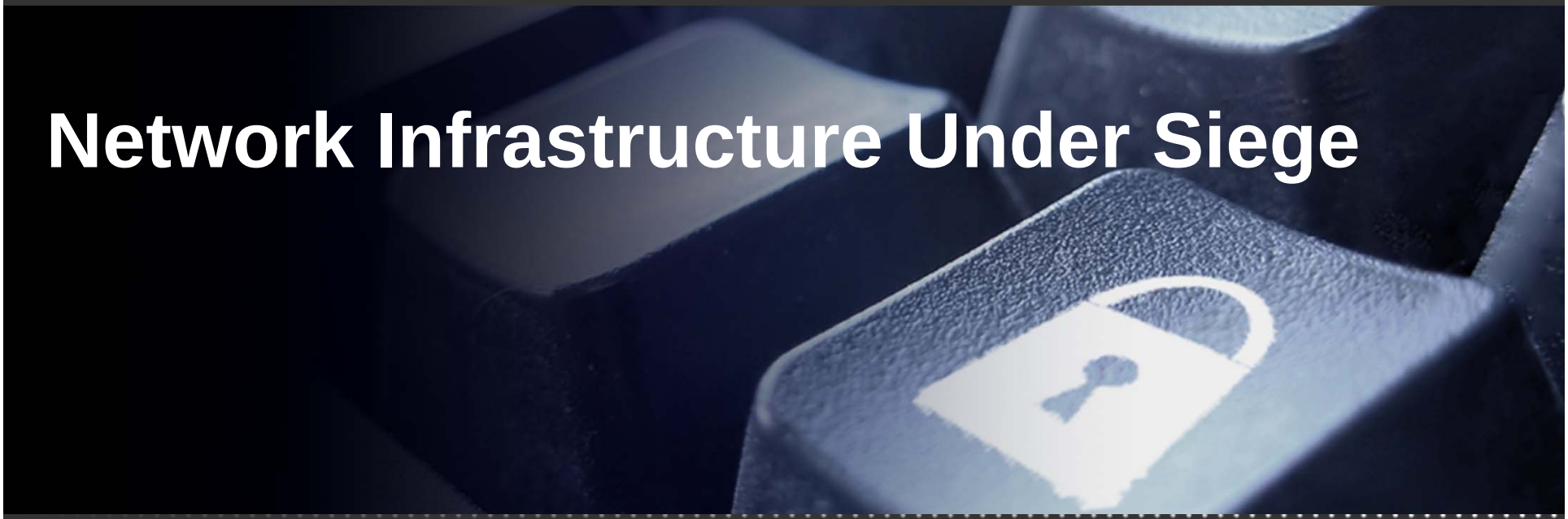
Information Security Decisions

TechTarget

Network Infrastructure Under Siege



Char Sample
Security Engineer,
CERT

Disclaimer

- Standard Disclaimer
  - This talk represents the opinions and research of the presenter only and not those of her employer. This talk is NOT a CERT sanctioned talk.

Introduction

- Who am I
  - Background
  - What is Infrastructure
  - Why do we care?

Agenda

- Network Layer: Routing
  - Global
  - Local
- Transport/Session Layer: SSL
- Application Layer: DNS

Network: Routing

- What is routing
- How does it work
  - Basic Routing Algorithm
  - Global
  - Local
- Routing Problems
  - Prefix hijacking
  - Byzantine Routing
- Routing Security

Routing

- How does it work
  - Packets are forwarded to neighbor router.
    - Router either recognizes from table or mask
    - Router forwards if it does not recognize.
  - Basic Routing Algorithm

    If packet prefix is on the network then deliver

    else if packet prefix matches static route then use it

    else if packet prefix in routing table then deliver

    else pass to default router

Routing

- Consider each step in the routing algorithm and where things can go wrong.
  - Is packet on the network? – Prefix hijacking.
  - Destination in the routing table?
    - Routing table secure?
    - Neighbors secure?

Routing

- Global: BGP
  - AS to IP mappings
  - 3 layers
    - Edge
    - Aggregation
    - Core
- Local: OSPF

Routing Example #1

Global Activity Map

Through its unparalleled, privileged relationships with the majority of worldwide service providers and global network operators, Arbor provides unequalled insight and actionable intelligence on global DDoS attack activity, Internet security and traffic trends.

Arbor's Threat Level Analysis System (ATLAS) aggregates data, which is analyzed by Arbor's world-renown security research team, and then fed back to customers via our products. Trends, commentary and insights are shared with the InfoSec community through this blog.

Tag Cloud

Olympics network malware World of Warcraft TechTarget.com IPv6 security mega Security SSH HyperGiants shut inauguration DNS cache poisoning Streaming media hijack "End of Internet" Crypto Botnet Armageddon IPv6 China Halloween down Facebook BGP

on European carriers was minimal) and Andree Toonk and his colleagues at BGPmon have a nice synopsis at the BGPMon blog.

Following shortly on the heels of the China hijack of DNS addresses in March, the April BGP incident generated a significant amount of discussion in the Internet engineering community.

TIME **NewsFeed**

TECHNOLOGY

Everybody Panic! China Hijacked 15% Of The Internet For 18 Minutes In April

Any corruption of DNS or global routing data (whatever the motive) is a cause of significant concern and reiterates the need for routing and DNS security. But in an industry crowded with security marketing and hype, it is important we limit the hyperbole and keep the discussion focused around the legitimate long-term infrastructure security threats and technical realities.

So, it was with a bit of a surprise that I watched an alarmed Wolf Blitzer report on prime time CNN about the China hijack of "15% of the Internet" last night. A bit less diplomatic, a discussion thread on the North American Network Operator Group (NANOG) mailing list called media reports an exaggeration or "complete FUD". Also on the NANOG mailing list, Bob Poortinga writes "This article … is full of false data. I assert that much less than 15%, probably on the order of 1% to 2% (much less in the US) was actually diverted."

If you read the USCESRC report, the committee only claims China hijacked "massive volumes" of Internet traffic but never get as specific as an exact percentage. The relevant excerpt from the report below:

2010

REPORT TO CONGRESS

of the

U.S.-CHINA ECONOMIC AND

Routing Example #1

- Prefix hijack BGP AS23724
- A lot of conflicting information
- 15% traffic or routes?
- Intentional or not?
- Who was affected?
  - A fair number of Chinese sites.
  - So too were US sites, .gov and .mil.
- Lessons learned and implications.

Routing Example #2

February 27th, 2012 | Filed Under: BGP instability | Tracebacks

How the Internet in Australia went down under

This Wednesday for about 30 minutes many Australians found themselves without Internet access. All these users were relying either directly of indirectly on the Telstra network, which at that point was isolated from the Internet. This story quickly hit the local headlines, in this blog we'll look at the technical details of this event and what the cause of this outage likely was.

Telstra is one of Australia's major Internet providers. It normally originates approximately 500 Ipv4 prefixes and 3 Ipv6 prefixes. Telstra also provides Transit for many ISP's and enterprises such as for example AS38285 'Dodo' an Australian ISP and AS10235 'National Australia Bank'. So how could such a large provider go down, surely it has lots of redundant hardware and multiple connections in and out of the country?

As it turns out Wednesday's outage was caused by a routing error many network engineers have first hand experience with, a simple routing leak. A routing leak can happen when small ISP X buys transit from ISP A and also from ISP B. ISP X receives a full bgp routing table from A and because of incorrect filtering relays these messages to ISP B. As a result ISP B now learns all Internet routes via ISP X to ISP B and ISP X (the customers) now became an upstream provider for ISP B.

The above is likely what happened last Wednesday between Telstra en Dodo (AS38285). Dodo a Telstra customer, re-announced all Internet routes to Telstra, which because it prefers customer routes now thinks the best way to the Internet is through Dodo. This post on the Ausnog mailings list shows how Telstra was using Dodo (a

Routing Example #2

- February 2012 Australia.
- Malice or not?
- Often the first reaction is to assume malice, while overlooking incompetence or laziness.
  - Lack of filters (max prefix limits instead)
  - Route leaks
- Lessons learned.

Routing Example #3

Routing with Byzantine Robustness

Author(s):
Radia Perlman

Report Number: TR-2005-146

Date Published: August 2005

Available Formats:
Portable Document Format (PDF)
Request Hard Copy

Abstract

This paper describes how a network can continue to function in the presence of Byzantine failures. A *Byzantine* failure is one in which a node, instead of halting (as it would in a *fail-stop* failure), continues to operate, but incorrectly. It might lie about routing information, perform the routing algorithm itself flawlessly, but then fail to forward some class of packets correctly, or flood the network with garbage traffic. Our goal is to design a network so that as long as one nonfaulty path connects nonfaulty nodes A and B, they will be able to communicate, with some fair share of bandwidth, even if all the other components in the network are maximally malicious. We review work from 1988 that presented a network design that had that property,

Securing Routing

- S-BGP
- Resource Infrastructure Public Key Infrastructure (RPKI)
- Route Origin Authentication (ROA)
- Route Origin Verification (ROVER)

Routing Security

- What can you do?
  - Find out what your provider is doing?
  - If planning a cloud migration find out what the provider is doing?
  - Consider the cloud virtual routing issues.

Transport/Session: SSL

- How SSL works
  - Browser gets a digital certificate from the site at session start.
    - That certificate has a public key to start an encrypted session, much like SSH.
    - But unlike SSH, which asks the user "should I trust the endpoint?", public key infrastructure automates the trust.
  - That certificate is signed by the CA.
    - The cert w/ associated public key) is built into the browser's certificate store.
    - Browser to verifies the signature.
- What can go wrong with SSL
  - Encryption itself is pretty good.
  - Key management issues.

SSL - Vulnerabilities

Login | Sign up

The Register®

Hardware Software Music & Media Networks **Security** Cloud Public Sector Business Jo

Crime Malware Enterprise Security Spam ID

Print Tweet Like 553 Alert

Hackers break SSL encryption used by millions of sites

Beware of BEAST decrypting secret PayPal cookies

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in ID, 19th September 2011 21:10 GMT

Researchers have discovered a serious weakness in virtually all websites protected by the secure sockets layer protocol that allows attackers to silently decrypt data that's passing between a webserver and an end-user browser.

SSL - Vulnerabilities

SSL - Security

- Client concerns
- Server concerns
- Transit concerns

SSL - Security

The EFF SSL Observatory

The EFF SSL Observatory is a project to investigate the certificates used to secure all of the sites encrypted with HTTPS on the Web. We have downloaded datasets of all of the publicly-visible

Application: DNS

- What is DNS
- How does it work
- Security Problems with DNS
- DNS Security

DNS & Why We Care

- Provides the name to IP address mappings.
- Created as scaleable method to replace original ARPANet host & address file.
- A globally distributed, loosely coherent, scalable, reliable, dynamic hierarchical database
- Originally DNS security not considered.
- DNS quickly became a critical service of the Internet infrastructure.

Why Do We Care?

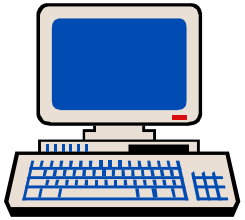
- Other applications rely on properly working DNS
- IPv6 is even more reliant on reliable DNS.
- Good attacks are invisible to the end user.

How DNSWorks

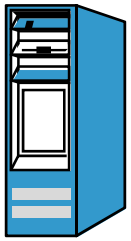
- 4 Major Components
  - Resolvers
    - Stub
    - Recursive
  - Servers
    - Caching
    - Authoritative

Split Functionality

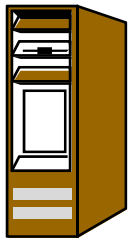
www.char.com



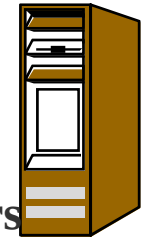
Stub resolver
End-user



Recursive
Resolver



Caching DNS Server



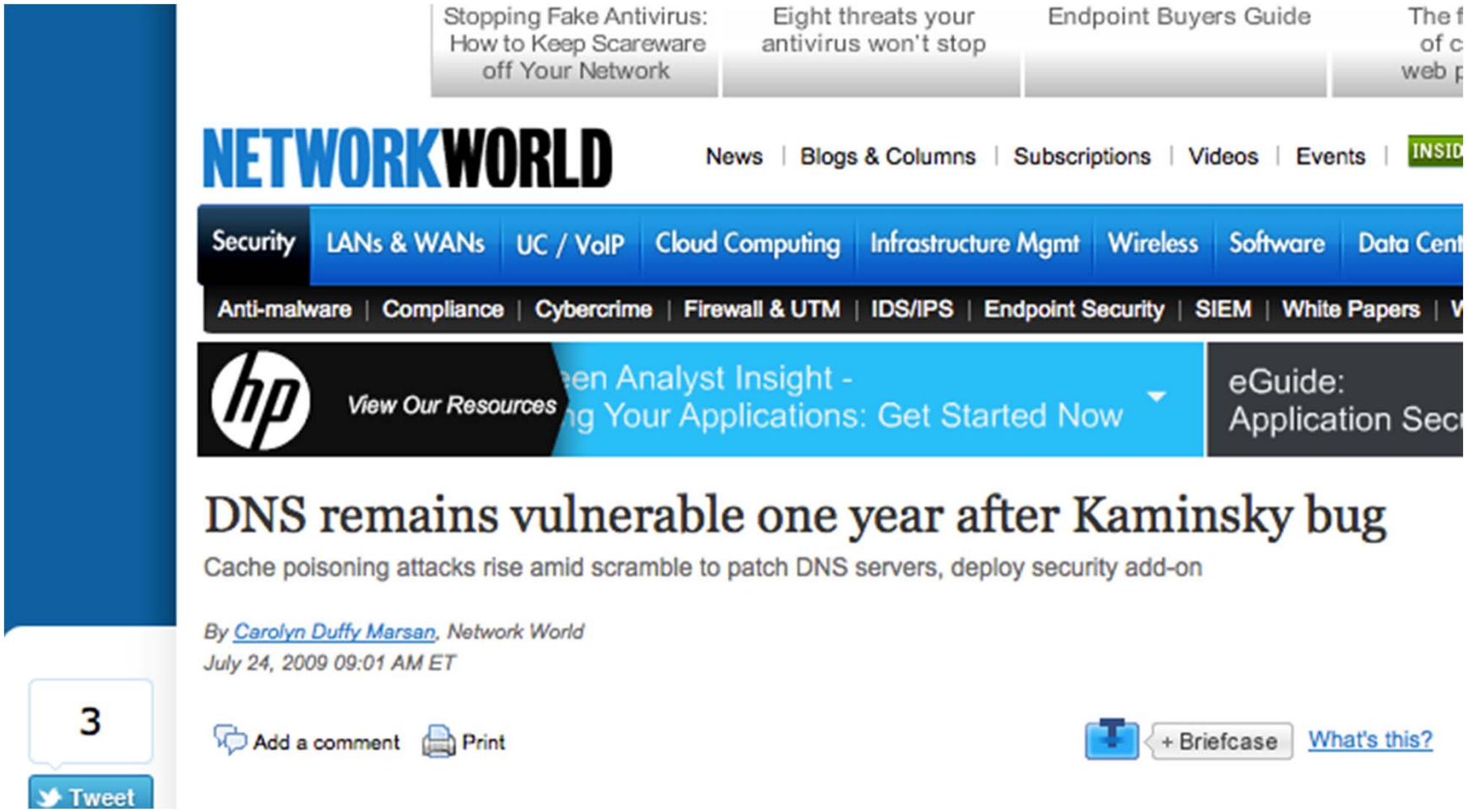
Authoritative DNS Servers

DNS Vulnerabilities

- Basic Vulnerability Types:
  - DoS
  - Data Modification
    - Cache poisoning
    - Request redirection/hijacking
  - Zone enumeration
  - Tunneling
  - Fast flux

DNS Vulnerabilities - DoS

DNS Vulnerabilities – Cache Poisoning



Stopping Fake Antivirus: How to Keep Scareware off Your Network | Eight threats your antivirus won't stop | Endpoint Buyers Guide | The f of c web p

NETWORKWORLD

News | Blogs & Columns | Subscriptions | Videos | Events | INSID

Security | LANs & WANs | UC / VoIP | Cloud Computing | Infrastructure Mgmt | Wireless | Software | Data Cent

Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SIEM | White Papers | W

hp View Our Resources

een Analyst Insight - g Your Applications: Get Started Now

eGuide: Application Sec

DNS remains vulnerable one year after Kaminsky bug

Cache poisoning attacks rise amid scramble to patch DNS servers, deploy security add-on

By Carolyn Duffy Marsan, Network World
July 24, 2009 09:01 AM ET

3

Tweet

Add a comment | Print | + Briefcase | What's this?

DNS Vulnerabilities – Request Hijacking

www.gfwvpn.com

HOME | BUY | HOW TO USE (PPTP) | L2TP/IPSEC VPN | OPENVPN | TROUBLE SHOOTING

Home » Forums » Ask and answer » DNS hijacking of Great Firewall of China

DNS hijacking of Great Firewall of China

Mon, 01/16/2012 - 17:30 — administrator

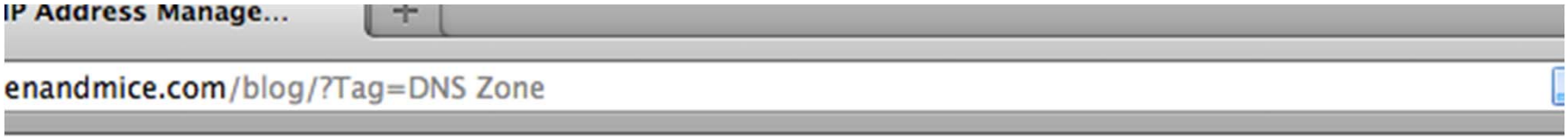
Ask and answer

Last time, we talked about DNS hijacking, and mentioned using trusted Google DNS or OpenDNS to defeat DNS hijacking.
However, your DNS will still be hijacked by Great Firewall of China if you only use Google DNS or OpenDNS.
Why does this happen?

Background knowledge:
The DNS server use UDP (User Datagram Protocol) 53 port to answer the request from user's computer.
UDP is a simpler message-based connectionless protocol which does not set up a dedicated end-to-end connection, and it's re
The client computer (your computer) will accept the first DNS reply from remote if its data format is correct and ignore other rep

Suppose you are in China and using Google DNS. You are going to open http://releases.mozilla.org
Your computer tries to get IP address of releases.mozilla.org from 8.8.8.8. This request is detected by IDS (Intrusion Detect Sys
your computer immediately. As we say above, your computer will accept this reply and ignore other replies (the real reply). In th
is hijacked.
Conclusion: Your DNS is still hijacked simply because **GFW is in the middle of your computer and the destination DNS ser**

DNS Vulnerabilities – Zone Enmumeration



Walking a DNS zone

Using NSEC is relatively simple, but it has a nasty side-effect: it allows anyone to list the zone content by follow linked list of NSEC records. This is called 'zone walking'. The 'ldns' library contains an tool called 'ldns-walk' tha be used to list all records inside a DNSSEC signed zone that uses NSEC:

```
$ ldns-walk paypal.com
paypal.com.      paypal.com. A NS SOA MX TXT RRSIG NSEC DNSKEY TYPE65534
3pimages.paypal.com. A RRSIG NSEC
_dmarc.paypal.com. TXT RRSIG NSEC
ym2._domainkey.paypal.com. TXT RRSIG NSEC
```

DNS Vulnerabilities - Tunneling

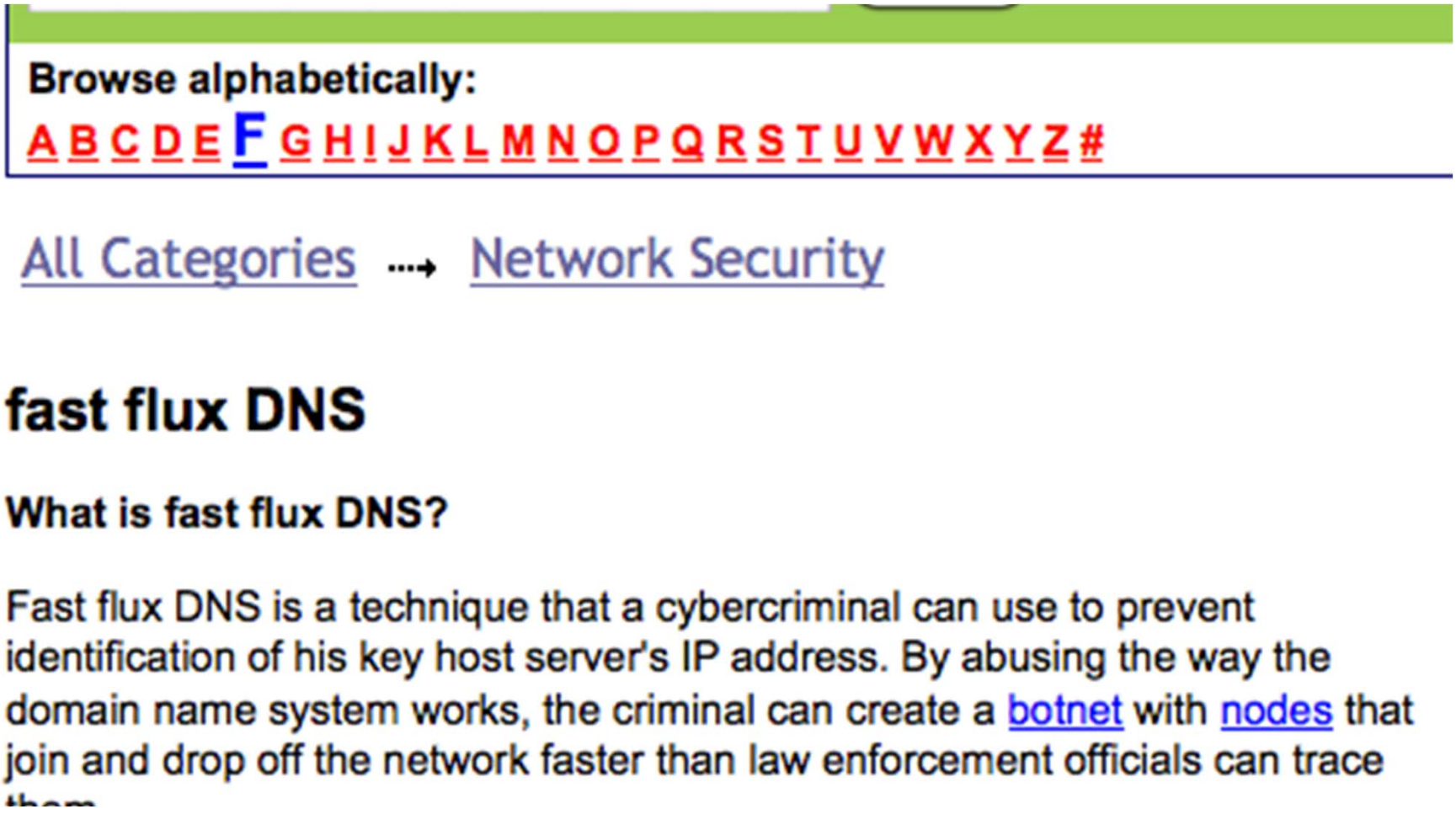
Weblog Linkblog

DNS Tunneling made easy

Yesterday I came across a technique to tunnel any traffic through the W DNS protocol: All the packages you send are base32 encoded and prepended as the hostname of a DNS lookup request. A specially prepared DNS server will then forward your packages and reply with TXT answers.

What is it good for? It's an interesting way to hide your traffic. Cory Doctorow wrote about it in Little Brother for example. But it can also be used to sneak into certain public hotspots which are protected by HTTP

DNS Vulnerabilities – Fast Flux



Browse alphabetically:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z #

All Categories ⇢ Network Security

fast flux DNS

What is fast flux DNS?

Fast flux DNS is a technique that a cybercriminal can use to prevent identification of his key host server's IP address. By abusing the way the domain name system works, the criminal can create a botnet with nodes that join and drop off the network faster than law enforcement officials can trace

Securing DNS

- Done through a combination of the following:
  - Configurations
  - Software
  - Monitoring

Configurations

- Separate out functionality
  - Authoritative nameserver (ANS) by itself, public.
  - Caching nameserver (CNS) ideally separated from recursive resolver.
    - CNS tightly secured and isolated.

Securing DNS - DNSSEC

- What is DNSSEC?
  - DNS Security Extensions
  - Digital signatures
- How does it work?
  - Signed Resource Record.
  - Zone signing key (ZSK) & (KSK).
- What do I need to know?
  - Read up.
  - Get training.
  - Determine provider’s knowledge.
  - Cloud implications.

DNSSEC – NASA example

Securing DNS - Monitoring

- DNS monitoring
  - As a part of IDS
  - As a form of IDS
- DNS in the cloud
  - 2009 Majority of operators did not know how to implement DNSSEC.
  - Tunneling problem.
  - DNSSEC configuration problem.

Conclusion

- There are lots of areas of concern within the infrastructure.
- The infrastructure offers an excellent target for cyber attacks and cyber crime.
- There are many efforts to improve security.
- Get involved, even if it’s just making your views known to your provider.

Sources of Information

- IETF: www.ietf.org
  - Routing
    - www.bgpmon.net
    - www.arbornetworks.com
    - www.teamcrymu.org
  - SSL
    - www.eff.org
    - www.sans.edu
  - DNS
    - www.isc.org
    - www.dnssec.net
    - tools.netsa.cert.org

Q&A

Questions

- …and Answers…

Contact

Char Sample
Security Engineer,
Carnegie Mellon University CERT
char_sample@yahoo.com

Featured Member of the TechTarget Editorial Speaker Bureau