A Brief History of DNS Hijackings

Morgan Marquis-Boire
Whois Morgan?

Incident Response Team - Google

Penetration Tester for Security-Assessment.com

Linux / CA work for .gov.nz
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.
Basic Concept

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

Advertising

Monetization / Mass Click Fraud
Fraud

FBI arrests six for DNS hijacking scam worth $14 million

Posted on 10 November 2011.

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.

http://www.fbi.gov
http://www.fbi.gov/contact-us

123.456.789
987.654.321

Legitimate DNS
Actors and Motivations

Advertising

Monetization / Mass Click Fraud

Regular Fraud
ChronoPay DNS Hijack

Russian e-Payment Giant ChronoPay Hacked

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.
Actors and Motivations

Advertising

Monetization / Mass Click Fraud / Fraud

Censorship
Censorship

Internet Censorship Mechanisms in China

Real Time Blacklisting
Web pages with censored words are identified and are blacklisted and blocked

IP and Domain Blocking
IP and domains of blacklisted websites are blocked

DNS Hijacking
DNS queries for high-profile websites are hijacked and fake answers are returned

Content Filtering
Emails, web content, IM messages containing blacklisted words are monitored and dropped (usually done at local ISP or net-café computers)

Other Factors
- Propaganda
- Punishment
- Economic coercion

Users in China

Email server or ISP proxy

Users outside China

Web server axpfoa.com

Web server voa.org

DNS server for rfa.org

Jamming Firewall
Actors and Motivations

Advertising

Monetization / Mass Click Fraud / Fraud

Censorship

Hacktivism / Defacement
Twitter - 18 December 2009

IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iranian.cyber.army@gmail.com
Actors and Motivations

Advertising

Monetization / Mass Click Fraud / Fraud

Censorship

Hacktivism / Defacement

Phishing

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

Tunisia, 25 December 2010

Facebook. Gmail. Etc.

Stealing an entire country's passwords.
Tunisia DNS Hijack
Mass Domain Hijackings

Registry Hacking

Highly Effective

High Traffic domains under a compromise ccTLD.
Mass Domain Hijackings

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/
Christine,

Please click on the following link.

Regards
Lotta Danielsson-Murphy
Effects

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 Deedil 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)
Hacked!

Agd_Scorp & R x 5 & Thehacker & Cr@zy_King

ax3L & Zombie_KSA

[root@markmonter (Peace-Crew) #] is back.
[root@markmonter (Peace-Crew) #] your system got down!

Avarma Zamani!

Well damn...

Thx: TilidAndre, Kerem123, jexxiconic, Reddolix, Kacak, 4R!F, 4NT!W4R

Net* Devil, splotter, x00mx00m

# or ur kewler ur ur...
tukaweight.info

2000-2009
Moroccain Security Cr3w

Security NONE

ShooTingly: H3ac ~ r1x ~ Ssa-Terrorist ~ Uinary ~ H-R4P ~ dr-death ~ Skandare ~ dgeeky All #sec-r1x All MorOccain's

GAZA in Ouer Hearths

contact: drag@hotmail.es

We are From ## MoRoCCo ##
Haxored by AlpHaNix
Nothing personal.
#alpha_[ A_T ]_HACKER_[ D_O_T ]_bz

## Tunisia Rulz
For some reason google.dk has been redelegated to our DNS. We look into the issue and we're in contact with Google in order to solve this.
Puerto Rico sites redirected in DNS attack

by Ryan Naraine

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]
Hackers Temporarily Seize Control Of Google Morocco Domain Name

Saturday, May 9th, 2009

HackeD By PAKbugs

We Are: ZombiE_KsA Cyber Criminal spoofer x00mx00m

GOOGLE MOROCO HACKED

Cyber-Criminal Was HERE

WWW.PAKBUGS.COM

(; We rock
Breaking: Google Morocco Google.co.ma is Hacked!

9 May, 2009
Compound Problems

Google Cautions Iranian Users After DigiNotar Hack Attack

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

Comodo

Diginotar

StartSSL

Trustwave
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?

Bad press.

DNS is trusted.

Trust is inherited from ICANN.

People die.
Solutions / Mitigations

Regular security audits

Registry in a box

Required minimum security posture

DNSSec
Questions / Comments ?