A Brief History of DNS Hijackings

Morgan Marquis-Boire

Whois Morgan?

Google™

Incident Response Team - Google

Penetration Tester for Security-Assessment.com

Linux / CA work for .gov.nz

Disclaimer

Google™

While this talk contains many examples specific to Google domains, none of these represent compromises of Google hosts or services.

This talk contains many real-world examples of domain hijacks. This is intended to highlight the systemic nature of this problem rather than specific security problems with any one organisation.

DNS Hijacking - Overview

Google™

Basic Concept

The practice of redirecting DNS lookups to other (rogue) DNS servers.

Actors and Motivations

Google™

Advertising

Monetization / Mass Click Fraud

Fraud

FBI arrests six for DNS hijacking scam worth $14 million

Posted on 10 November 2011.

BOOKMARK

Charges against six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries have been raised by the United States Attorney for the Southern District of New York.

Fraud

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

Actors and Motivations

Google™

Advertising

Monetization / Mass Click Fraud

Regular Fraud

ChronoPay DNS Hijack

Google

Russian e-Payment Giant ChronoPay Hacked

42 tweets
TOP ★5K
retweet

Criminals this week hijacked **ChronoPay.com**, the domain name for Russia's largest online payment processor, redirecting hundreds of unsuspecting visitors to a fake ChronoPay page that stole customer financial data.

Reached via phone in Moscow, ChronoPay chief executive Pavel Vrublevsky said the bogus payment page was up for several hours spanning December 25 and 26, during which time the attackers collected roughly 800 credit card numbers from customers visiting the site to make payments for various Russian businesses that rely on ChronoPay for processing.

In the attack, ChronoPay's domain was transferred to Network Solutions, and its domain name system (DNS) servers were changed to "anotherbeast.com," a domain registered at **Network Solutions** on Dec. 19, 2010.

ОБРАЩЕНИЕ К ПОЛЬЗОВАТЕЛЯМ CHRONOPAY.COM

Уважаемые пользователи!

Мы с сожалением вынуждены сообщить, что в период 25-26 декабря 2010 года в нашей компании произошел взлом базы данных, приведший к полной утечке всех имеющихся персональных данных пользователей Хронопей за 2009-2010 годы, включая полные номера кредитных карт и cvv-кодов.

В связи с произошедшей компрометацией базы данных кредитных карточек, для предотвращения массового списания злоумышленниками денег в период новогодних и рождественских праздников, мы рекомендуем выполнить следующие действия:

1. Незамедлительно позвонить в свой банк (телефон вы найдете на обратной стороне своей кредитной карты) и немедленно заблокировать ее.
2. Сообщить данную информацию всем своим знакомым, которые могли пользоваться нашей системой в указанный период, для того что бы они не потеряли свои деньги из-за действий злоумышленников.

Руководство нашей компании уже обратилось в правоохранительные органы и надеется на скорейшее расследование этого преступления.

В связи с произошедшим инцидентом руководством компании Хронопей принято решение временно прекратить работу на рынке приема платежей по пластиковым картам до прояснения ситуации.

Приносим самые искренние извинения своим партнерам и клиентам. Компания Хронопей готова возместить ущерб всем пострадавшим от инцидента сторонам в установленном законом порядке.

Actors and Motivations

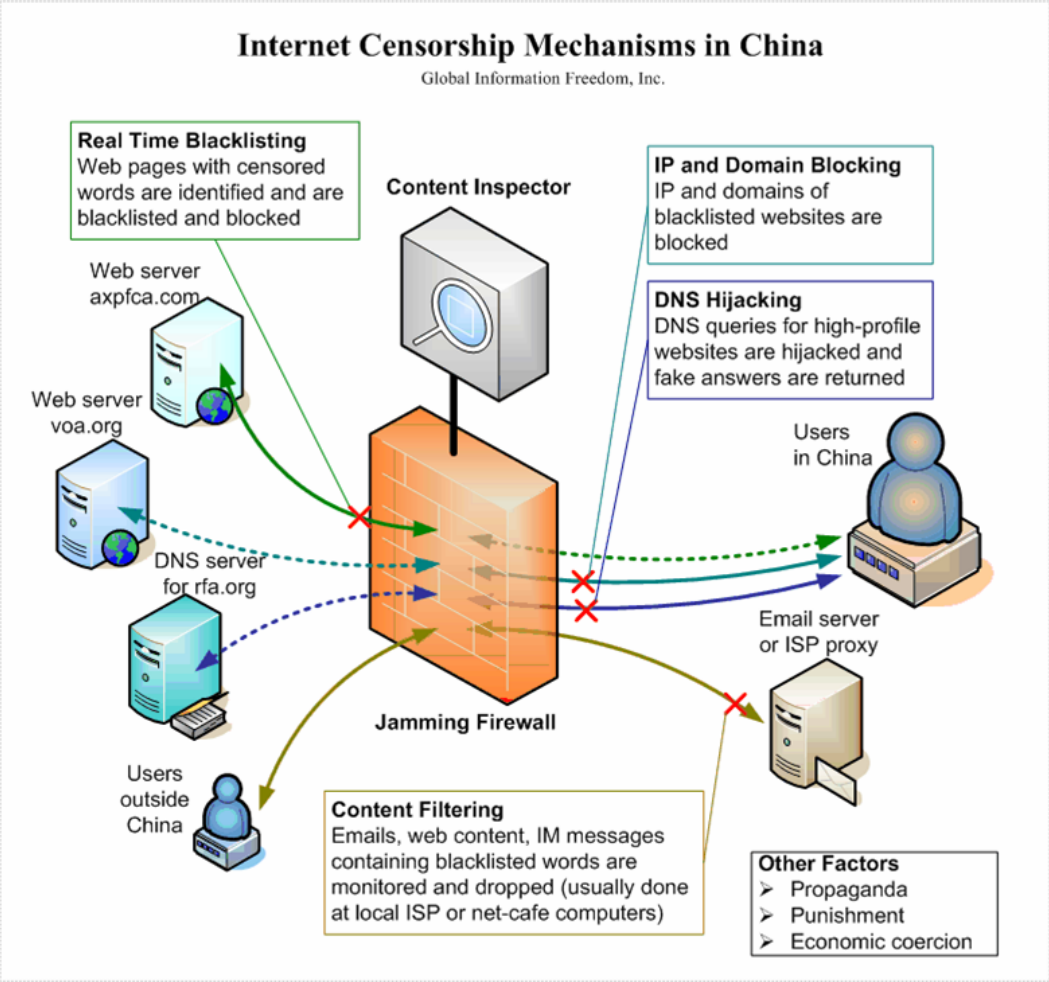
Google™

Advertising

Monetization / Mass Click Fraud / Fraud

Censorship

Censorship



Actors and Motivations

Google

Advertising

Monetization / Mass Click Fraud / Fraud

Censorship

Hacktivism / Defacement

Twitter - 18 December 2009

Actors and Motivations

Google™

Advertising

Monetization / Mass Click Fraud / Fraud

Censorship

Hacktivism / Defacement

Phishing

Account Access (Man-in-the-middle attacks)

Credentials

Google

Home > News > Security

August 13th, 2010, 09:25 GMT · By **Lucian Constantin**

Chinese Gmail Phishing Attack Employs DNS Hijacking

SHARE: Tweet

Adjust text size:

ENLARGE

Reports coming in from China suggest that an ongoing phishing attack targeting Gmail users in the country might employ some form of DNS hijacking.

According to New Tang Dynasty Television (NTDTV) [via Google Translate], when trying to access Google's email service by typing www.gmail.com into the browser address bar, users affected by this attack are redirected to a fake copy of the Gmail login page.

The fake page is hosted on a server (124.117.227.201) that is not owned by the search giant and loads content from a mail.google.com-sFmail-[LONG_PART]-ServerLogin.beij900.ndns01.com address.

Tunisia DNS Hijack

Google

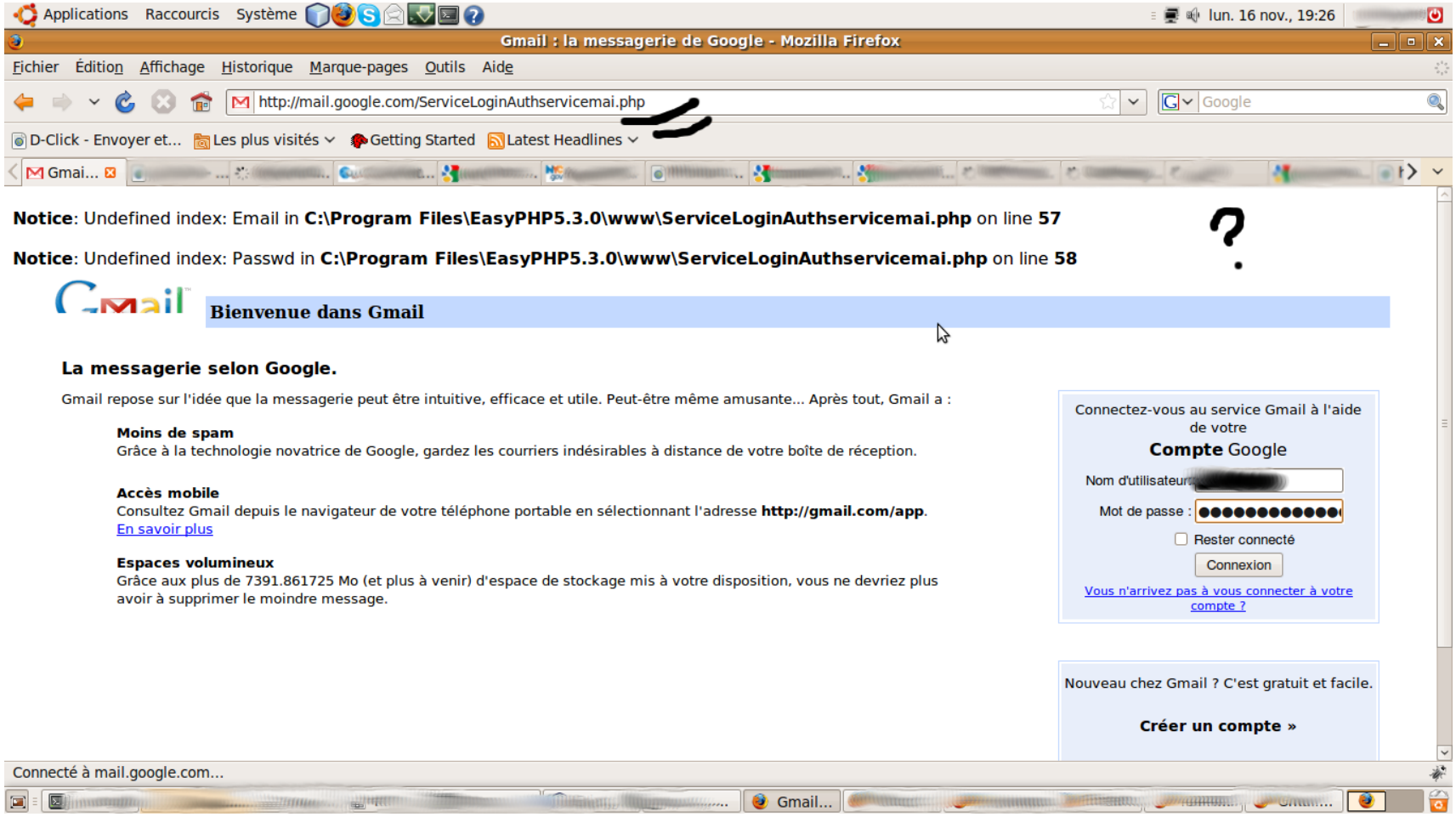
Tunisia, 25 December 2010

Facebook. Gmail. Etc.

Stealing an entire country's passwords.

Tunisia DNS Hijack

Google



Mass Domain Hijackings

Google™

Registry Hacking

Highly Effective

High Traffic domains under a compromise ccTLD.

Mass Domain Hijackings

Google™

Started tracking 3 years ago.

Simple code to monitor changes to Google-owned domains

Chronology

2009 - Morroco,Tunisia,Tajikistan, Ecuador, Kenya, New Zealand

2010 - Uganda, Puerto Rico, Denmark

2011 - Suriname, Malawi, Congo, Guadaloupe, Fiji, Bangladesh

2012 - Nepal

How does this happen

Misc software bugs

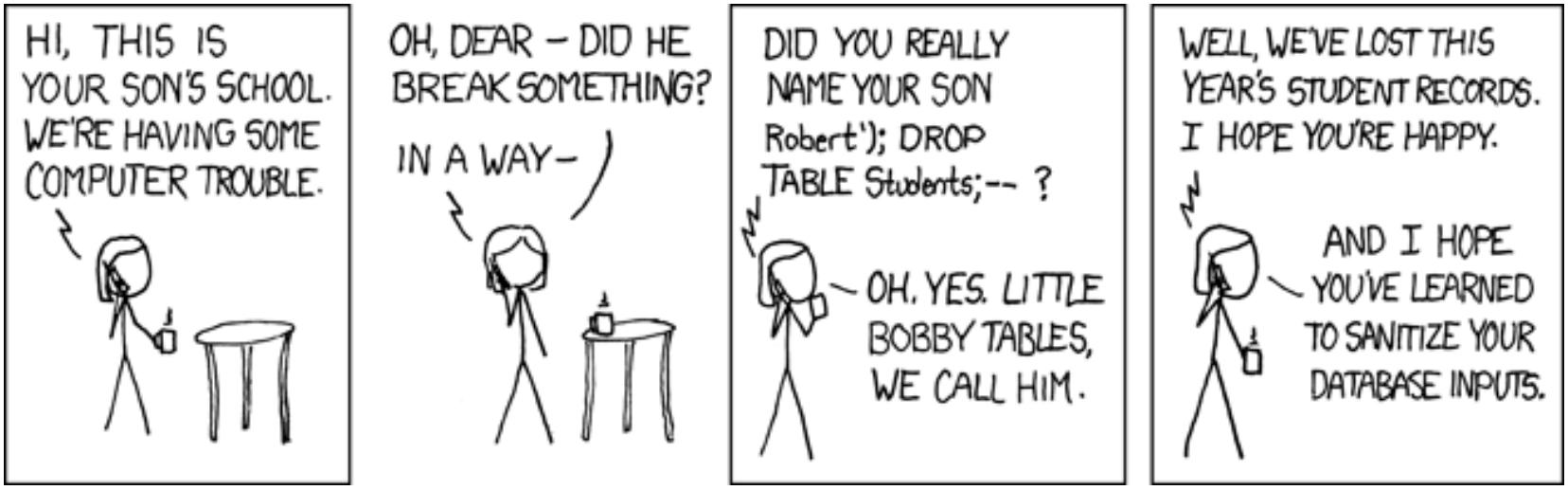
Password Re-use

Social Engineering

Bribery / coercion

SQL Injection

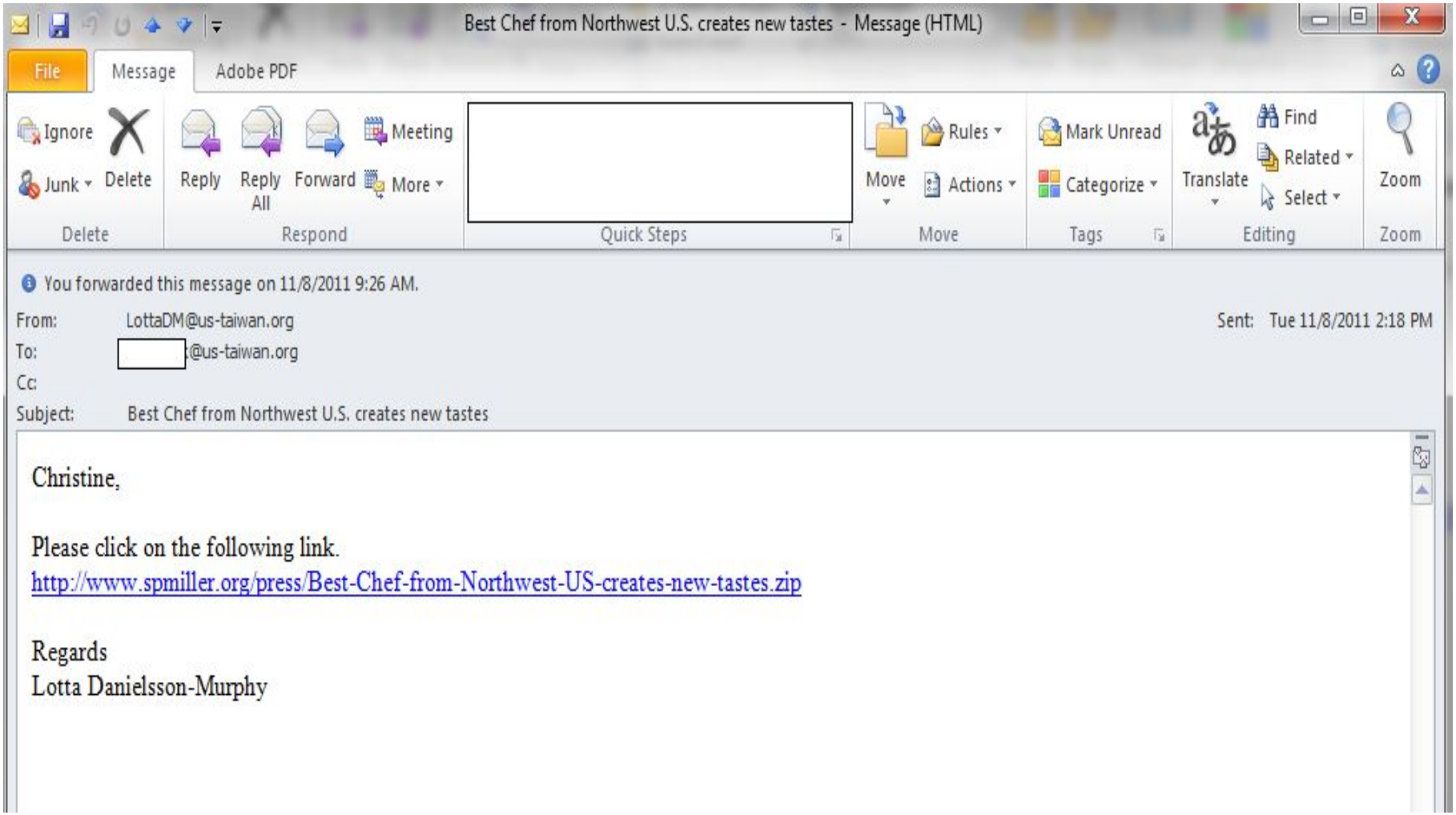
SQL Injection



https://xkcd.com/327/

Social Engineering

Google™



Effects

Google™

Mostly web defacement - bragging rights

Visibility for political causes

Monetize via spam / affiliate advertising

User credential / data theft


HACKED
By_Ogmass & S4S_7 & Spy
Cyber Mafia Crew Corp.
Özenen Deðil Daima Özenilen Oluruz.
google - tunus hacked ?
(:
uname -a ;
Linux webnx1 2.6.16.54-0.2.5-smp #1 SMP Mon Jan 21 13:29:51 UTC 2008 x86_64 x86_64 x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
Cyber Mafia Crew

File Edit View History Bookmarks Tools Help

http://www.google.com.tj/

lesbian vampire killers

Most Visited Getting Started Latest Headlines Digg menu openpacket[.]org Direct Net Vontu GNUCITIZEN Risky Business Security Wiki Corporate Machine ... Status for Discovery... WhoDoINotify Data Integrity and A...

Canon u... auschwit... Rule of t... DEFCON... Google T... Flickr Ph... Villa d'Es... GettingS... Research. Discuss ... Faceboo... Lesbian ... Email Re... Malware ... Google Zone-H.... DNS Hija... cPanel® [root...

Hacked !

Agd_Scorp & R x 5 & Thehacker & Cr@zy_King

ax3L & Zombie_KSA

[root@markmonitor:/Peace-Crew] # is back
[root@markmonitor:/Peace-Crew] # your system get down.!

Avlanma Zamani !

Thx: TilkiAndre, Kerem125, Jextoxic , Redrolix, Kacak , 4R!F, 4NT!W4R

Net^Devil, spo0fer , xOOmxOOm

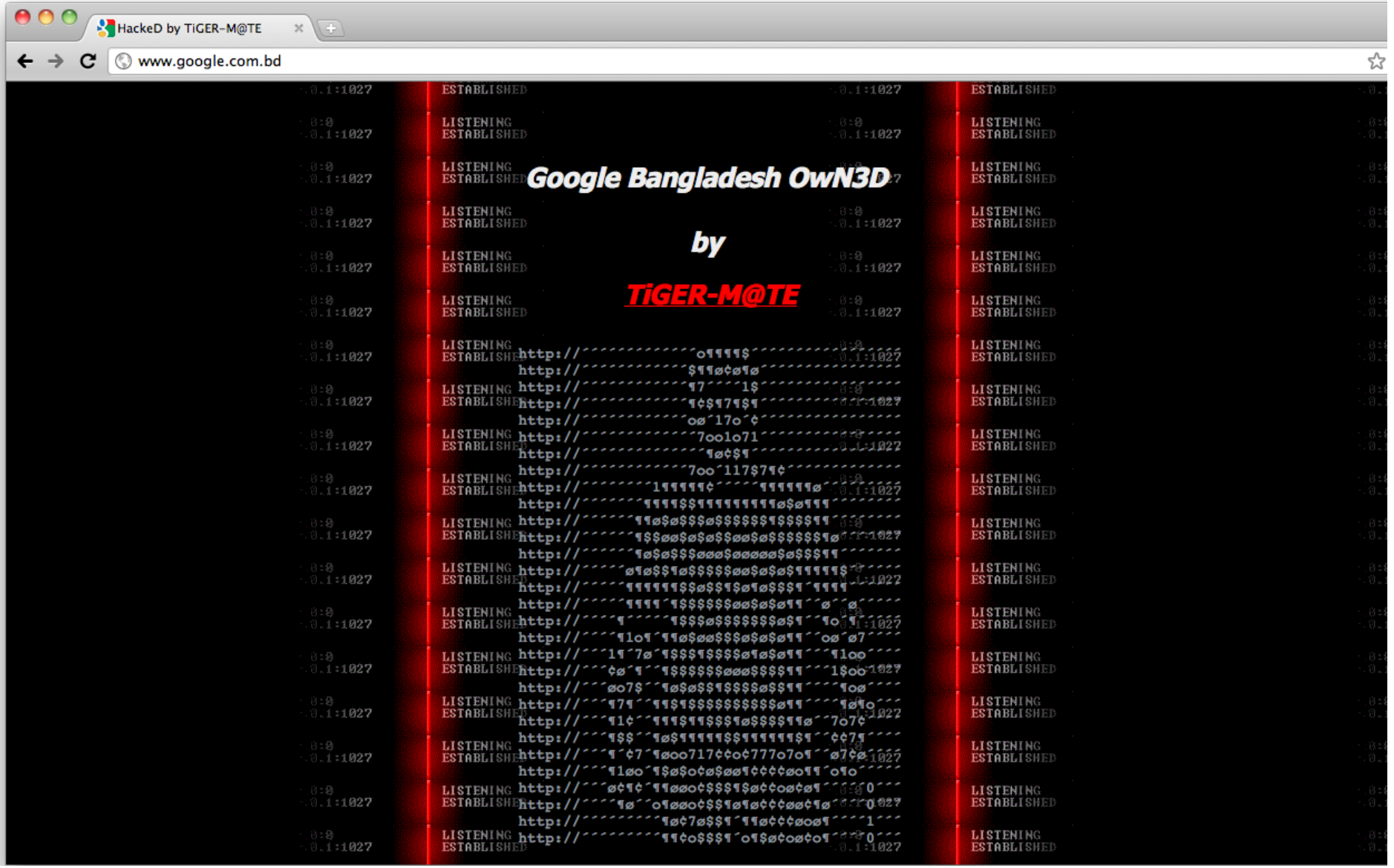
it ürür kervan yürür..

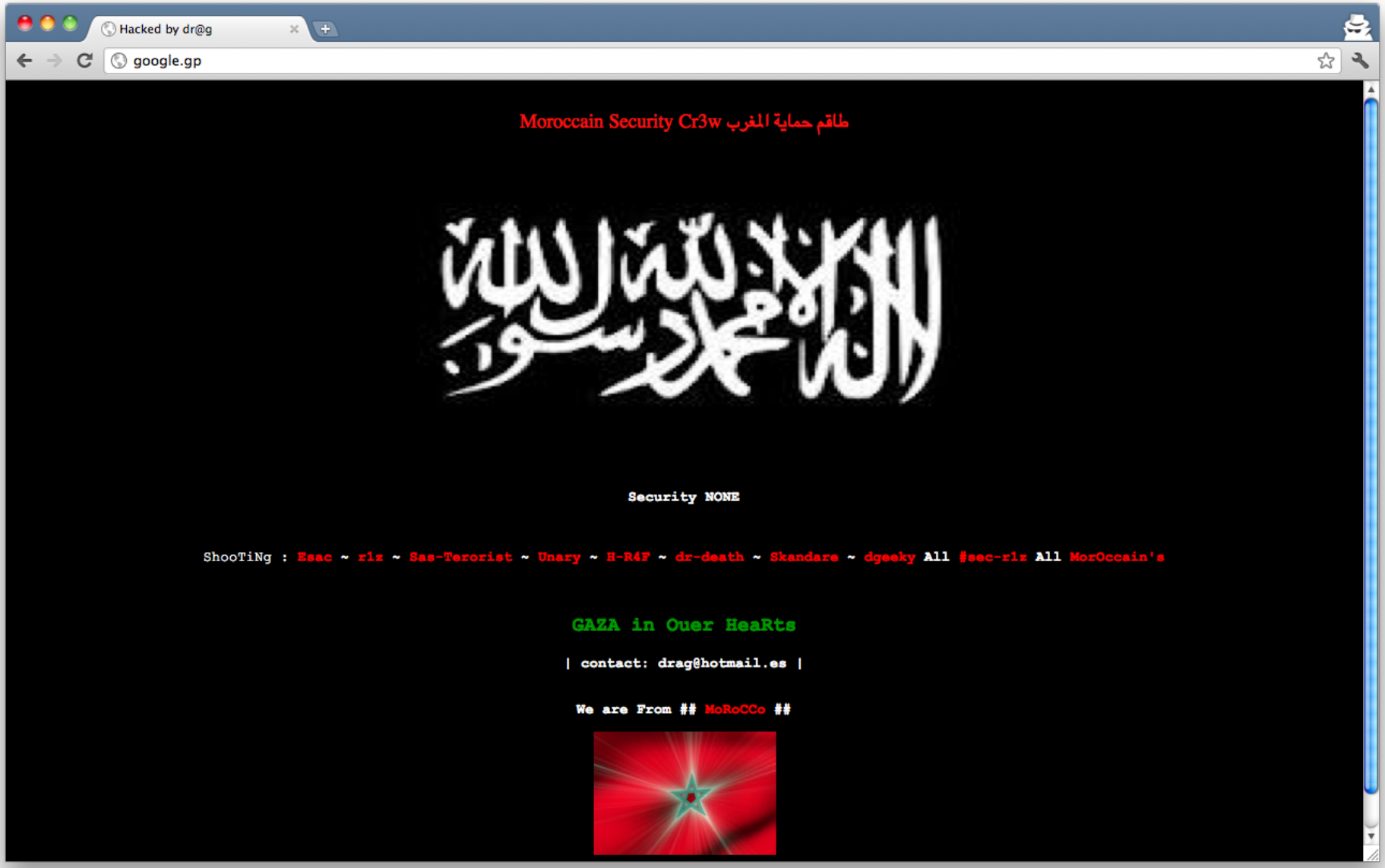
turkguvenligi.info

2000-2009

Find: Previous Next Highlight all Match case

Transferring data from kervangecmez.org...





google.cd

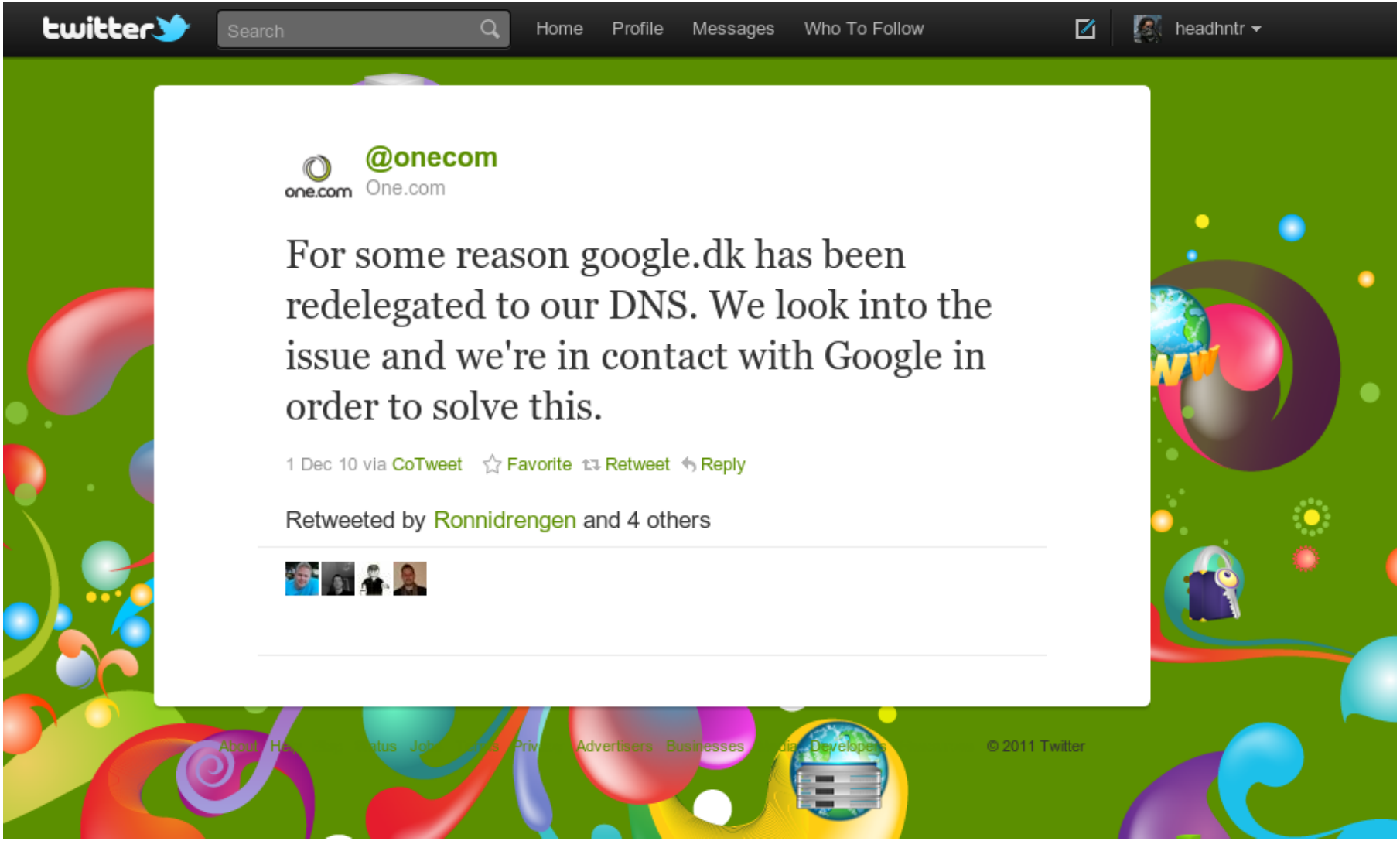
google.cd

The QuickTime plug-in needs your permission to run. Learn more

Always run on this site | Run this time

Haxored by AlpHaNiX
Nothing personal ,
#alpha_[A_T]_HACKER_[D_O_T]_bz

Tunisia Rullz



Press

Google

April 28, 2009, 8:04AM

Puerto Rico sites redirected in DNS attack

by Ryan Naraine

Comment Share

From CNet News (Elinor Mills)

An attack on the main domain name system registrar in Puerto Rico led to the local Web sites of Google, Microsoft, Yahoo, Coca-Cola, and other big companies being redirected for a few hours on Sunday to sites that were defaced, according to security firm Imperva.

Those sites and others including PayPal, Nike, Dell, and Nokia, were redirected to sites that were black except for messages in hacker lingo saying that the sites had been hacked. However, the sites themselves were not hacked, Amichai Shulman, chief technology officer at Imperva, said on Monday. Read the full story [cnet.com]

Press

Google

TechCrunch

HOME STARTUPS MOBILE GADGETS EUROPE

Hackers Temporarily Seize Control Of Google Morocco Domain Name

ROBIN WAUTERS

Saturday, May 9th, 2009 Comments

HackeD By PAKbugs

We Are: ZombiE_KsA Cyber Criminal spo0fer x00mx00m

GOOGLE MOROCO HACKED

Cyber-Criminal Was HERE

WWW.PAKBUGS.COM

(; We rock

Press

Google

ArabCrunch en
عرب كرنش

Home | Startups | Mobile | Social Media | Tech | Internet | Funding & VC

Breaking: Google Morocco Google.co.ma is Hacked!

9 May, 2009

Compound Problems

Google

Google Cautions Iranian Users After DigiNotar Hack Attack

First Posted: 09/ 9/11 06:35 PM ET ¦Updated: 09/ 9/11 06:44 PM ET

React > Inspiring | Funny | Obsolete | Scary | Must-Have | Amazing | Innovative | Nerdy

Follow > Cybersecurity , Google , Hackers , Iran , Video , Google Iran , Diginotar , Diginotar Hack , Diginotar Hacking , Diginotar Iran , Iran Google , Technology News

SHARE THIS STORY

Like 6 people like this. Be the first of your friends.

4 | 20 | 1 | 3

REUTERS

Google Inc is advising its Gmail email service customers in Iran to change their passwords in the wake of a cyberattack that has affected a major swath of the country.

Compound Problems

Google

Comodo

Diginotar

StartSSL

Trustwave

Compound Problems

Google™

SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate.

Why Should You Care?

Google™

Bad press.

DNS is trusted.

Trust is inherited from ICANN.

People die.

Solutions / Mitigations

Google™

Regular security audits

Registry in a box

Required minimum security posture

DNSSec

Google™

Questions / Comments ?