black hat ASIA 2014

OFFENSIVE: Exploiting changes on DNS server configuration

Leonardo Nve Egea

S21sec

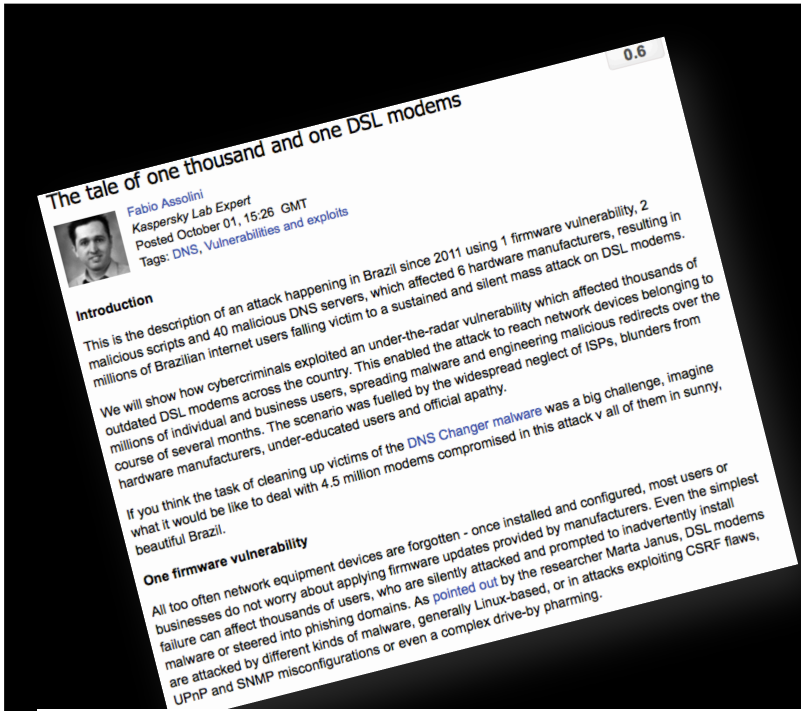
Leonardo.nve@gmail.com
@leonardonve

About me

- Security researcher since… (a lot of time) in SPAIN.
- Pentester & Incident researcher
- At the Offensive side (more funny).
- I love protocol level.

INTRODUCTION

What.



The tale of one thousand and one DSL modems

0.6

Fabio Assolini
Kaspersky Lab Expert
Posted October 01, 15:26 GMT
Tags: DNS, Vulnerabilities and exploits

Introduction

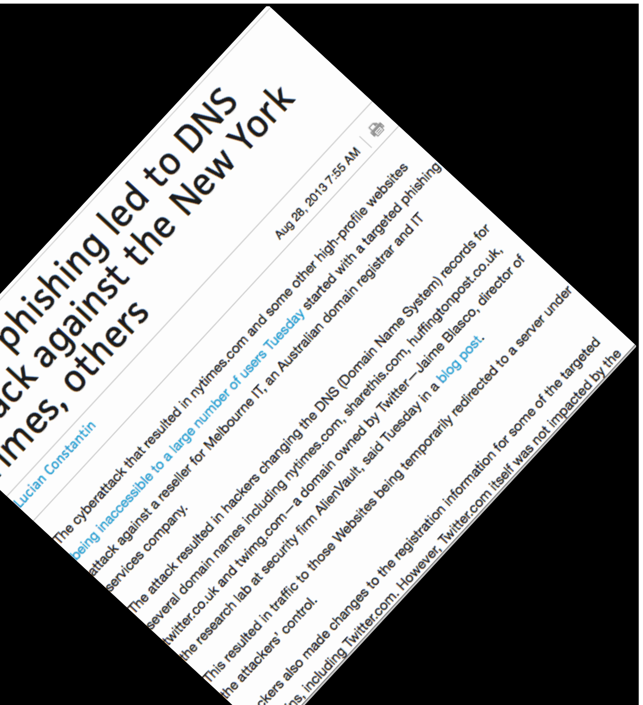
This is the description of an attack happening in Brazil since 2011 using 1 firmware vulnerability, 2 malicious scripts and 40 malicious DNS servers, which affected 6 hardware manufacturers, resulting in millions of Brazilian internet users falling victim to a sustained and silent mass attack on DSL modems.

We will show how cybercriminals exploited an under-the-radar vulnerability which affected thousands of outdated DSL modems across the country. This enabled the attack to reach network devices belonging to millions of individual and business users, spreading malware and engineering malicious redirects over the course of several months. The scenario was fuelled by the widespread neglect of ISPs, blunders from hardware manufacturers, under-educated users and official apathy.

If you think the task of cleaning up victims of the DNS Changer malware was a big challenge, imagine what it would be like to deal with 4.5 million modems compromised in this attack v all of them in sunny, beautiful Brazil.

One firmware vulnerability

All too often network equipment devices are forgotten - once installed and configured, most users or businesses do not worry about applying firmware updates provided by manufacturers. Even the simplest failure can affect thousands of users, who are silently attacked and prompted to inadvertently install malware or steered into phishing domains. As pointed out by the researcher Marta Janus, DSL modems are attacked by different kinds of malware, generally Linux-based, or in attacks exploiting CSRF flaws, UPnP and SNMP misconfigurations or even a complex drive-by pharming.



Spear phishing led to DNS attack against the New York Times, others

Lucian Constantin

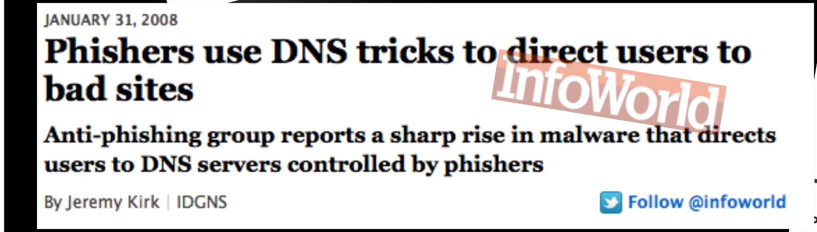
Aug 28, 2013 7:55 AM

The cyberattack that resulted in nytimes.com and some other high-profile websites being inaccessible to a large number of users Tuesday started with a targeted phishing attack against a reseller for Melbourne IT, an Australian domain registrar and IT services company.

The attack resulted in hackers changing the DNS (Domain Name System) records for several domain names including nytimes.com, sharethis.com, huffingtonpost.co.uk, twitter.co.uk and twimg.com—a domain owned by Twitter—Jaime Blasco, director of the research lab at security firm AlienVault, said Tuesday in a blog post.

This resulted in traffic to those Websites being temporarily redirected to a server under the attackers' control.

Hackers also made changes to the registration information for some of the targeted domains, including Twitter.com. However, Twitter.com itself was not impacted by the



JANUARY 31, 2008

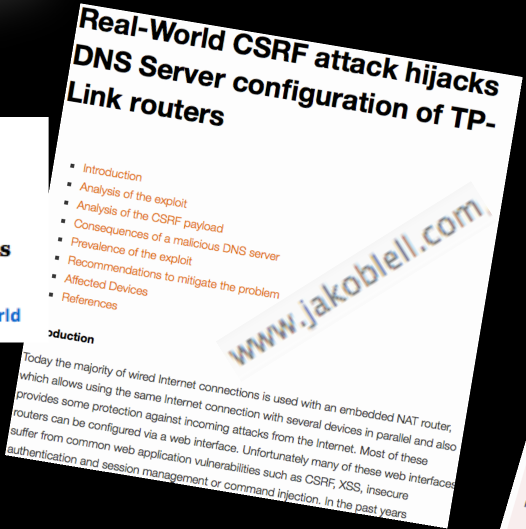
Phishers use DNS tricks to direct users to bad sites

InfoWorld

Anti-phishing group reports a sharp rise in malware that directs users to DNS servers controlled by phishers

By Jeremy Kirk | IDGNS

Follow @infoworld



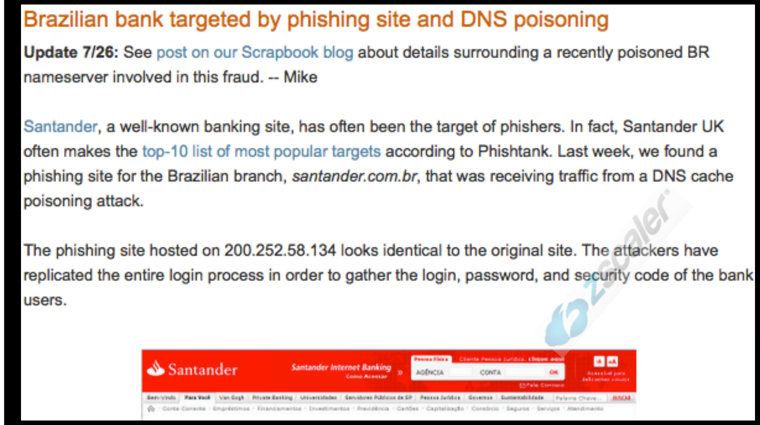
Real-World CSRF attack hijacks DNS Server configuration of TP-Link routers

- Introduction
- Analysis of the exploit
- Analysis of the CSRF payload
- Consequences of a malicious DNS server
- Prevalence of the exploit
- Recommendations to mitigate the problem
- Affected Devices
- References

www.jakoblell.com

oduction

Today the majority of wired Internet connections is used with an embedded NAT router, which allows using the same Internet connection with several devices in parallel and also provides some protection against incoming attacks from the Internet. Most of these routers can be configured via a web interface. Unfortunately many of these web interfaces suffer from common web application vulnerabilities such as CSRF, XSS, insecure authentication and session management or command injection. In the past years



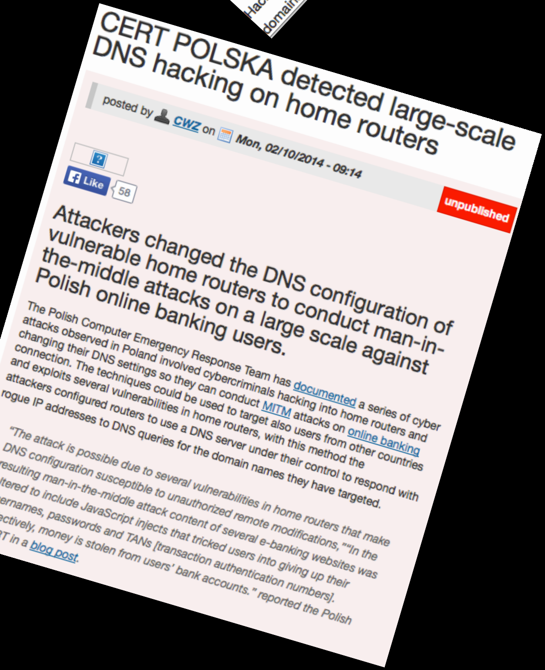
Brazilian bank targeted by phishing site and DNS poisoning

Update 7/26: See post on our Scrapbook blog about details surrounding a recently poisoned BR nameserver involved in this fraud. -- Mike

Santander, a well-known banking site, has often been the target of phishers. In fact, Santander UK often makes the top-10 list of most popular targets according to Phishtank. Last week, we found a phishing site for the Brazilian branch, *santander.com.br*, that was receiving traffic from a DNS cache poisoning attack.

The phishing site hosted on 200.252.58.134 looks identical to the original site. The attackers have replicated the entire login process in order to gather the login, password, and security code of the bank users.

zscaler



CERT POLSKA detected large-scale DNS hacking on home routers

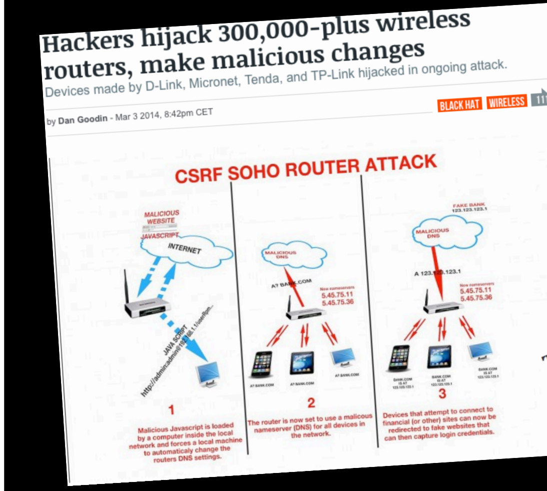
posted by CWZ on Mon, 02/10/2014 - 09:14

Attackers changed the DNS configuration of vulnerable home routers to conduct man-in-the-middle attacks on a large scale against Polish online banking users.

The Polish Computer Emergency Response Team has documented a series of cyber attacks observed in Poland involved cybercriminals hacking into home routers and changing their DNS settings so they can conduct MITM attacks on online banking connection. The techniques could be used to target also users from other countries and exploits several vulnerabilities in home routers, with this method the attackers configured routers to use a DNS server under their control to respond with rogue IP addresses to DNS queries for the domain names they have targeted.

"The attack is possible due to several vulnerabilities in home routers that make DNS configuration susceptible to unauthorized remote modifications,""In the resulting man-in-the-middle attack content of several e-banking websites was altered to include JavaScript injects that tricked users into giving up their usernames, passwords and TANs [transaction authentication numbers]. Effectively, money is stolen from users' bank accounts." reported the Polish CERT in a blog post.

Why.



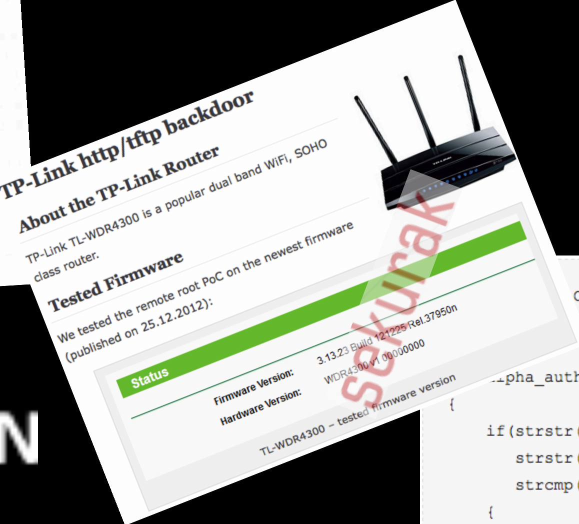
Hackers hijack 300,000-plus wireless routers, make malicious changes

Devices made by D-Link, Micronet, Tenda, and TP-Link hijacked in ongoing attack.

by Dan Goodin - Mar 3 2014, 8:42pm CET

BLACK HAT WIRELESS 111

CSRF SOHO ROUTER ATTACK
MALICIOUS WEBSITE
JAVASCRIPT
INTERNET
JAVA SCRIPT
http://admin:admin@192.168.1.1/userRpm...
1
Malicious Javascript is loaded by a computer inside the local network and forces a local machine to automaticaly change the routers DNS settings.
MALICIOUS DNS
A? BANK.COM
New nameservers 5.45.75.11 5.45.75.36
2
The router is now set to use a malicous nameserver (DNS) for all devices in the network.
FAKE BANK 123.123.123.1
MALICIOUS DNS
A 123.123.123.1
New nameservers 5.45.75.11 5.45.75.36
BANK.COM IS AT 123.123.123.1
3
Devices that attempt to connect to financial (or other) sites can now be redirected to fake websites that can then capture login credentials.



TP-Link http/tftp backdoor

About the TP-Link Router

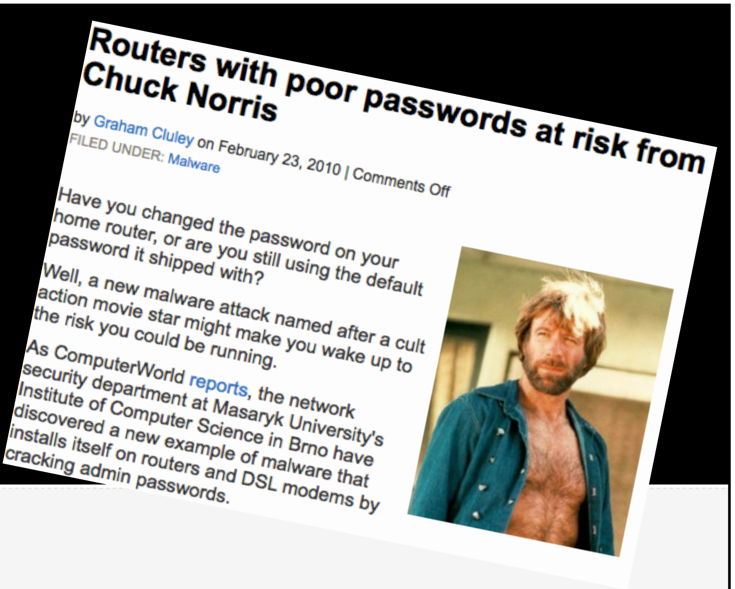
TP-Link TL-WDR4300 is a popular dual band WiFi, SOHO class router.

Tested Firmware

We tested the remote root PoC on the newest firmware (published on 25.12.2012):

Status
Firmware Version: 3.13.23 Build 121225 Rel.37950n
Hardware Version: WDR4300 v1 00000000

TL-WDR4300 – tested firmware version



Routers with poor passwords at risk from Chuck Norris

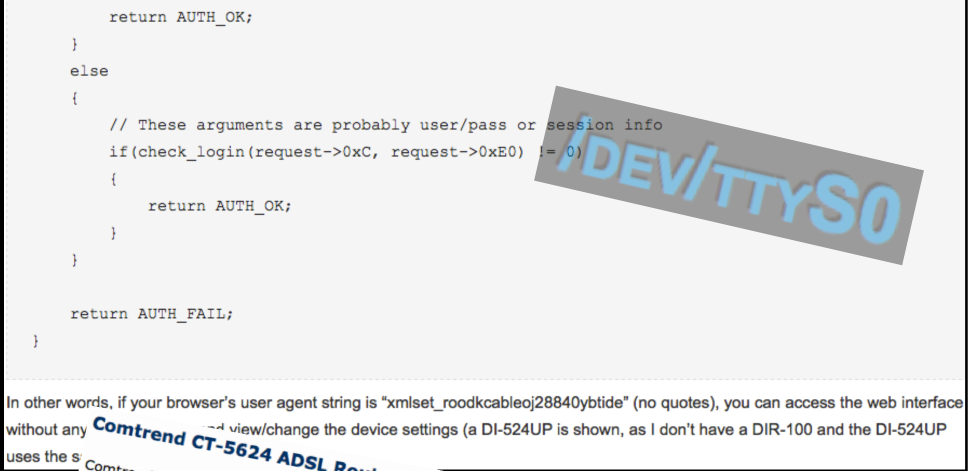
by Graham Cluley on February 23, 2010 | Comments Off
FILED UNDER: Malware

Have you changed the password on your home router, or are you still using the default password it shipped with?

Well, a new malware attack named after a cult action movie star might make you wake up to the risk you could be running.

As ComputerWorld reports, the network security department at Masaryk University's Institute of Computer Science in Brno have discovered a new example of malware that installs itself on routers and DSL modems by cracking admin passwords.

SHODAN



```
OK 1
AIL -1

lpha_auth_check(struct http_request_t *request)
{
    if(strstr(request->url, "graphic/") ||
       strstr(request->url, "public/") ||
       strcmp(request->user_agent, "xmlset_roodkcableoj28840ybtide") == 0)
    {
        return AUTH_OK;
    }
    else
    {
        // These arguments are probably user/pass or session info
        if(check_login(request->0xC, request->0xE0) != 0)
        {
            return AUTH_OK;
        }
    }

    return AUTH_FAIL;
}
```

In other words, if your browser's user agent string is "xmlset_roodkcableoj28840ybtide" (no quotes), you can access the web interface without any view/change the device settings (a DI-524UP is shown, as I don't have a DIR-100 and the DI-524UP uses the s

WRT120N fprintf Stack Overflow

By Craig | February 19, 2014 | Embedded Systems, Security, Tutorials

Vulnerability Details : CVE-2010-0470 (1 public exploit)

Cross-site scripting (XSS) vulnerability in scvrtsrv.cmd in Comtrend CT-507IT ADSL Router allows remote attackers to inject arbitrary web script or HTML via the srvName parameter.

Publish Date : 2010-02-02 Last Update Date : 2010-02-03

Comtrend CT-5624 ADSL Router 'password.c' Root Password Disclosure Vulnerability

Comtrend CT-5624 ADSL Router is prone to a password-disclosure vulnerability due to a design error.

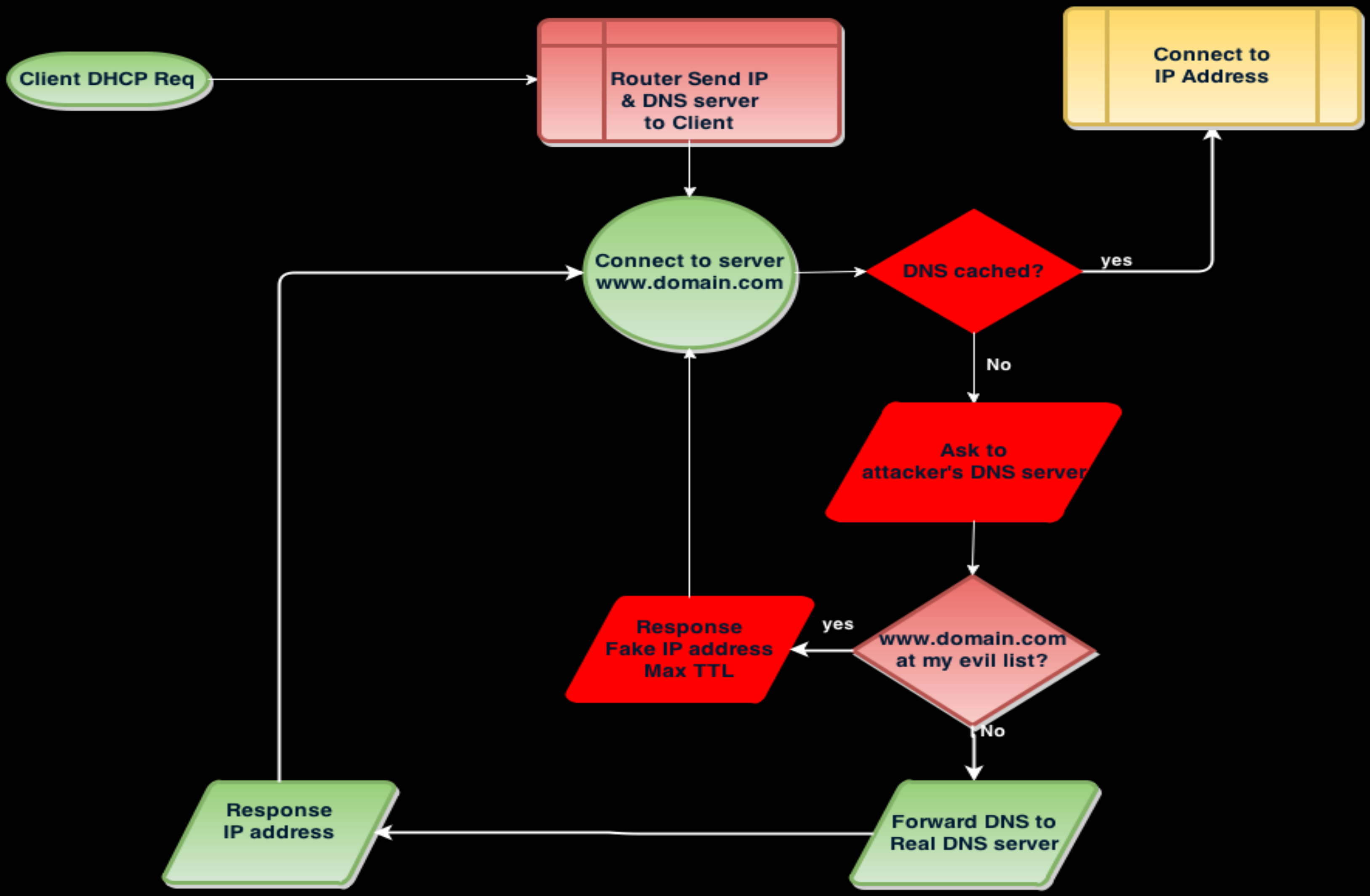
Attackers can exploit this issue to obtain sensitive information. Successfully exploiting this issue may lead to other attacks.

EXPLOITATION (I) NORMAL PROCEDURE

How.

- CSRF/XSS.
- Insufficient authorization.
- SNMP/TFTP.
- Default password + external administration.
- Cracking wifi passwords + default password.
- Command line DNS change.
- Rogue DSLAM.
- Malware.

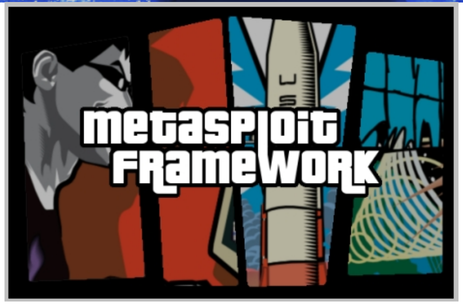
What.


Client DHCP Req
Router Send IP & DNS server to Client
Connect to IP Address
Connect to server www.domain.com
DNS cached?
yes
No
Ask to attacker's DNS server
Response Fake IP address Max TTL
yes
www.domain.com at my evil list?
No
Response IP address
Forward DNS to Real DNS server

black hat ASIA 2014

Tools.

- Metasploit.



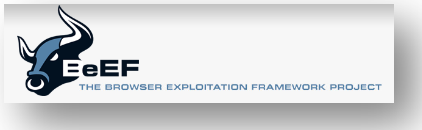
- Dnsmasq.

- Bind server.

Then.

- Invisible proxy.
  - Burp suite, mitmproxy
- SSLstrip.
- HTML injection.
  - BeEF
  - Exploit kits
- Bouncing to known servers.
  - SSLsplit
- Fake web servers.
  - defacing.
  - Phishing
- Sniffing data.

BURPSUITE
FREE EDITION
Burp Suite Free Edition v1.5
© PortSwigger Ltd. All rights reserved

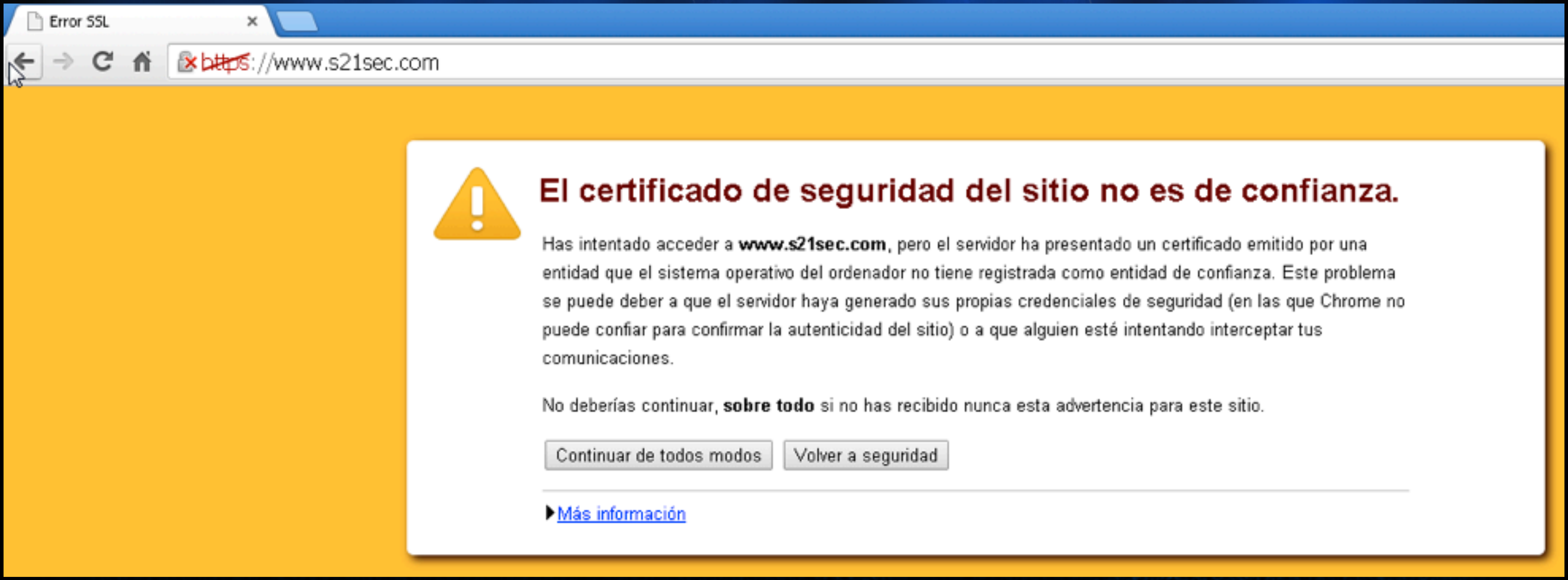


black hat ASIA 2014

OBSTACLES OF NORMAL EXPLOITATION

Obstacles.

- SSL certificates (Critical).



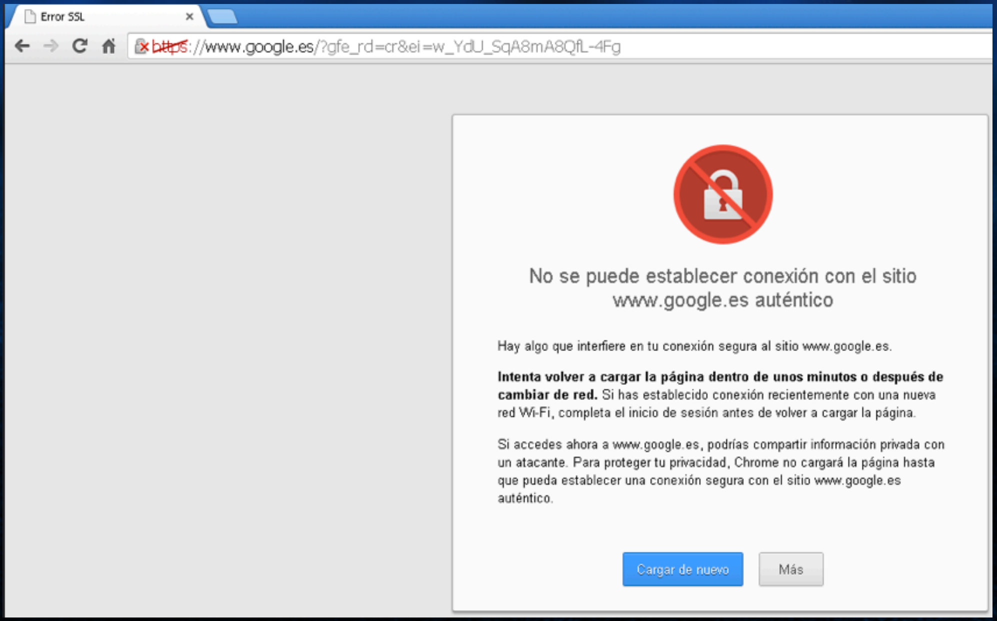
El certificado de seguridad del sitio no es de confianza.

Has intentado acceder a **www.s21sec.com**, pero el servidor ha presentado un certificado emitido por una entidad que el sistema operativo del ordenador no tiene registrada como entidad de confianza. Este problema se puede deber a que el servidor haya generado sus propias credenciales de seguridad (en las que Chrome no puede confiar para confirmar la autenticidad del sitio) o a que alguien esté intentando interceptar tus comunicaciones.

No deberías continuar, **sobre todo** si no has recibido nunca esta advertencia para este sitio.

Obstacles.

- SSL certificate pinning / EMET (Critical).



~~https~~://www.google.es/?gfe_rd=cr&ei=w_YdU_SqA8mA8QfL-4Fg

No se puede establecer conexión con el sitio www.google.es auténtico

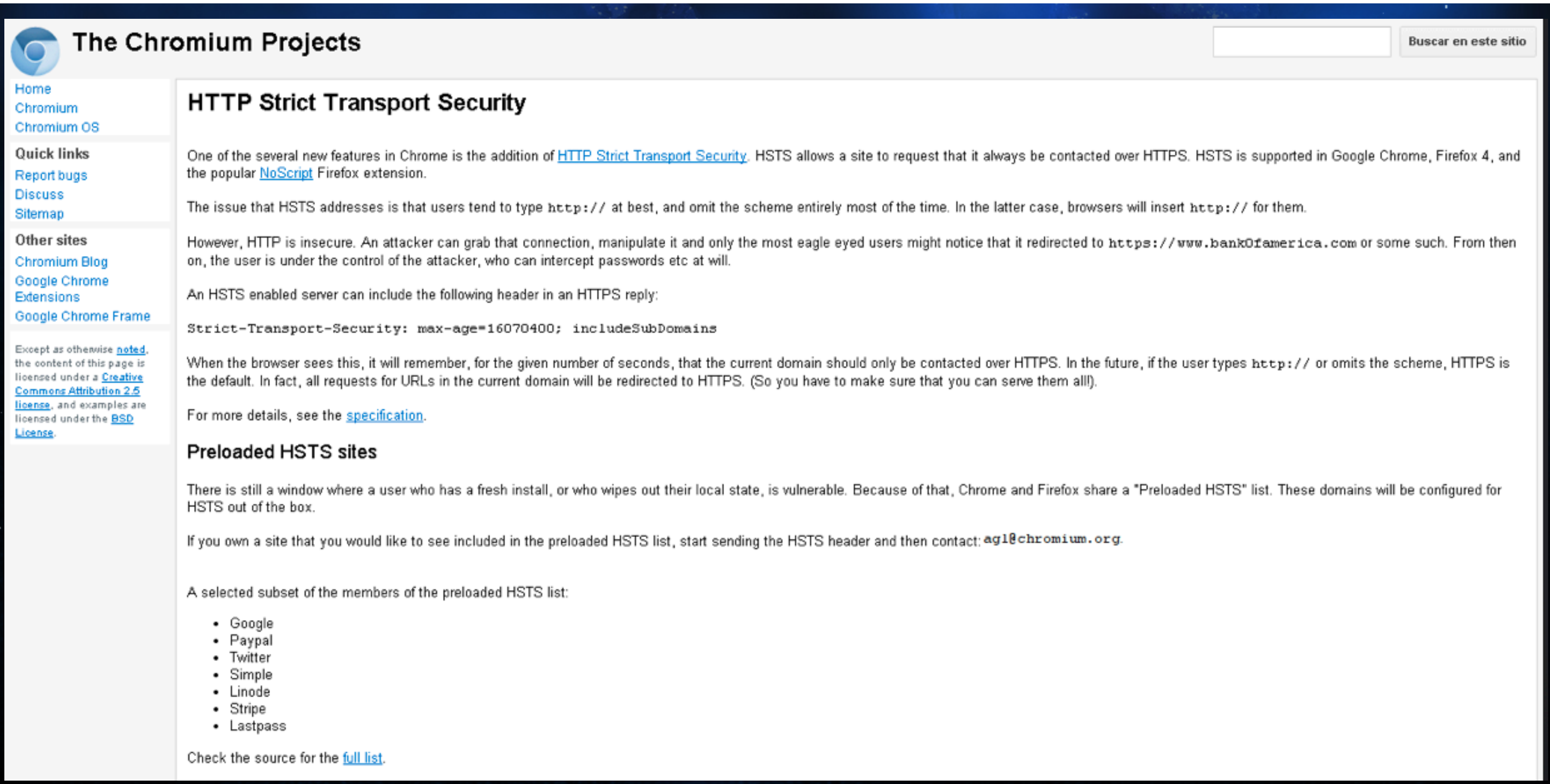
Hay algo que interfiere en tu conexión segura al sitio www.google.es.

Intenta volver a cargar la página dentro de unos minutos o después de cambiar de red. Si has establecido conexión recientemente con una nueva red Wi-Fi, completa el inicio de sesión antes de volver a cargar la página.

Si accedes ahora a www.google.es, podrías compartir información privada con un atacante. Para proteger tu privacidad, Chrome no cargará la página hasta que pueda establecer una conexión segura con el sitio www.google.es auténtico.

Obstacles.

- HSTS + Preloaded HSTS sites (Non critical).



HTTP Strict Transport Security

One of the several new features in Chrome is the addition of HTTP Strict Transport Security. HSTS allows a site to request that it always be contacted over HTTPS. HSTS is supported in Google Chrome, Firefox 4, and the popular NoScript Firefox extension.

The issue that HSTS addresses is that users tend to type `http://` at best, and omit the scheme entirely most of the time. In the latter case, browsers will insert `http://` for them.

However, HTTP is insecure. An attacker can grab that connection, manipulate it and only the most eagle eyed users might notice that it redirected to `https://www.bank0famerica.com` or some such. From then on, the user is under the control of the attacker, who can intercept passwords etc at will.

An HSTS enabled server can include the following header in an HTTPS reply:

```
Strict-Transport-Security: max-age=16070400; includeSubDomains
```

When the browser sees this, it will remember, for the given number of seconds, that the current domain should only be contacted over HTTPS. In the future, if the user types `http://` or omits the scheme, HTTPS is the default. In fact, all requests for URLs in the current domain will be redirected to HTTPS. (So you have to make sure that you can serve them all!).

For more details, see the specification.

Preloaded HSTS sites

There is still a window where a user who has a fresh install, or who wipes out their local state, is vulnerable. Because of that, Chrome and Firefox share a "Preloaded HSTS" list. These domains will be configured for HSTS out of the box.

If you own a site that you would like to see included in the preloaded HSTS list, start sending the HSTS header and then contact: `agl@chromium.org`.

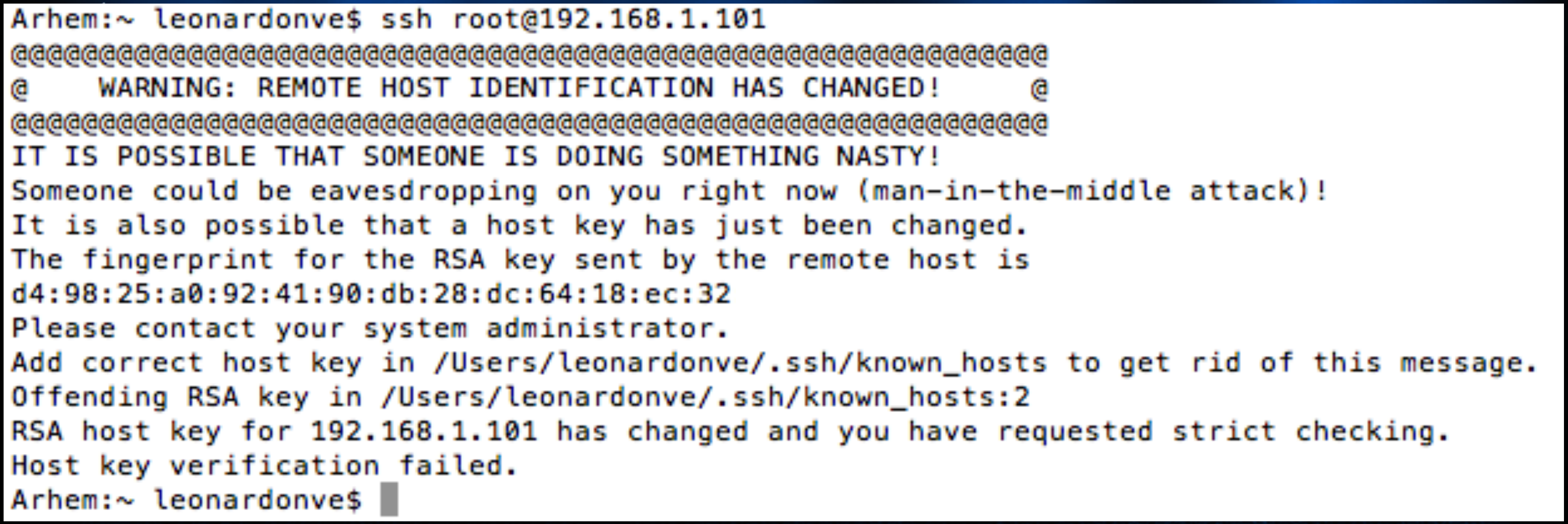
A selected subset of the members of the preloaded HSTS list:

- Google
- Paypal
- Twitter
- Simple
- Linode
- Stripe
- Lastpass

Check the source for the full list.

Obstacles.

- SSH signatures failure (Critical).



```
Arhem:~ leonardonve$ ssh root@192.168.1.101
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
d4:98:25:a0:92:41:90:db:28:dc:64:18:ec:32
Please contact your system administrator.
Add correct host key in /Users/leonardonve/.ssh/known_hosts to get rid of this message.
Offending RSA key in /Users/leonardonve/.ssh/known_hosts:2
RSA host key for 192.168.1.101 has changed and you have requested strict checking.
Host key verification failed.
Arhem:~ leonardonve$
```

Obstacles.

- POP3/SMTP Banner (Non critical problem).
- FTP Banner (This can be critical).
- Limited host interception.
- Limited protocol interception.

Limitations.

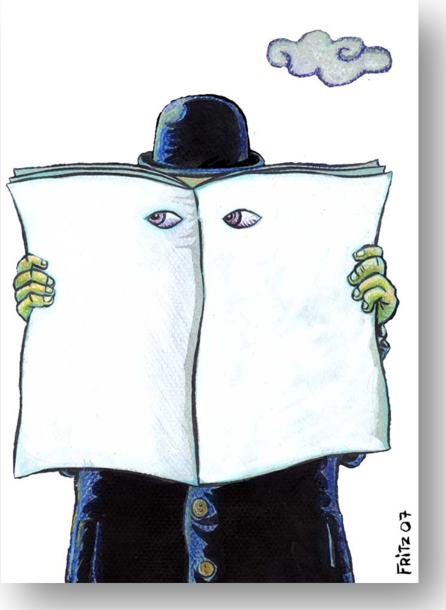
- Limited of hosts interception.
- Time to study IP communication manners.
- Limited cleartext protocols interception.
- No SSL & ciphered protocols interception.
- Accept the loose of a lot information.

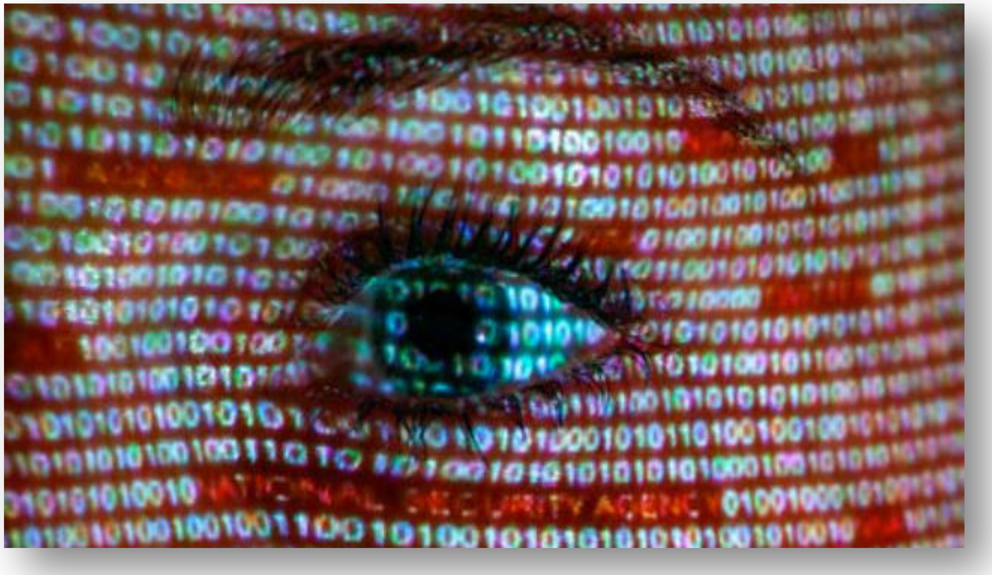
black hat ASIA 2014

EXPLOITATION (II)
IMPROVE THE ATTACK PROCEDURE

Objectives.

- Discretion.

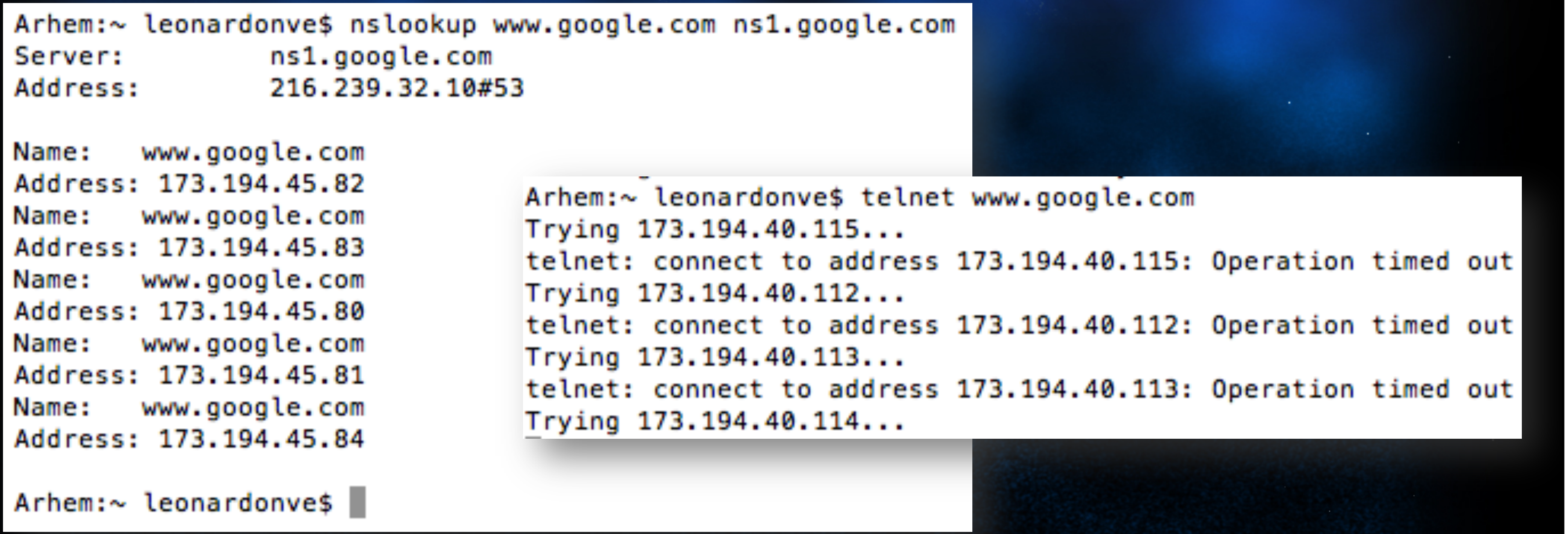




- Improve data acquisitions from time 0.

Improve the attack.

- A DNS feature for high availability:



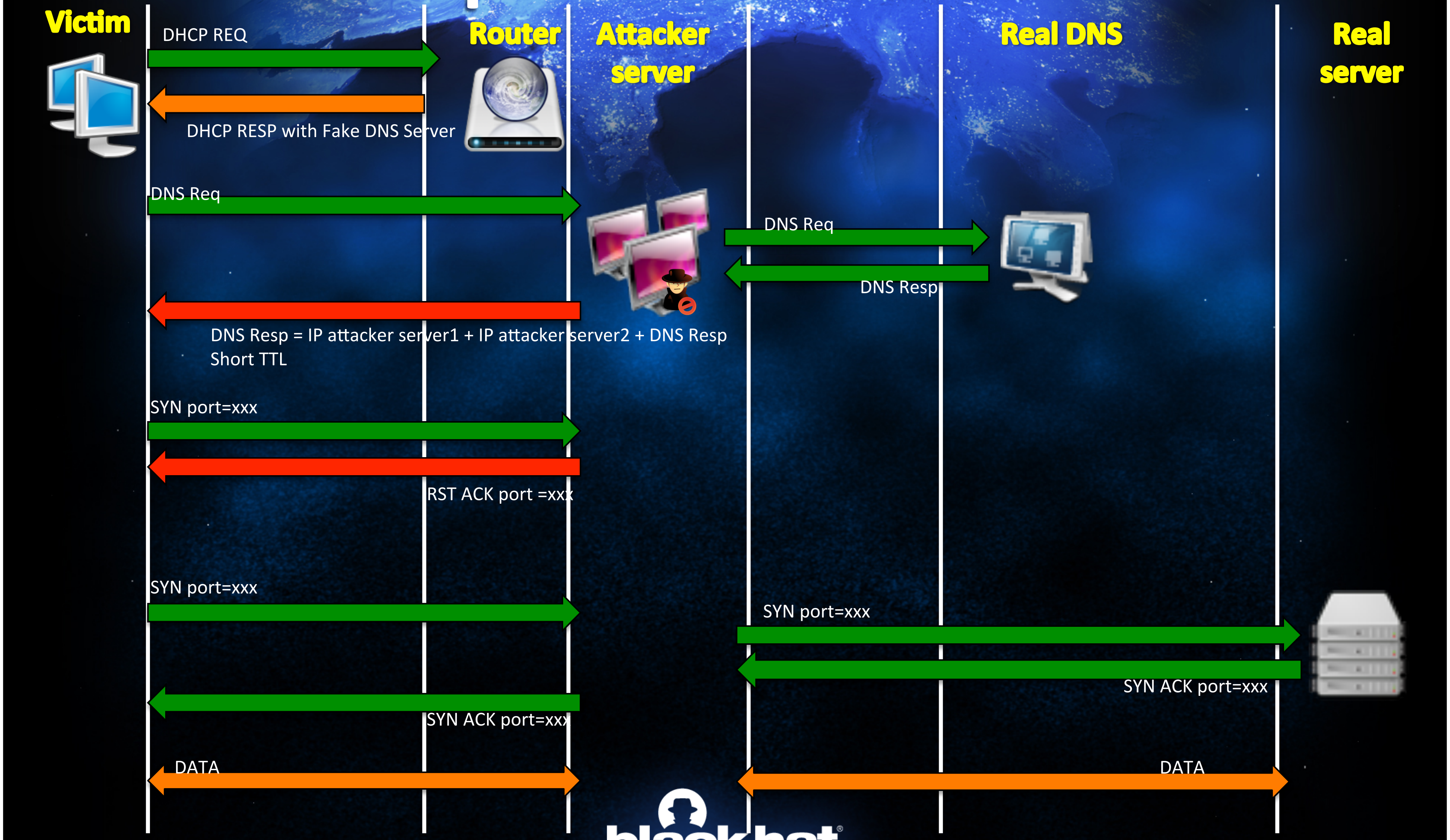
```
Arhem:~ leonardonve$ nslookup www.google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   www.google.com
Address: 173.194.45.82
Name:   www.google.com
Address: 173.194.45.83
Name:   www.google.com
Address: 173.194.45.80
Name:   www.google.com
Address: 173.194.45.81
Name:   www.google.com
Address: 173.194.45.84

Arhem:~ leonardonve$
```

```
Arhem:~ leonardonve$ telnet www.google.com
Trying 173.194.40.115...
telnet: connect to address 173.194.40.115: Operation timed out
Trying 173.194.40.112...
telnet: connect to address 173.194.40.112: Operation timed out
Trying 173.194.40.113...
telnet: connect to address 173.194.40.113: Operation timed out
Trying 173.194.40.114...
```

Improve the attack.



Victim

Router

Attacker server

Real DNS

Real server

DHCP REQ

DHCP RESP with Fake DNS Server

DNS Req

DNS Req

DNS Resp

DNS Resp = IP attacker server1 + IP attacker server2 + DNS Resp
Short TTL

SYN port=xxx

RST ACK port =xxx

SYN port=xxx

SYN port=xxx

SYN ACK port=xxx

SYN ACK port=xxx

DATA

DATA

Improve the attack.

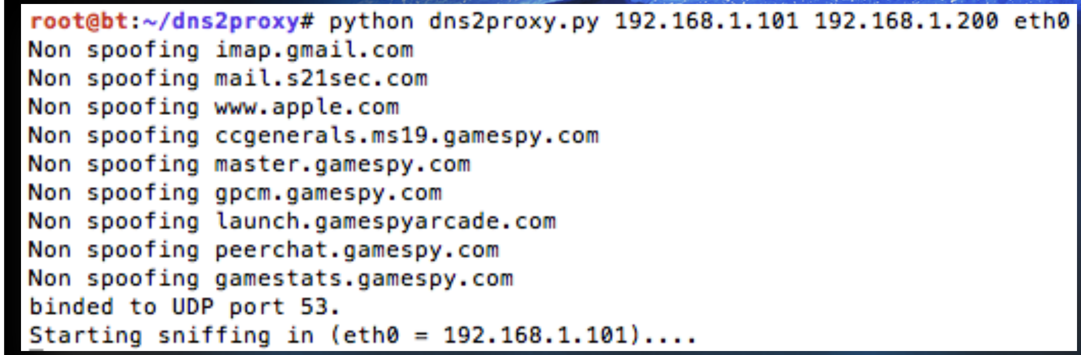
- On port 80 the attacker can put a invisible proxy.
- The attacker can reject SSL ports always because the client will later connect to the real server.
- Other connections data will be forward through the evil server since the first moment.
- And there is a tool.

Tool.

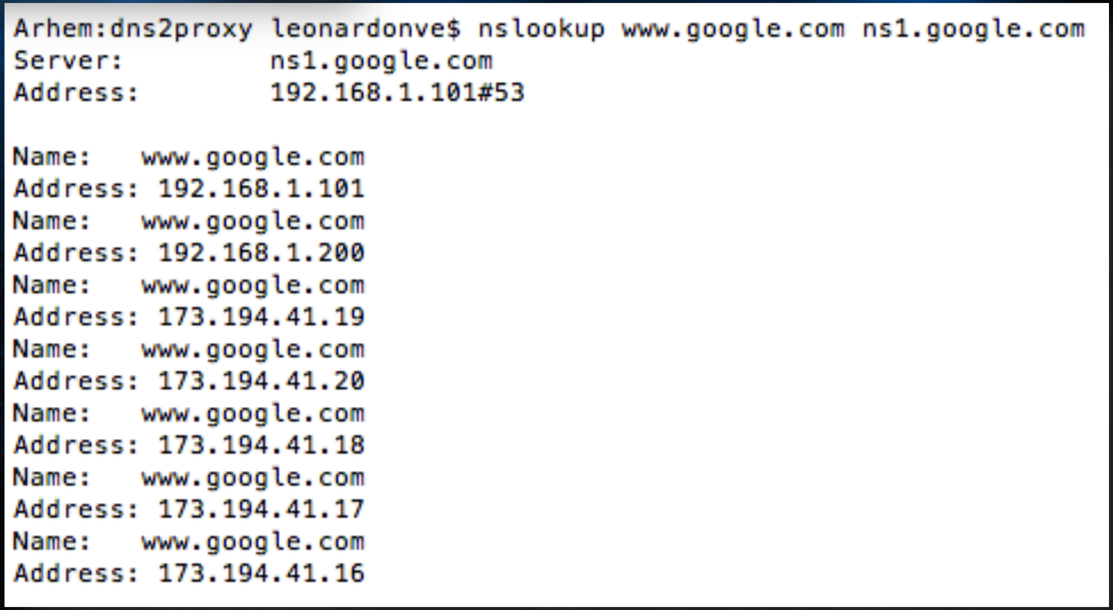
- dns2proxy (still in beta).
- Full in python (PyDNS).
- Permit spoof, direct forwarding and add IPs to the response.
- Interact directly with iptables to forward connections.

https://github.com/LeonardoNve/dns2proxy

Improve the attack.



```
root@bt:~/dns2proxy# python dns2proxy.py 192.168.1.101 192.168.1.200 eth0
Non spoofing imap.gmail.com
Non spoofing mail.s21sec.com
Non spoofing www.apple.com
Non spoofing ccgenerals.ms19.gamespy.com
Non spoofing master.gamespy.com
Non spoofing gpcm.gamespy.com
Non spoofing launch.gamespyarcade.com
Non spoofing peerchat.gamespy.com
Non spoofing gamestats.gamespy.com
binded to UDP port 53.
Starting sniffing in (eth0 = 192.168.1.101)....
```



```
Arhem:dns2proxy leonardonve$ nslookup www.google.com ns1.google.com
Server:         ns1.google.com
Address:        192.168.1.101#53

Name:    www.google.com
Address: 192.168.1.101
Name:    www.google.com
Address: 192.168.1.200
Name:    www.google.com
Address: 173.194.41.19
Name:    www.google.com
Address: 173.194.41.20
Name:    www.google.com
Address: 173.194.41.18
Name:    www.google.com
Address: 173.194.41.17
Name:    www.google.com
Address: 173.194.41.16
```

DEMO

(or video if demo effect ;)

Previous limitations.

- ~~Limited of hosts interception.~~
- ~~Time to study IP communication manners.~~
- ~~Limited cleartext protocol interception.~~
- No SSL and ciphered protocols interception.
- ~~Accept the loose of a lot information.~~

SSLStrip vs HSTS.

SSLStrip+ to defeat HSTS.

- Strict Transport Security based in domain names predefined or not.
- Change HTTPS to HTTP.
- Also change domain names to connect based on predefined rules.
- DNS Server can resolve based on these predefined rules.
- HSTS. PWNED!

https://github.com/LeonardoNve/sslstrip2.git

DEMO
(or video if demo effect…)

UDP?

- With UDP the application have the control over the communication not the OS.

- If this application resend a lost UDP packet, we have it! If not… ☹

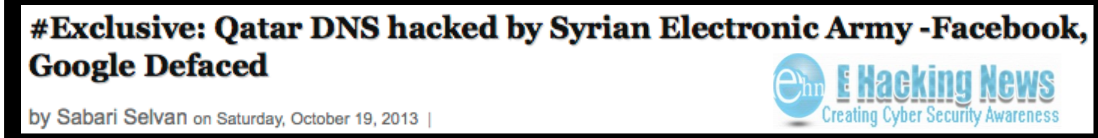
- Dns2proxy is still a beta and only control TCP but it is really easy extend it too UDP.

Other steps.

- Use other attacks against SSL (Beast, Crime,…).
- Attack SSL implementations (iPhone, Linux).
- Downgrade attacks.
- JavaScript infections.

http://media.blackhat.com/bh-us-12/Briefings/Alonso/BH_US_12_Alonso_Owning_Bad_Guys_Slides.pdf

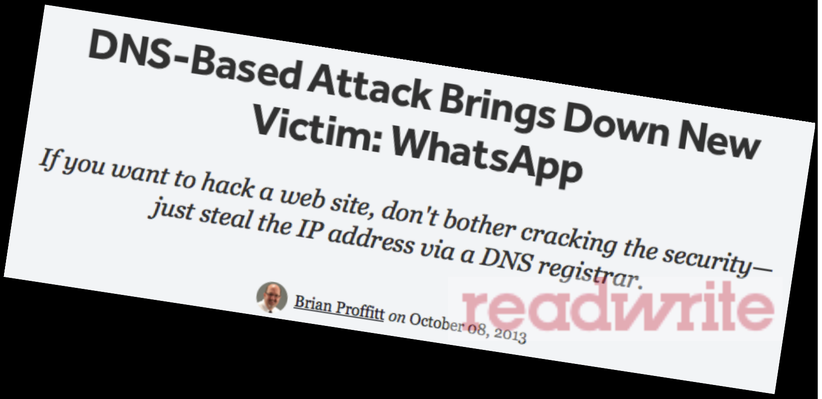
Other scenario.



#Exclusive: Qatar DNS hacked by Syrian Electronic Army -Facebook, Google Defaced

E Hacking News
Creating Cyber Security Awareness

by Sabari Selvan on Saturday, October 19, 2013 |

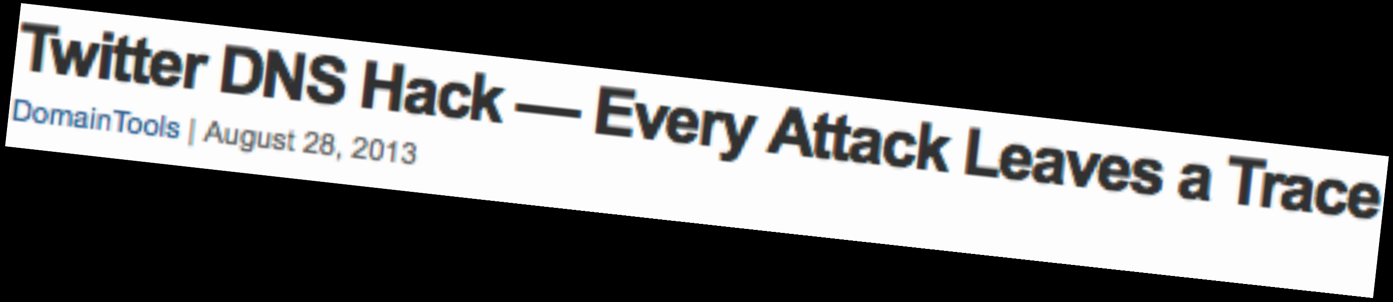


DNS-Based Attack Brings Down New Victim: WhatsApp

If you want to hack a web site, don't bother cracking the security—just steal the IP address via a DNS registrar.

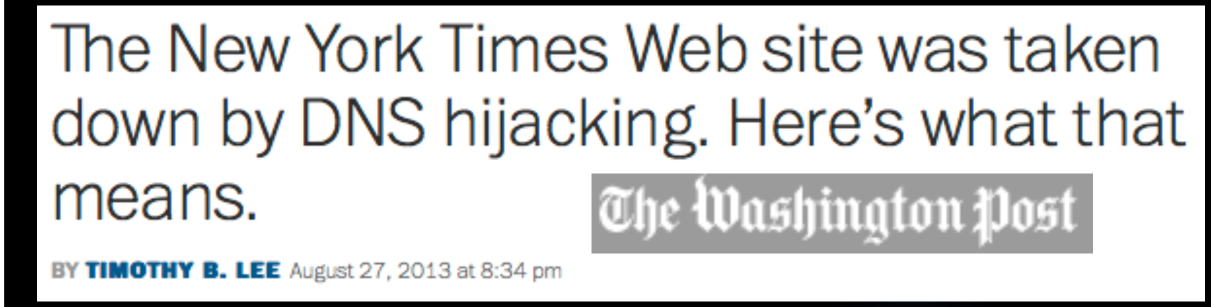
Brian Proffitt on October 08, 2013

readwrite



Twitter DNS Hack — Every Attack Leaves a Trace

DomainTools | August 28, 2013



The New York Times Web site was taken down by DNS hijacking. Here's what that means.

The Washington Post

BY TIMOTHY B. LEE August 27, 2013 at 8:34 pm

Conclusions.

- Improve DNS server configurations hijacks with two tools.
- Much information capture than typical attacks.
- Old protocols – Old security.
- New protocols + Old protocols – Old security+
- Solutions… DNSSEC.

THANKs.

Maia Nve

Ramon Pinuaga

Abel Gomez

Jose Selvi

Floren Molina

Eugeni Delfa

Olga Solera

Miguel Hernandez

Hannibal Ngu

Farid Fadaie

Moxie Marlinspike