Victimless Malware – How Blackhats Make a Killing Targeting Companies

Lou Manousos
RiskIQ

Session ID: HT2-401
Session Classification: Intermediate

Serendipity – Simple Browser Tricks, Hacks and Kits

- Large scale web crawling turned up needles in haystacks
- No “malicious” behavior on the compromised machine
- Some VM aware and only taking action once a day
- Distributed via Exploit Kits or simply within the browser

Serendipity – Finding a Zero Day

“Victimless” Malware

- What is it?
  - The victim is a company or entity
  - Supports a long-term goal to build a business
  - SaaS, part of an ecosystem of bad guys
- How is it different from other malware?
  - Not greedy on system resources
  - Doesn’t attack the user directly
  - Grey

Vulnerable Online Business Models

- Affiliate Marketing Fraud → Retail, FI's, Insurance
- Social Media Clickjacking → Business on FB
- Video Impression Fraud → Online Brand Advertisers
- Rogue Mobile App Distribution → Mobile Developers

Examples

- Lead Gen
  - Credit Card, Insurance, Home Repair. Anything where your business collects Name, Phone, Addy.
- Online Advertising
  - Banner, Video Ads
- Mobile Marketing Budgets
  - Pay-Per-Install Services, App Promotion

How much $ do they make?

Affiliate Marketing Fraud

Target: eBay

- Between 2006 and June 2007, Shawn Hogan (Digital Point Solutions) earned approximately $15.5 million in commissions from eBay. Hogan was eBay's number one affiliate.
- Between 2006 and June 2007, Dunning (Kessler's Flying Circus) earned approximately $5.3 million in commissions from eBay. Dunning was eBay's number two affiliate.

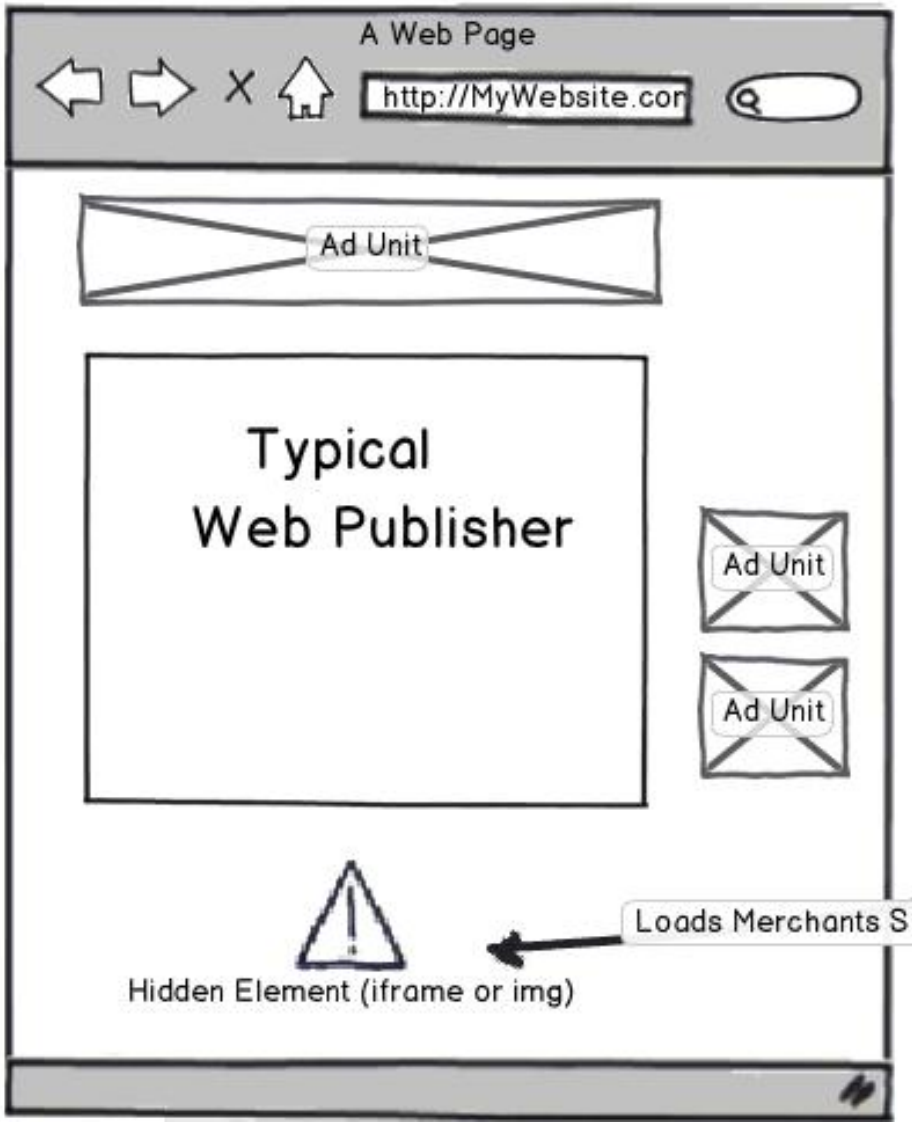
- **Total Revenue > USD $30M**

Threat: Cookie Stuffing

- Cookie stuffing occurs when a user visits a website, and as a result of that visit receives a third-party cookie from an entirely different website (the target affiliate website), usually without the user being aware of it.
- When (if) the user visits the target website and completes a qualifying transaction, the cookie stuffer is paid a commission.
- Depending on the terms of the affiliate agreement a qualifying transaction may refer to creating an account, making a purchase, completing an application (loan, credit, etc.), or subscribing to a newsletter.

Source: wikipedia

Publisher Site



Facebook, AG File Clickjacking Suits Against Adscend Media

Washington Attorney General Doesn't "like" clickjacking

By **Chris Crum** · January 27, 2012 · Leave a Comment

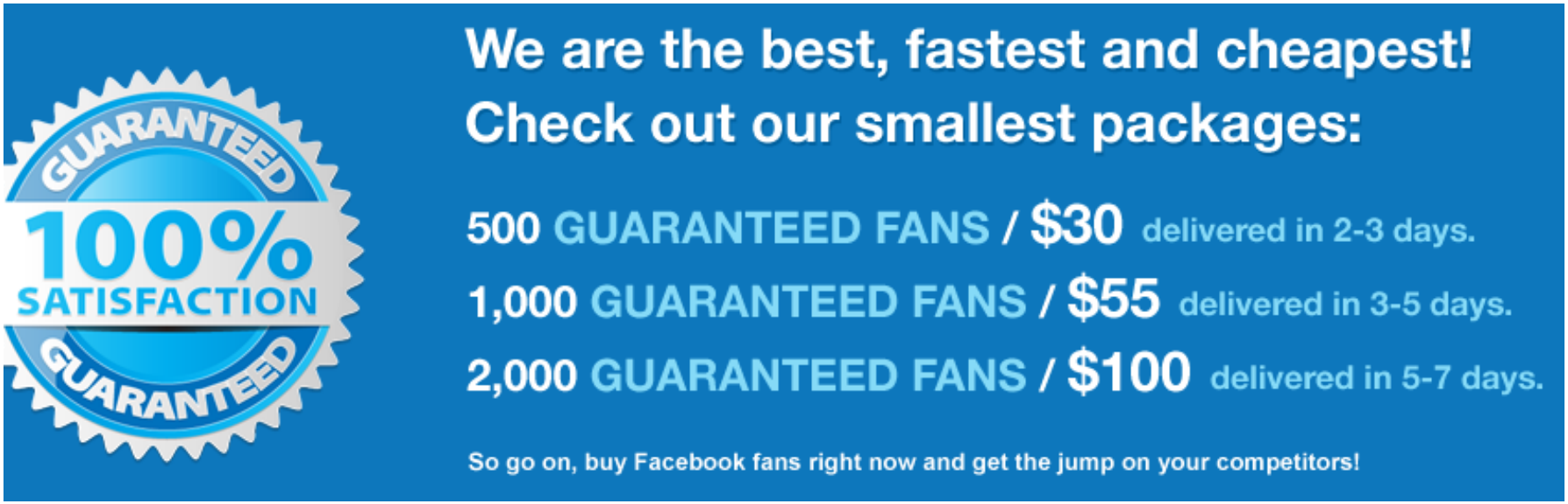
…..at one point Adscend spam lined the defendants' pockets with up to **$1.2 million** a month….

Social Media Clickjacking

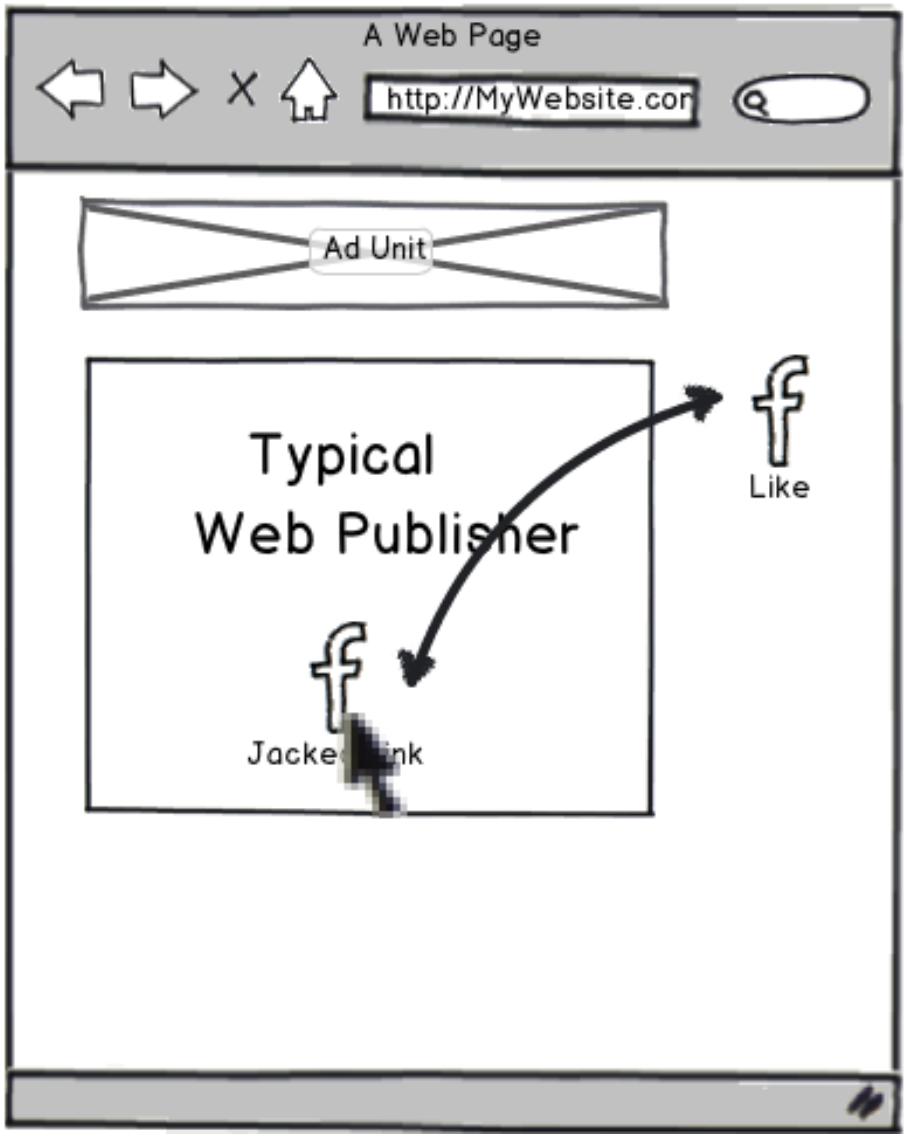
"a malicious technique of tricking a Web user into clicking on something different to what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages."

- Powers an entire industry of unethical marketing and "Social Media Experts"
- Legit Companies unknowingly contract with Clickjacking firms via middlemen

Social Media Clickjacking



Clickjacking Site



Video Marketing Fraud

- From an email recently sent to me:

…… nests of traffic generation, click fraud and malware. We occasionally find a publisher sourcing traffic through there and serving up different landing pages on their site based on the referrer - I estimated that the first publisher we located made approximately $**500K pa from UK ad networks alone** before we discovered him and contacted the other networks he was working with…..

Mobile

- Have you ever wondered why there are 500,000 apps in the app stores but 499,000 of them are worthless?

Mobile Payout Examples

L R	AU - TWILIGHT IQ TEST - FB COMPLIANT	Real	2010-01-04	Allowed Traffic: Banner, Social Media. Can be incentivized (no restrictions). Mobile IQ quiz for the AU market, users can test their intelligence through their mobile phone. SEE EXTRA TERMS FOR DISQUALIFIERS. Pays out on pin submit	2030-12-31	**$7.00/lead**
	- HOROSCOPE	Real	2009-11-23	Traffic Allowed: Banner, Search Cannot be incentivized offer converts when a user enters their mobile number, enters the PIN that is sent to them via SMS-text, and clicks submit. Accepted carriers: Telus, Rogers, Microcell, Bell, MTS, and Virgin	2014-12-31	**$4.35/lead**

Payout

Your Affiliate Manager

Name: [redacted]

Phone: [redacted]

Email: [redacted]

AIM: [redacted]

Interests: Snowboarding, spending time with my two little boys, shopping and vacations in Hawaii :)

Message From Your Affiliate Manager

Fall is in the air!!!! Looking for a place to put your international traffic or exit pop traffic hit me up!!!

Welcome Back, [redacted]

Revenue To Date: $856,415.31

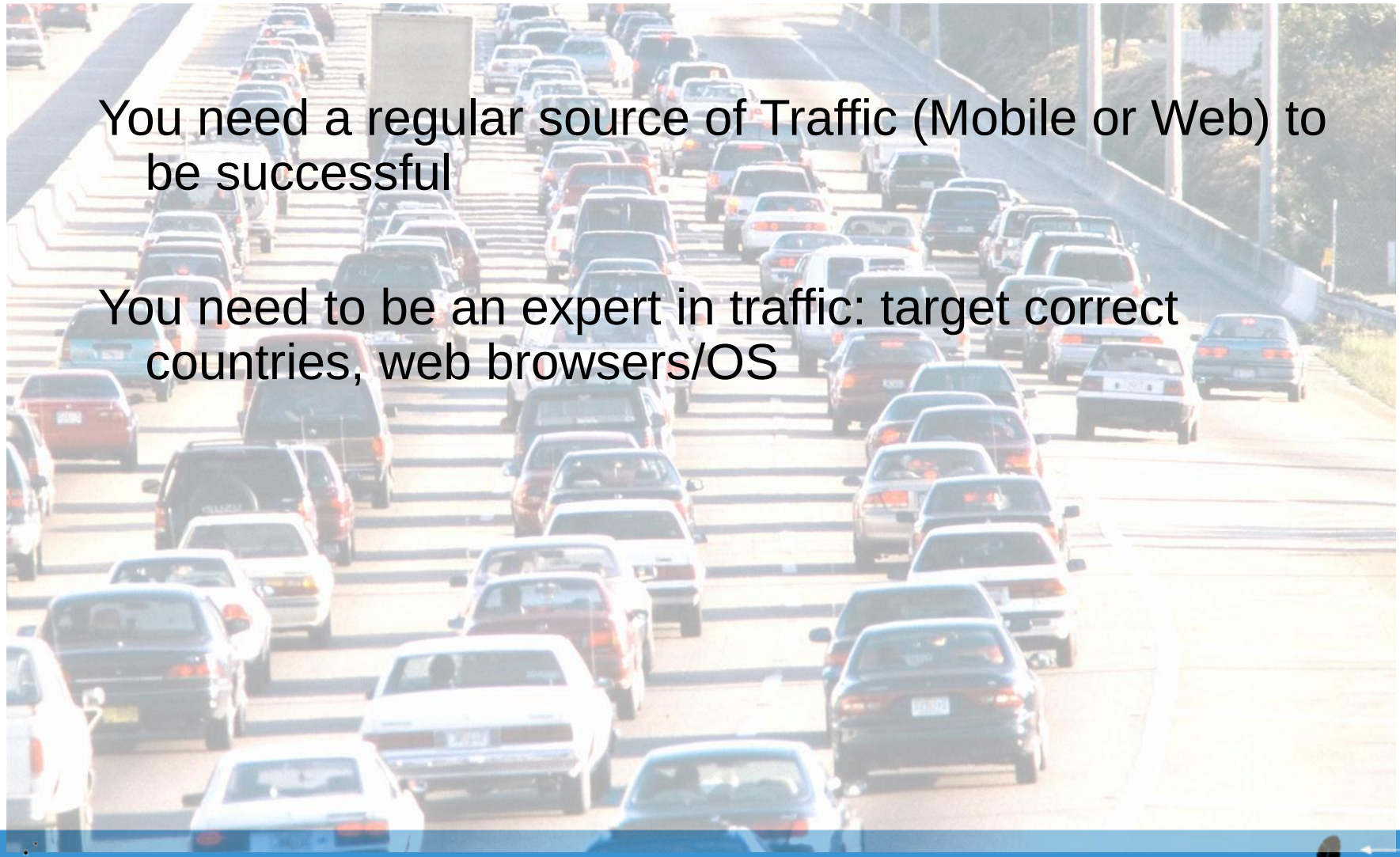
Revenue Today: $0.00

Revenue This Month: $0.00

$856,415.31

Powering the schemes

Traffic



You need a regular source of Traffic (Mobile or Web) to be successful

You need to be an expert in traffic: target correct countries, web browsers/OS

Targeting Users

Attribute	Description	Examples
Location	GeoLocation, City / County	San Francisco, USA
Cookies	Where this user has been before	Gmail.com
ASN Records	What Company they work for?	Ebay.com, Gitibank
Behavior	Search and Prior Contextual Content	Car rental, vegas
OS/Browser	What type of computer setup?	Microsoft XP, ie6
Keywords & Content of the current page	Sports, Business, News, etc.	S&P 500, latest MSFT Stock Price
Cookie Data Sharing	Has this user been on my site before? Have they seen my ad before?	Don't show my ad twice!

Why Traffic is so Important

- Increases the potential size of the scheme
- Geo coverage
- Not every user is vulnerable so bad guys need to cast a wider net
- Keep the metrics looking good
  - Unique Visits / Device Id
  - Conversion Ratios: Impression to Action/Click

Malvertising

Malvertising (from "malicious advertising") is the use of online advertising to spread malware

…

Malware perpetrators will go to great lengths to infiltrate online advertising networks, including the creation of fake advertising agencies that appear to represent legitimate brands.

source: wikipedia

The Role of Malvertising

A new vector for Malware Distro

- **Targeted** – the nature of advertising
- **Quick, Cheap, Scale** – like spam/phish campaigns
- **Slow Detection times** – 3 to 7 days based on OTA numbers

Recent Traffic Incidents From Top 10 Sites in their Category

E-Commerce	amazon.com	via Double Click
News	THE WEATHER CHANNEL weather.com	via Clicksor
Online News	reddit	via Clicksor
News	BusinessWeek	via Double Click
Entertainment	IMDb Earth's Biggest Movie Database™	via Double Click
Sports	FOX SPORTS	via App Nexus

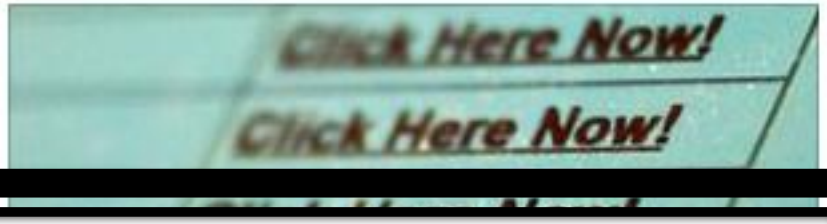
Malvertising Works and is Profitable

23 June 2011 Last updated at 06:14 ET

658 Share

FBI targets cyber security scammers

A gang that made more than $72m (£45m) peddling fake security software has been shut down in a series of raids.



According to the FBI, the pair worked their scam by pretending to be an advertising agency that wanted to put ads on the website of the Minneapolis Star Tribune newspaper.

The raids seized 40 computers used to do fake

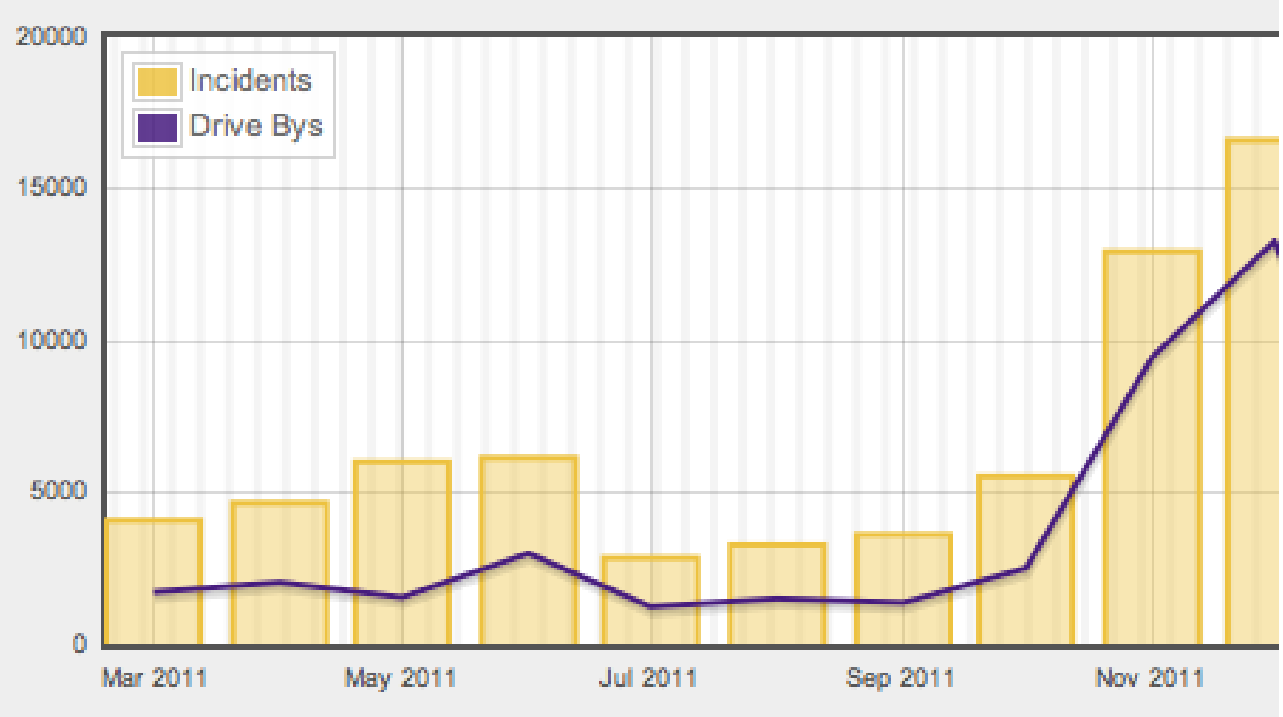
This ruse is believed to have generated a return of about $2m.

Malvertising Keyword Targeting

After Date: last month **Malware**: true **Search Term**: bank **Ad Type**: Paid Search Edit Reset

Search Term	Phishing	Malware	Spam	Total Reach	URLs	Incidents ▼
citibank ecuador		✔		200	2	2
wachovia bank now		✔		200	2	2
hsbc bank loans	✔	✔		100	2	2
bank of america job search		✔		0	1	1
citibank cd interest rates		✔		50	1	1
citibank loan consolidation		✔		50	1	1
bank of america high interest		✔		50	1	1
chase bank money market interest rates		✔		16	1	1
bank of america cost charlotte building		✔		50	1	1
bank of america loans		✔		50	1	1
citibank drivers edge		✔		0	1	1

Overall Trends & Metrics



- 3X increase from 1 year ago
- Most agree problem is getting worse
- Trends show attackers changing tactics

Detection & Countermeasures

Apply - Detection

- Build a list of your affiliates, agents & partners
- Store metrics and performance data for each
- Regularly check the “reputation” of their web presence, mobile apps
- Implement scanning of partner websites, mobile apps and randomly test for fraud use-cases that apply to your business

Apply - Remediation

- Communicate your policy to partners
- Variable pricing models based on your metrics (developed during detection)
- Education. Non-technical users should understand the risks
- Shorten Tracking Durations, Lengthen Payment Cycles
- Lock the Front-Door. Stop the bad guys from getting back into your programs

Questions?