
MarkMonitor®

▶ **The Threats to Brand Online
and a Holistic Strategy to Mitigate Them**

Charlie Abrahams

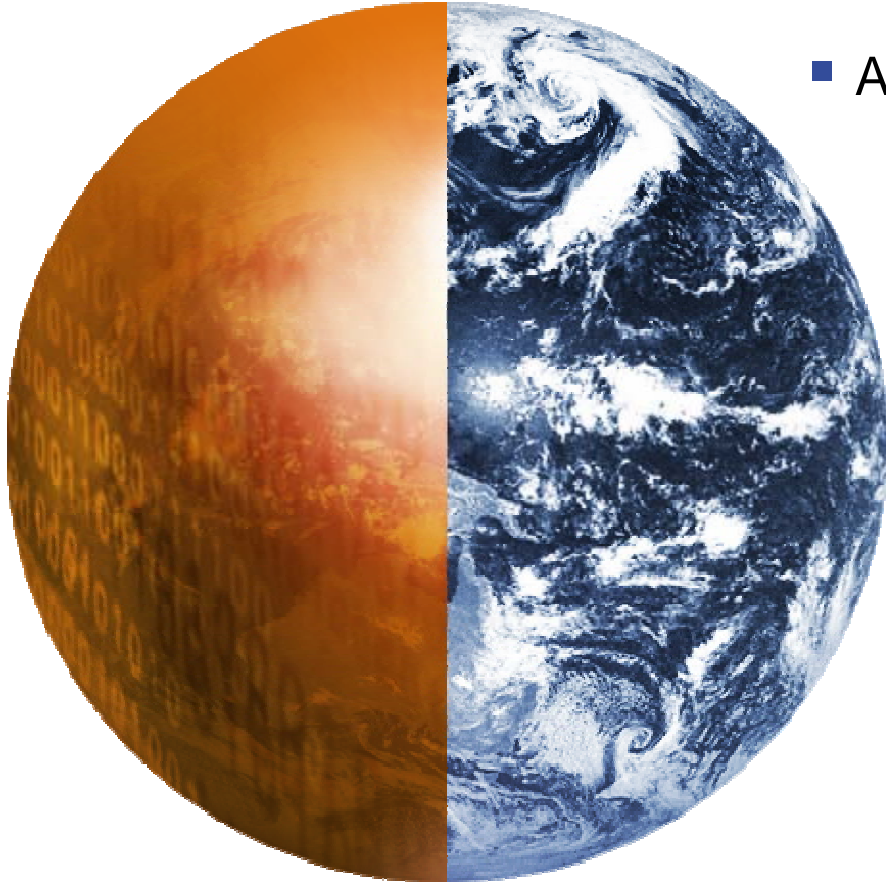
MAKING THE INTERNET SAFE FOR BUSINESS

▶ Agenda

- Characteristics of the internet which pose a threat
- Types of threat to IP online
- Current research in the space – The Brandjacking Index
- Key elements of a mitigation strategy
- Case Studies

▶ Same Characteristics that Make the Internet Attractive as a Low-Cost Channel...

.... Also Attract Fraudsters

- 
- Global reach
 - Ability to set up low cost store-front in a matter of hours
 - Ease and low cost of registering domain names
 - Anonymity
 - Easy to copy electronic brand images
 - Policing limited or non-existent

▶ Types of Threat

- Trademark related abuse
 - Traffic diversion
 - Negative association
 - “Kiting” and “Tasting”
- Counterfeit product sales
 - eCommerce sites
 - Auction listings
 - B2B
 - Spam
- Financial Fraud
 - Phishing
 - 419 Scams

▶ The MarkMonitor Brandjacking Index

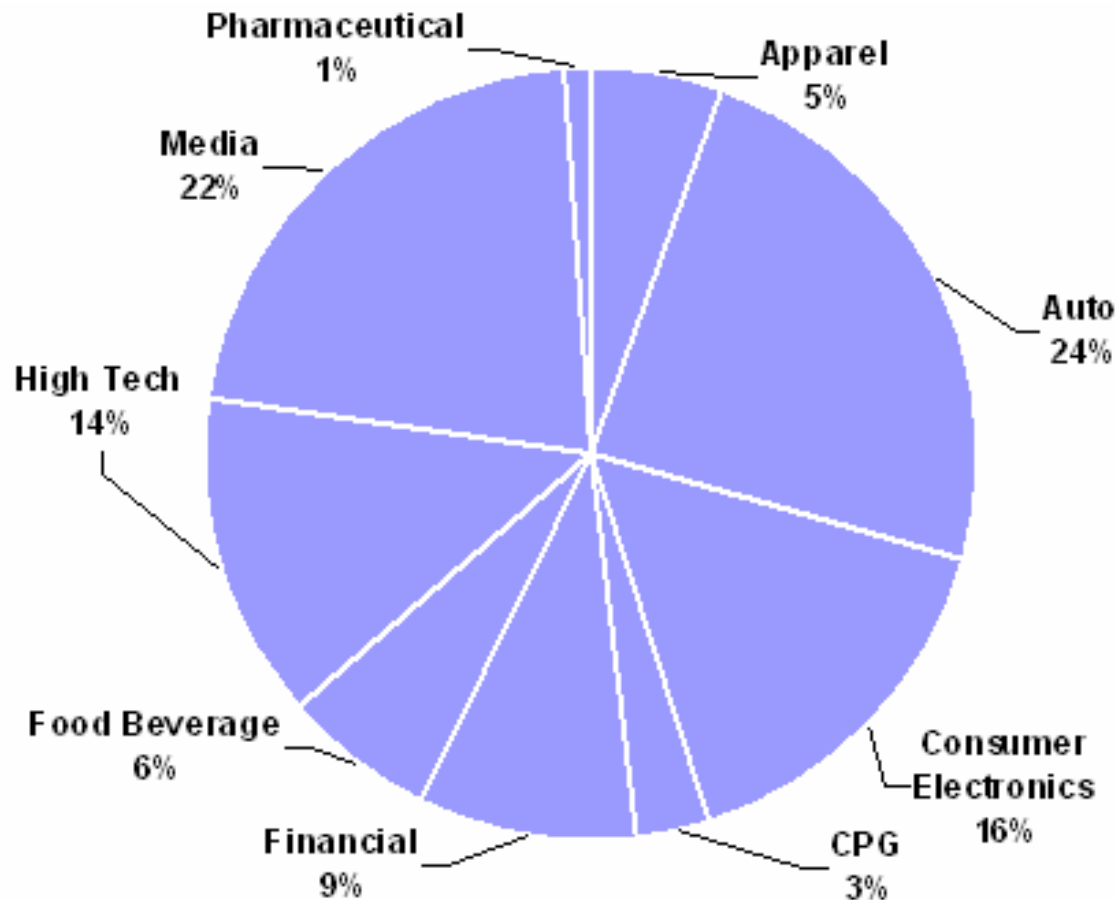
- Quarterly assessment of the global threat to brands
 - Overall abuse level and trending for 32 major brands
 - Phishing threat analysis
 - Focused review of one particular vertical
- Methodology
 - No customer data used in the study
 - Weekly sampling over four week period
 - 32 brands from the Interbrand 100, across 9 vertical segments
- Analysis
 - Trends
 - New threats
 - Conclusions about state of the online world

▶ Brand Abuse – Summary

Threat Type*	Q1-07 Results*	Q2-07 Results*	% Change
Domain Kiting	11,015	37,634	242%
Offensive Content	1,395	2,138	53%
Pay-Per-Click	50,743	73,774	45%
False Association	75,167	107,316	43%
Cybersquatting	286,801	311,050	8%
E-commerce Sites	21,093	22,639	7%

* Threat types are not exclusive of other threats. Data is based on weekly samples averaged over one quarter.

▶ Brand Abuse – By Industry Segment 2007



Media (22%) and Auto (24%) still lead all segments of abuse

Brand Abuse – Traffic Diversion

- Cybersquatting
- Example of false association to drive traffic
- Pay-Per-Click advertising on site

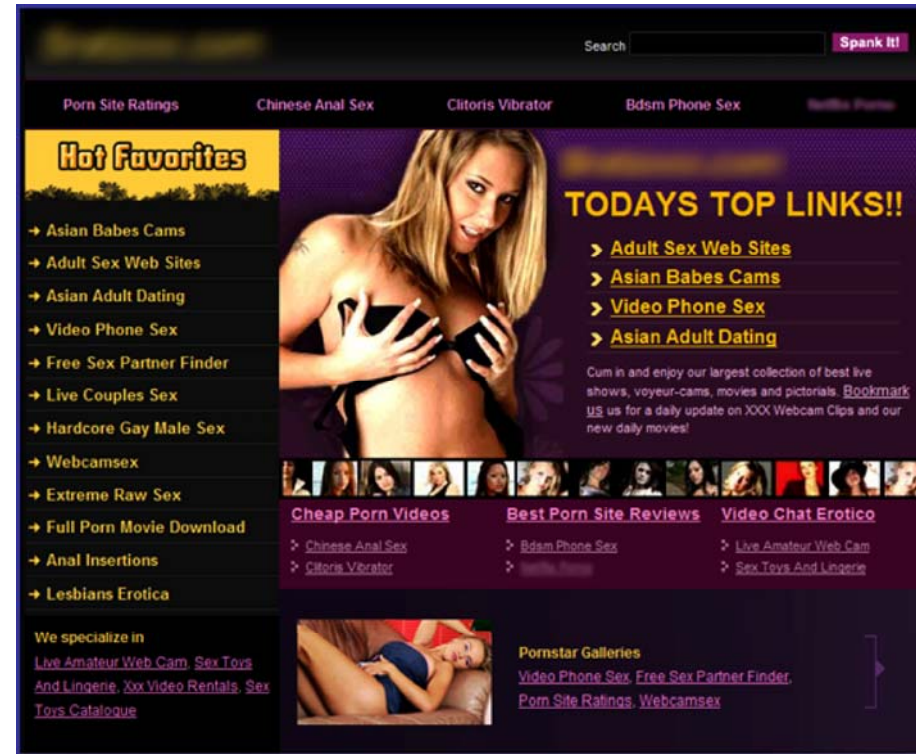


Example of PPC Traffic Diversion

Popular toy brand used to divert traffic

► Brand Abuse – Negative association

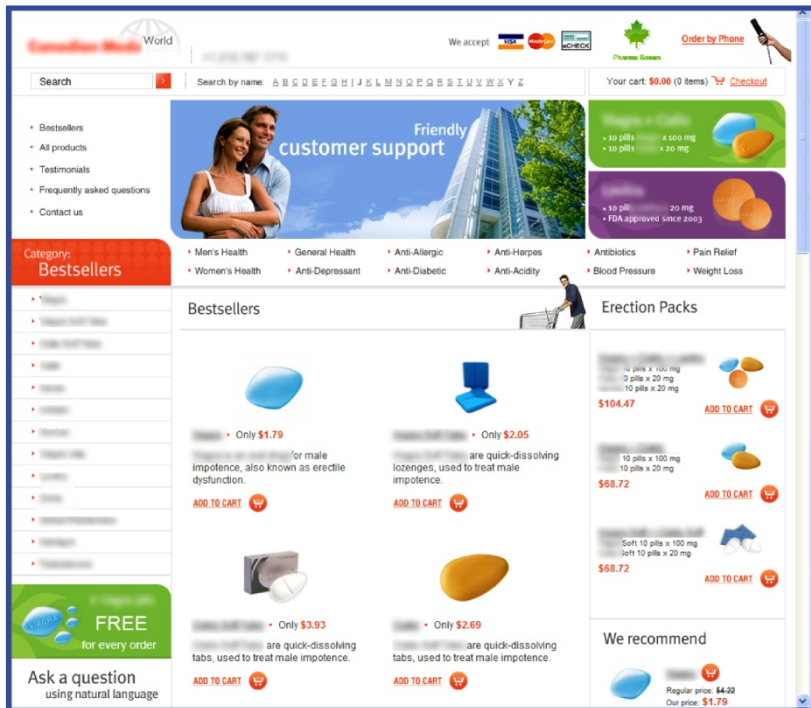
- Cybersquatting
- PPC on page
- Sexually suggestive images associated with toy brand
- Sexually explicit language associated with toy brand



PPC Traffic Diversion Example

Inappropriate content using children's toy brand

► eCommerce sites – “unregulated” Product sales



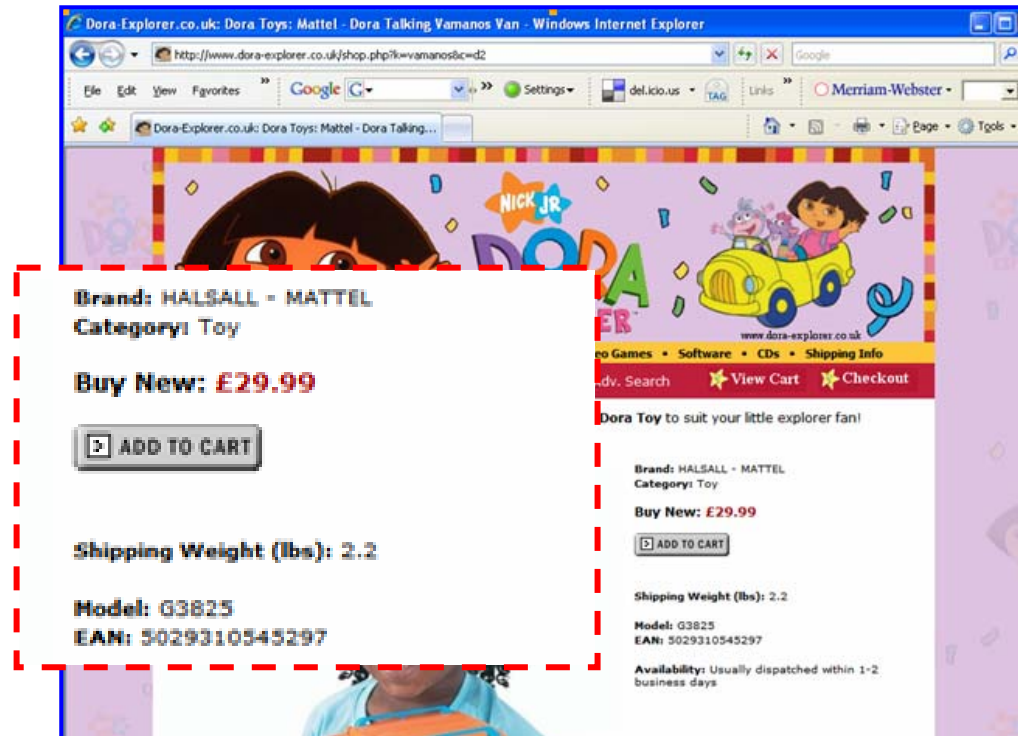
Online pharmacy example

- “Canadian” online pharmacy with host server in Russian Federation
- Faked accreditation and certification
- Selling individual pills

Significant brand threat

▶ Toy Brand Abuse – Unaffiliated Site

- Cybersquatting with brand in domain
- Trademark abuse with images and copyrights
- Not an authorised vendor – false association
- Recalled toys for sale*



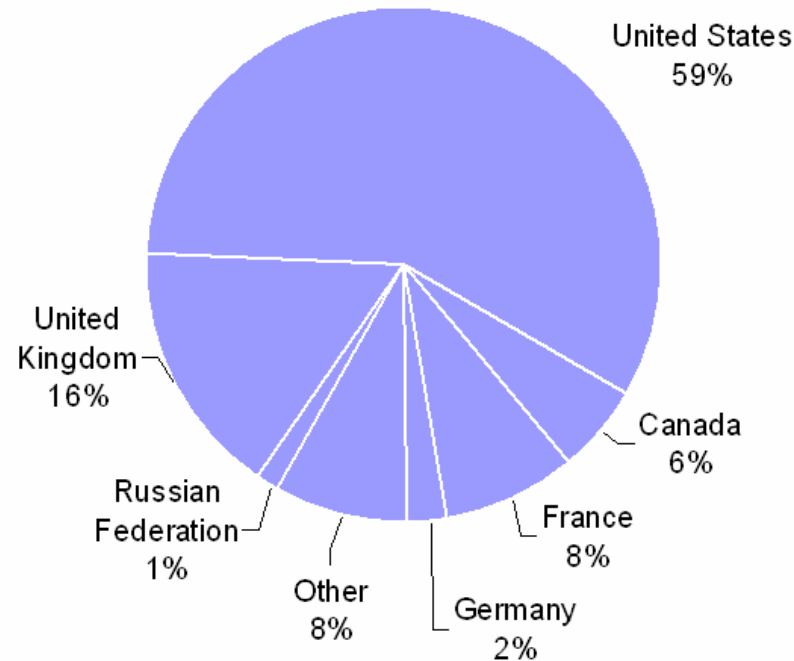
- Product codes match CPSC recalls
- Site removed recalled toy in late Oct., approx. 6 weeks after recall

Example of Unauthorised Vendor Site

Another example of a risky channel

► Scale of the eCommerce problem - pharmaceuticals

Online Pharmacy Hosting By Country, Q2 '07



- 3,160 online pharmacies
 - One-third have Alexa rankings
 - 32K average daily visitors per ranked site
- Four of 3,160 pharmacies are VIPPS certified
- > 50% do not protect customer data
- 10% of sites state: “No prescription required”
- U.S. hosts 59% of the sites
- Estimated \$4 billion* in annual sales from ranked sites

* Based upon total annual traffic, 0.5% conversion rate, \$70 average transaction

▶ B2B Exchanges – counterfeit or recalled?

Product Description
advance cassettes for sell, we have more than 500 game available.

Product Details

GBA Game Card- Lego Star Wars 2 (M7122) [+ Add to Basket](#)

Product Group: [GBA games](#)

Product Description
Gameboy advance cassettes for sell, we have more than 500 game available.
Minimum order 10pcs/model. With retail package (color gift box, white box & user's guide.)
delivery within 7 days after get payment. We can accept paypal. Products quality under
guarantee.

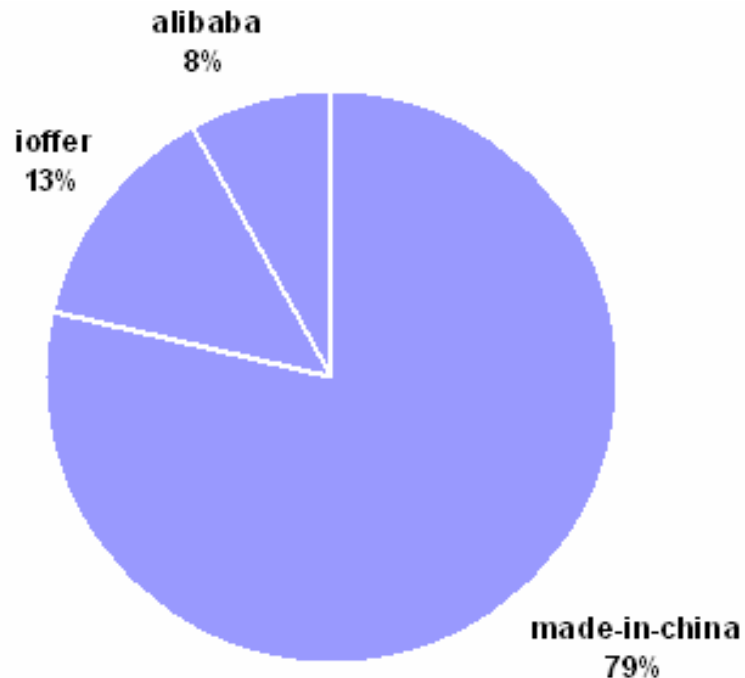
Contact us now if you

Origin: CHINA
Min. Order: 10

- “Name your price” for a game that retails for \$29.99
- Risk of counterfeit
- Source China
- “More than 500”
- Minimum order ten

► Scale of the B2B problem - Toys

Toy Listings by Exchange Site

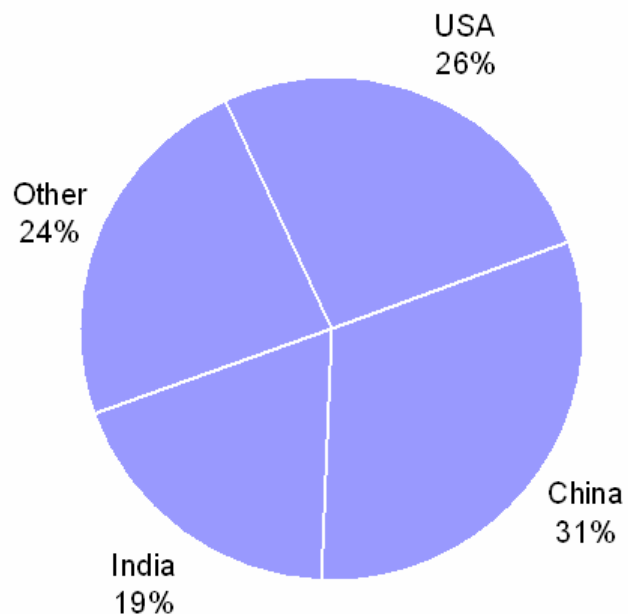


- 1,150* exchange listings for nine toys
- Over 1 million toys available
- Exchange site “Made-In-China” leading source for toys, 79%
- 8% listings for recalled toys

Sample single day results from 09/07

► Scale of the B2B Problem - Pharmaceuticals

Exchange Listings by Origin, Q2 '07



- 390 exchange listings
- 21 listings analysed
 - 75 million pills available
 - \$150 million value*
- China is the primary source (31%)

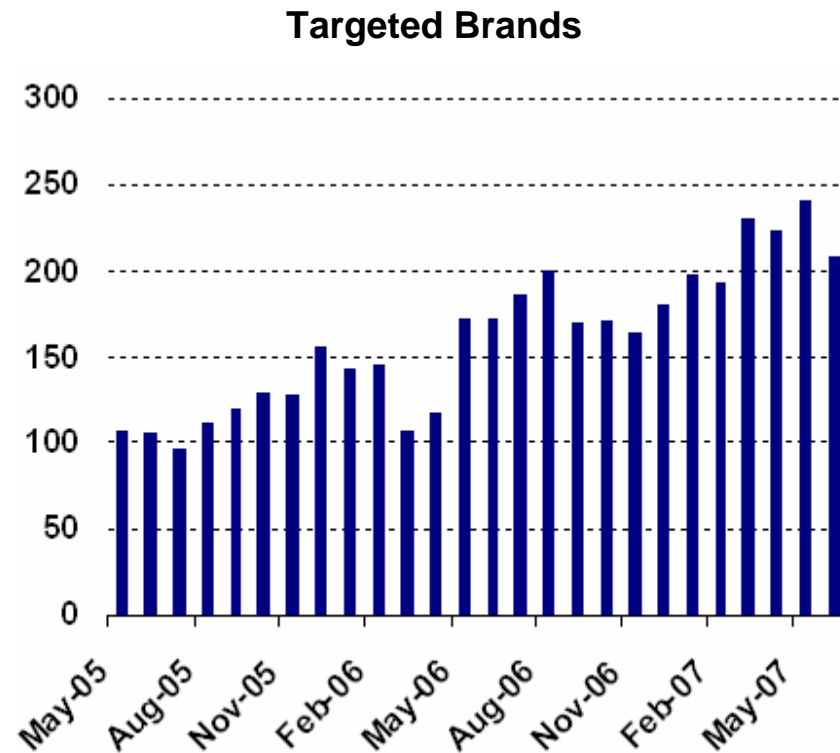
* Estimated \$2 per pill

Robust, global supply chain

▶ Phishing - Observations

- Continued growth in number of organisations phished
 - Diversity in targets
 - Diversity of fraud
- Increased technical sophistication of attacks
 - Techniques target consumer security tools in browsers
 - Tactics indicate sophisticated IT resources and infrastructure
- Non-financial sector attacks growing

▶ Phishing – Increasing Number of Brands Targeted



- 45% increase in organisations targeted (Q2-06 to Q2-07)
- 8% increase in organisations targeted (Q1-07 to Q2-07)
- 240 organisations targeted in May 2007
- 189 new targets in Q2-07, 83% increase from Q1-07

▶ A Holistic Strategy to Protect the Brand Online

- Establish a Brand Protection Task Force
- Register & enforce Trademarks
- Have a conscious Domain registration policy
- Detect infringements
- Drive education / awareness
- Focus on the internet channel
- Attack the supply chain
- Take legal action
- Influence regulation
- **Embrace Technology to Fight Technology**

▶ Embrace Technology to Fight Technology

Why use Technology?

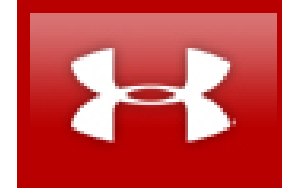
- Scale of the “Haystack”
 - >17 billion web pages
 - 100 million domain names
 - 50 million blog sites
 - ~\$50 billion worth of goods are sold on eBay alone every year
 - ~ 171 billion emails sent every day – 2 million per second (~70% are spam)
- It’s a moving haystack
 - 2 million new articles per day posted to newsgroups from over 100,000 newsgroups
 - 40% of web pages change every week, 23% of .com change daily
 - Billions of pages added every year
- Case Management is near impossible on a manual basis

*“The internet is simply too big just to have somebody doing Google searches for counterfeit products. You’d go insane.”
Nils Montan, President, International Anti-Counterfeiting Coalition (IACC)
Business 2.0, March 2007*

▶ Technology Allows You To...

- Monitor the online channels used to commit fraud in your industry
- Comb through billions of sites, registrations and emails daily
- Analyse and prioritise the most likely suspects
- Investigate using Reverse Whois, IP ownership
- Automatically capture evidence
- Document all activities associated with each case
- Automatically send a cease & desist
- Direct interface into eBay VeRO process

▶ Under Armour



■ Challenge

- Significant brand equity to protect from potential erosion
- Unauthorised online sales causing disgruntled channel partners
- No automated means of identifying fraud and taking action against offenders

■ Solution

- MarkMonitor Online Channel Protection selected for its powerful Web monitoring technology and comprehensive case management capabilities

■ Results

- Estimated \$2 million in unauthorised listings removed from e-commerce sites
- Over 21,000 items removed from 9,800 listings
- Significant revenue recovered via elimination of gray market sales
- Listings from major online auction site reduced from 9,500 to 2,000 items
- Kiplinger calls Under Armour “master of its retail domain”

Acushnet



THE ENFORCER
Rogan uses software to hunt down fake golf gear

3 WAYS TO SPOT BOGUS PRODUCTS

LABELS Cyveillance, of Arlington, Va., looks for fishy pharmaceutical dosages and products on sale in countries where they shouldn't be.

TAGS Boston-based DeSec Security Group slips anti-fraud tags into products on the factory floor and later buys goods to check their pedigree.

LINKS BrandDimensions, based in Toronto, watches who's linking to whom. 50 human "data analysts" then flag likely counterfeiters.

doing Google searches for counterfeit products. You'd go insane."

Instead, companies pay outfits like San Francisco-based MarkMonitor to handle the problem. The privately held company says its revenue grew by 50 percent in 2006 to an estimated \$25 million. Its 500 corporate clients pay fees starting at \$50,000 a year—a small price to help save millions in fraudulent sales. For example, Acushnet, maker of Titleist golf balls and clubs, was able to shut down 75 auctions of knockoff gear in one day last June using MarkMonitor's software—and it took just one mouse click and "about three minutes from starting enforcement to ending the auctions," says Acushnet trademark manager Lisa Rogan.

MarkMonitor isn't alone. About two dozen other companies are using Web-crawling technology to search for counterfeit storefronts and sales. They detect fraudsters who set up shop using domain names similar to legitimate brands or who plaster brands' trademarks and logos on their online storefronts. The companies also monitor counterfeit sales, looking for keywords like "cheap," "discount," "authentic," and "factory variants." They flag colors that the original product wasn't made in and prices that are far too low. Fighting online counterfeiting represents "a big opportunity, and it's just starting to get tapped," says Avivah Litan, a senior analyst at research firm Gartner. Looks like 2007 could be a banner year for the anti-fraud business too. — **DEBORAH KONG**

6 SMART TECH FIGHTS FAKES

This is already shaping up to be a banner year for one Internet industry. Unfortunately, it's the fraud business. Though official numbers are scarce, online protection company MarkMonitor says a record \$119 billion in knockoff goods will be sold on the Web in 2007, up from \$84 billion last year—everything from counterfeit watches to fraudulent pharmaceuticals. eBay has ballooned into a city-size megastore that only an army of security guards could monitor for shady merchants. New online services make it simple and cheap for any site to accept credit card or bank payments, and ads on Google can lure bargain-hunting shoppers within hours.

But just as fake goods are enjoying a heyday online, so are virtual sleuths. New tech firms are arming brand holders with a smart solution. Web-crawling software that detects fraud and sends warnings to apparent violators, often with minimal human action. "There's no other way to do it," says Nils Montan, president of the International Anti-Counterfeiting Coalition, which in November created a special committee to combat online piracy. "The Internet is simply too big just to have somebody

\$119 BILLION
in fake goods will be sold online in 2007.
Source: MarkMonitor

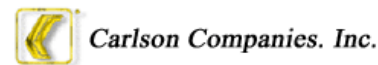
Acushnet, maker of Titleist golf balls and clubs, was able to shut down 75 auctions of knockoff gear in one day last June using MarkMonitor's software – and it took just one mouse click and 'about three minutes from starting enforcement to ending the auctions.'

Lisa Rogan, Acushnet trademark manager
Business 2.0, March 2007

Global Corporate Clients



NORDSTROM



Protecting 53 Of The Fortune 100

▶ Summary

- Brandjackers find substantial economic incentives to target major brands
- Same technologies that aid companies to effectively market are being employed by Brandjackers
- Enforcement is left to brand holders, as governmental and non-governmental regulations are ineffective
- The internet will become an increasingly significant part of the threat to brands
- The internet is so vast and fast-moving that technology is required to combat the problem