde as pessoas que trabalham no alvo possam se reunir para se descontrair ou apenas tomar um café.

Assim, podemos puxar conversa com o pessoal, ou até mesmo atacar os dispositivos móveis deles com Wi-Fi Caffe-Lette ou Wi-Fi Honeypot.

Outras áreas de interesse são a identificação de onde podemos acampar para procurar por redes sem fio, e observar como é feito o controle de acesso físico, trajes das pessoas, logo das roupas ou crachás.

E além de ouvir ou conduzir uma conversa no local, podemos seguir os funcionários nos prédios, isso se chama **“piggybacking”** e podemos ter êxito. Uma pessoa não autorizada dentro do prédio pode verificar a existência de portas destrancadas que oferecem acesso a áreas adicionais para que ele acesse ou tenha a sua disposição.

****

Figura 02 – Google Maps – Proximidades – Cafeteria

**4 – Wikipédia**

Podemos conhecer muitos detalhes das empresas fazendo uma pesquisa no Google pela empresa e Wikipédia (<https://wikipedia.org>). Podemos pegar como exemplo o Banco Banespa, um grande banco que era estatal.

Quais os tipos de informações podemos adquirir através do Wikipédia? Vamos fazer uma busca no Google por: banespa Wikipedia

Clique no link referente a Wikipédia.

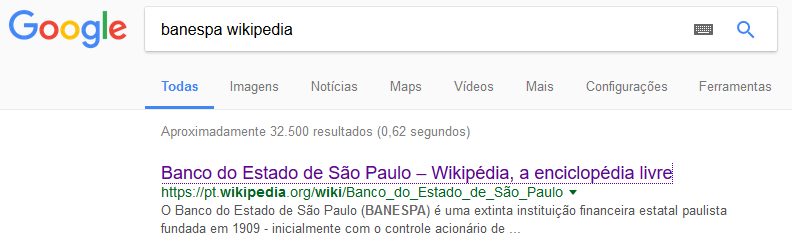


Figura 03 – Pesquisa no Google

Depois que abrir a página da Wikipédia vamos olhar dados que nos interessa, tais como: A história do banco dados financeiros, etc.



Figura 04 – Dados a Instituição

Observe a quantidade de informações interessante na figura acima. Também podemos ver que o banco foi adquirido pelo Banco Santander, vamos clicar neste link.

Então somos direcionados a página da Wikipédia referente ao Banco Santander que contém outras tantas informações sobre a instituição.



Figura 05 – Dados da Instituição Adquirente

Pois bem assim estamos mapeando e garimpando as informações para guardamos em nosso alforje para utiliza-las.

**5 – Robtex**

É um site que faz diversas consultas DNS e colhe o maior número de informações a respeito do domínio procurado. Mais uma vez vamos pesquisar pelo domínio da instituição Banespa.

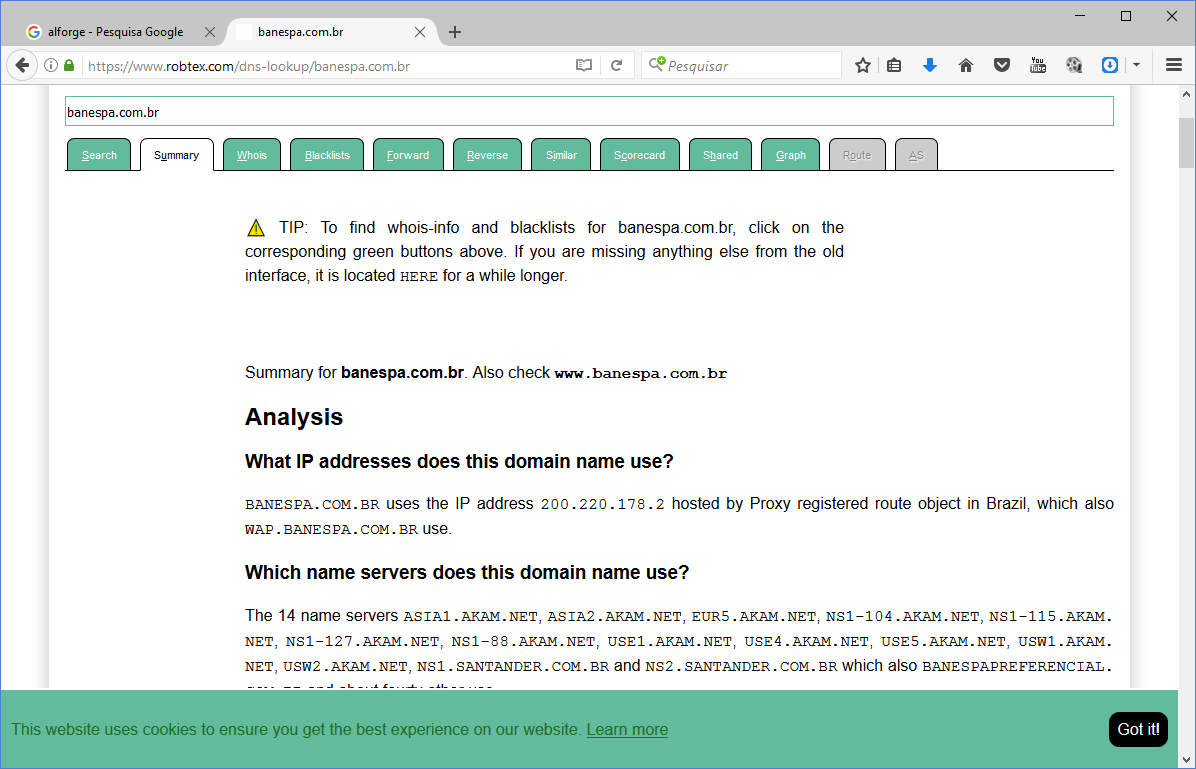


Figura 06 – Site Robtex

Nele podemos ver diversas informações de DNS, tais como: Endereços IP utilizados (IPv4 e IPv6), Servidores DNS com autoridade para o domínio em questão, Servidores de E-Mail, Geo-Localização, Domínios semelhantes, Endereços IP, Registro PTR e Subdomínios.

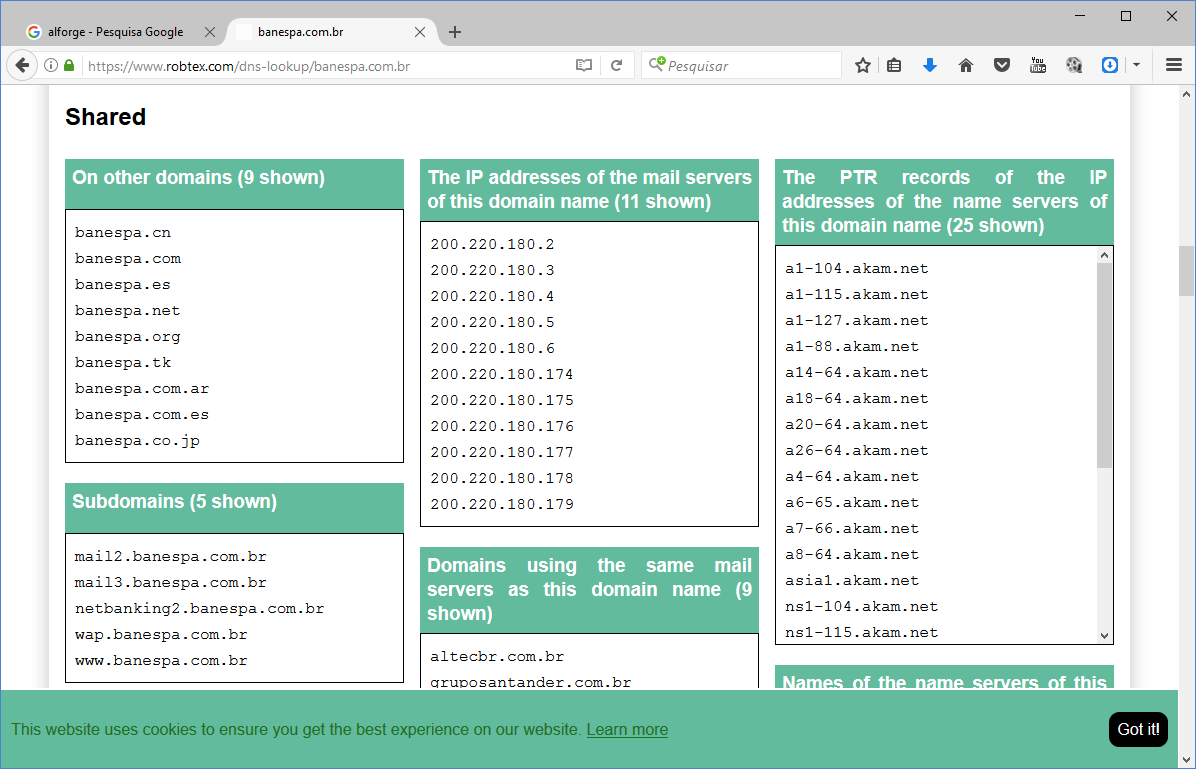


Figura 07 – Mais Informações

Podemos ver um gráfico da pesquisa clicando na aba **Graph**.

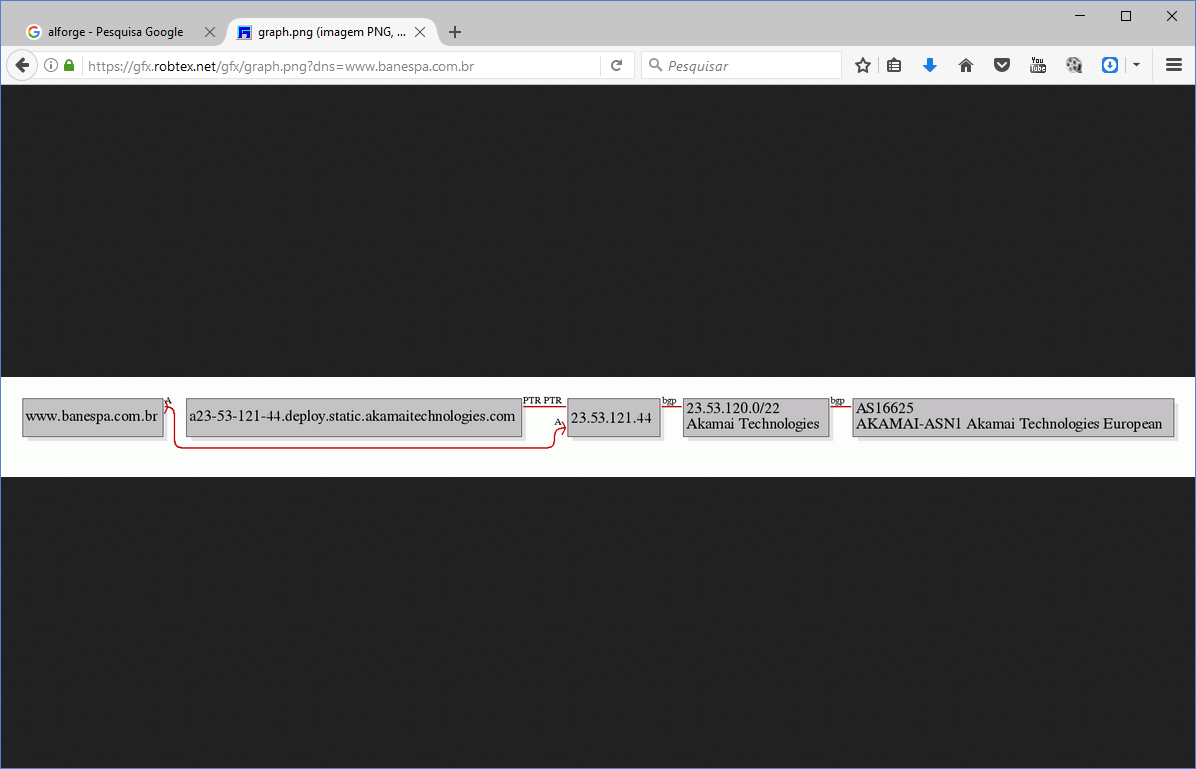


Figura 07 – Gráfico gerado pelo Robtex

Desta forma levantamos algumas informações interessantes, por exemplo, na pesquisa ele nos retornou Akamai Tecnologies, podemos pesquisar para saber qual serviço a Akamai oferece aos seus clientes.

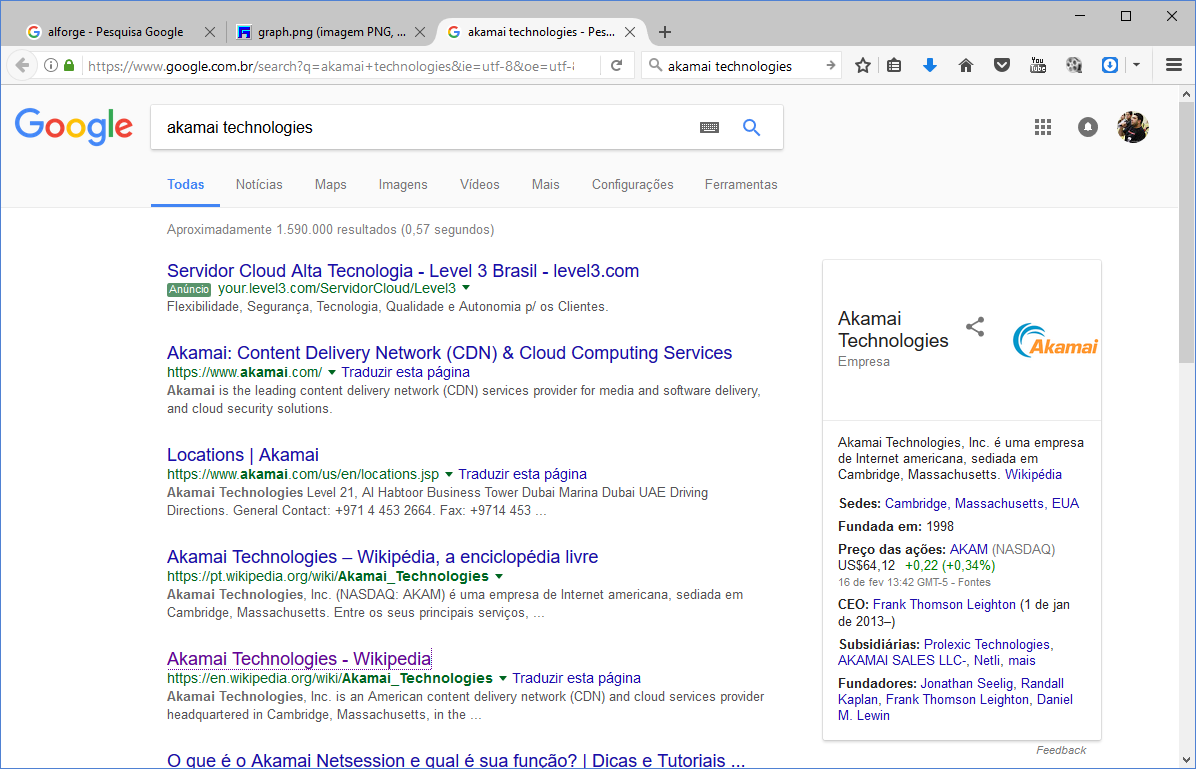
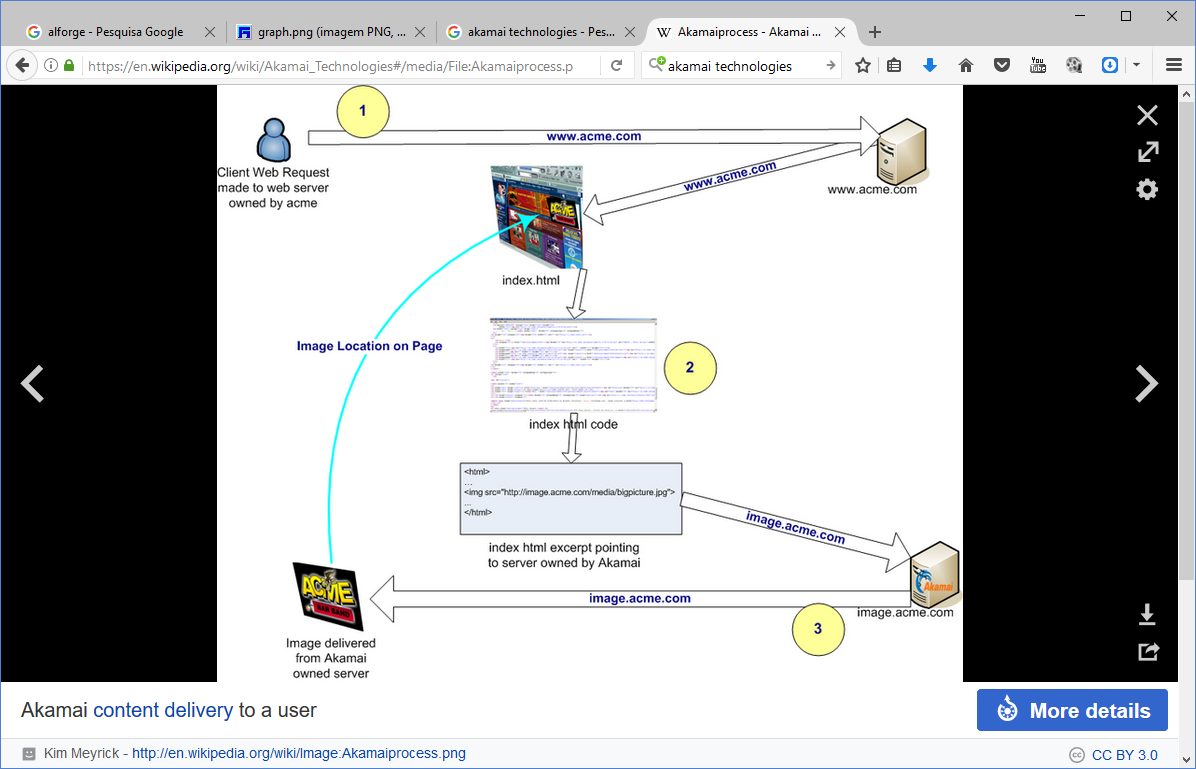


Figura 08 – Akamai Tecnologies

Figura 09 – Esquema de Uso de Um dos Serviços da Akamai

**6 – Hoovers**

Saber questões de valores $$ das instituições podemos utilizar o HooVers (http://www.hoovers.com). Vamos pesquisar sobre o Banespa nele.

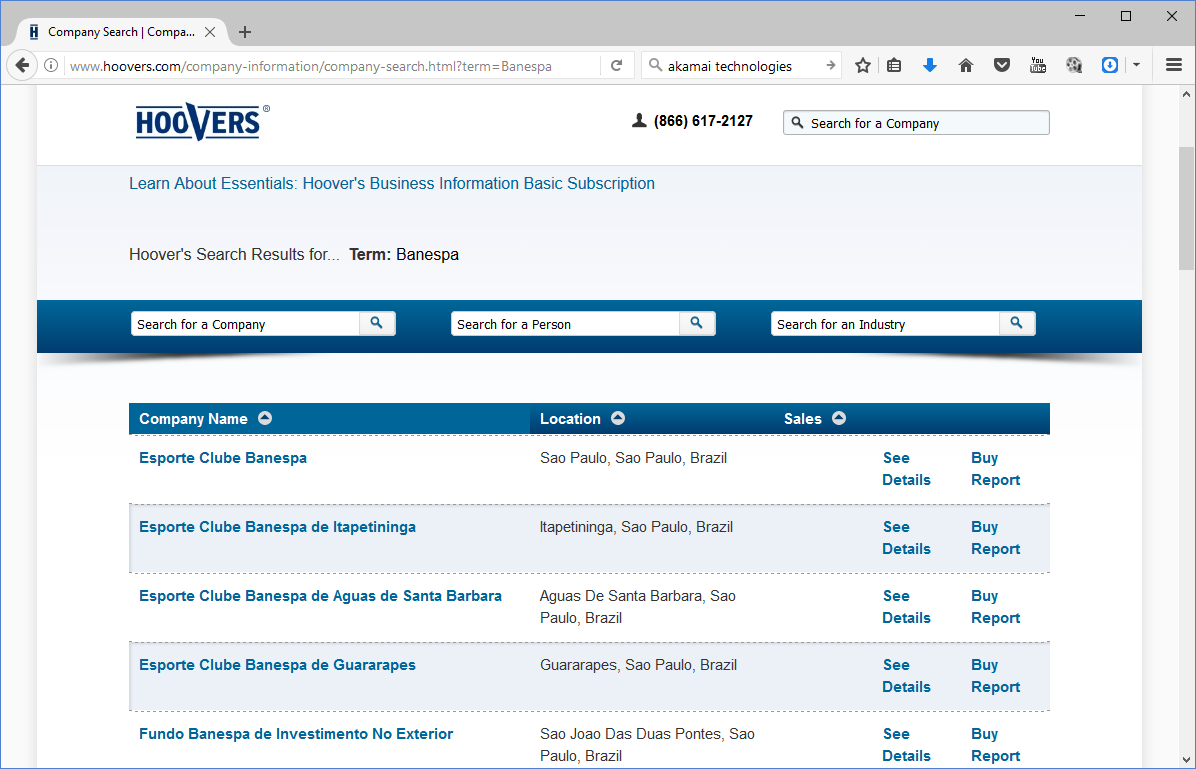


Figura 10 – Informações Sobre Fundos do Banespa

**6 – Plugin Firefox Passive Recon**

Podemos utilizar esse plug-in para fazer o reconhecimento utilizando os mesmos sites que utilizamos mais em poucos cliques.

No exemplo que irei fazer vamos entrar no site alvo (<http://www.altoromutual.com>) e clicar com o botão direito no site selecionar **PassiveRecon**, aponte para **Show All** para que o plug-in faça todas as buscas passivas.

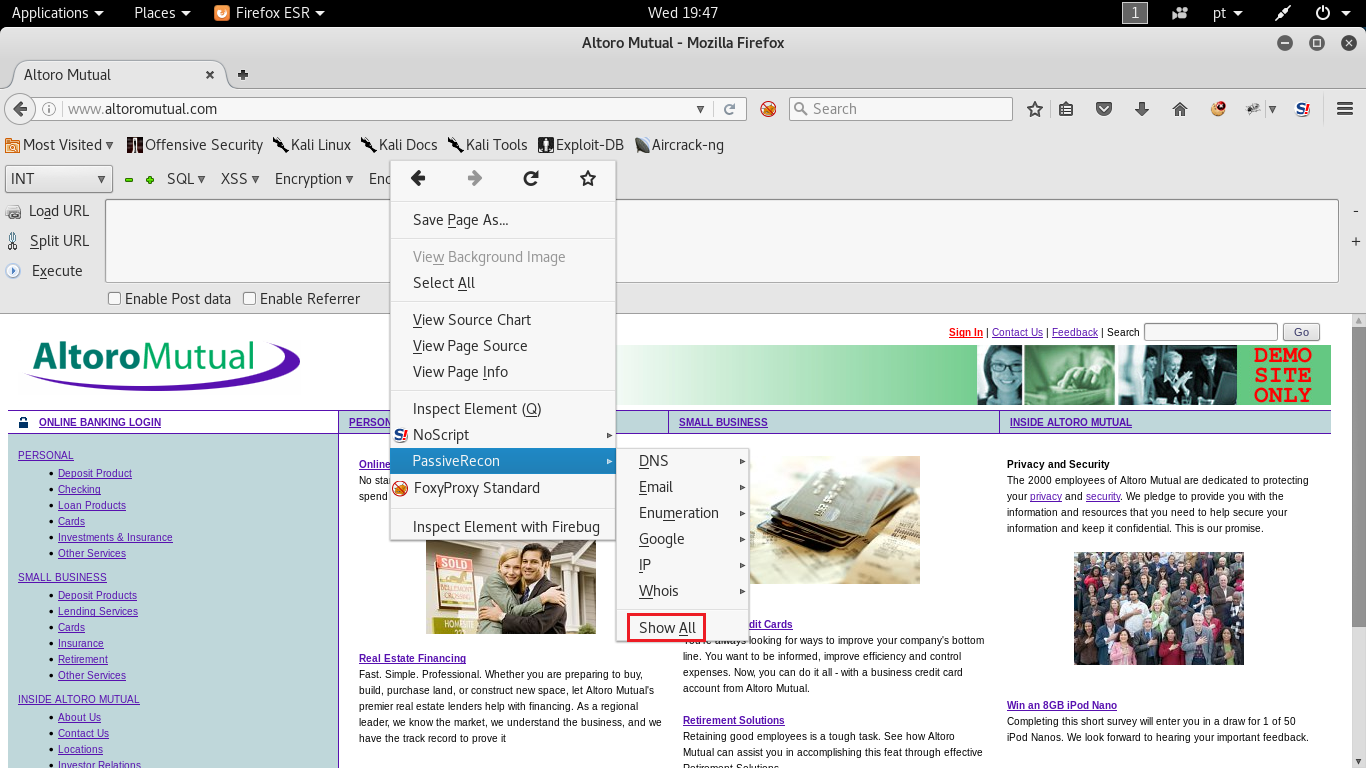


Figura 11 – Passive Recon

Ele irá abrir diversas abas cada um com o seguinte endereço:

* http://whois.domaintools.com/altoromutual.com
* http://network-tools.com/default.asp?prog=trace&host=www.altoromutual.com
* http://network-tools.com/default.asp?prog=network&host=www.altoromutual.com
* http://centralops.net/co/DomainDossier.aspx?dom\_whois=true&dom\_dns=true&traceroute=true&net\_whois=true&svc\_scan=true&x=15&y=11&addr=altoromutual.com
* https://www.google.com/search?hl=en&q=filetype%3Atxt+site%3Awww.altoromutual.com
* https://www.google.com/search?hl=en&q=site%3Aaltoromutual.com+-www.altoromutual.com
* https://www.google.com.br/search?hl=en&q=filetype:rtf+site:www.altoromutual.com&gws\_rd=cr&ei=nRWuWMzKDMOpwgT13o74Bg
* https://www.google.com.br/search?q=filetype:xls+OR+filetype:ppt+OR+filetype:doc+site:www.altoromutual.com&gws\_rd=cr&ei=nRWuWJ2iDMu2wAS-16GgAw
* https://www.google.com.br/search?q=filetype:xlsx+OR+filetype:pptx+OR+filetype:docx+site:www.altoromutual.com&gws\_rd=cr&ei=nRWuWJqmDIH-wQTDkIb4DA
* https://www.google.com.br/search?hl=en&q=filetype:doc+OR+filetype:docx+site:www.altoromutual.com&gws\_rd=cr&ei=nBWuWO22OIO7wASq45b4DA
* https://www.google.com.br/search?hl=en&q=filetype:ppt+OR+filetype:pptx+site:www.altoromutual.com&gws\_rd=cr&ei=nBWuWM\_4N8KpwgTIqbigCg
* https://www.google.com.br/search?hl=en&q=filetype:xls+OR+filetype:xlsx+site:www.altoromutual.com&gws\_rd=cr&ei=nBWuWKu-N8GVwgTB3JzQBw
* https://www.google.com.br/search?q=link:www.altoromutual.com&gws\_rd=cr&ei=nBWuWI6kN8KZwATtwpfwCA
* https://www.google.com.br/search?hl=en&q=filetype:pdf+site:www.altoromutual.com&gws\_rd=cr&ei=nBWuWOqUN4K4wATFvLKYBA
* https://www.google.com.br/search?q=+%22%40altoromutual.com%22+-www.altoromutual.com&gws\_rd=cr&ei=nRWuWLL8C8X6wQSBzonACQ
* https://groups.google.com/forum/#!search/altoromutual.com
* http://toolbar.netcraft.com/site\_report?url=www.altoromutual.com#last\_reboot
* http://toolbar.netcraft.com/site\_report?url=http://www.altoromutual.com
* http://www.hashemian.com/tools/domain-email.php?b=altoromutual.com
* https://www.robtex.com/dns-lookup/www.altoromutual.com
* https://www.robtex.com/dns-lookup/altoromutual.com
* https://intodns.com/altoromutual.com

Observe a quantidade de sites utilizados para colher informações para abrilhantar nosso Recon.

**4 – Referências Bibliográficas**

**[1]** MUNIZ, JOSEPH and LAKHANI, AAMIR – Web Penetration Testing with Kali Linux, 2013, Birmingham – Mumbai, Packet Publishing

**[2]** GRAVES, KIMBERLY – CEH – Official Ethical Hacker Review Guide, Indianapolis - Indiana, 2007, Wiley Publishing Inc.

**[3]** STUTTARD, DAFYDD and PINTO, MARCUS – The Web Application Hacker’s Handbook, Indianapolis - Indiana, 2º Edition, Wiley Publishing Inc.

**[4]** SCAMBRAY, JOEL, McCLURE, STUART and KURTZ, GEORGE – Hackers Expostos Segredos e Soluções para a Segurança de Redes, São Paulo, 2001, MAKRON Books Ltda.

**[5]** LONG, JOHNNY - GOOGLE HACKING - Para Teste de Invasão [tradução Sérgio Pereira Couto] 2005, DIGERATI (BOOKS)

**[6]** MELO, Sandro – Estudo de Técnicas para Exploração de Vulnerabilidades em Redes TCP/IP, 2º Ed, Rio de Janeiro, 2006, Editora Alta Books Ltda.

**[7]** AHARONI, Mati; Offensive Security Lab Exercises - Curso de Pen-Test oferecido pela Offensive Security, 2007

**[8]** SCAMBRAY, Joel; LIU, Vicent; SIMA, Caleb - Hacking Exposed Web Application: Web Application Security Secrets And Solutions – 3ª Edition, New York – 2011, McGraw-Hill

**[9]** DHANJANI, Nitesh; RIOS, Billy; HARDIN, Brett - Hacking A Próxima Geração – Rio de Janeiro – 2011, Alta Books