Domain Names

How do they work?

How do they affect spoofing?

PRESENTED BY AUGUST ETECH
• What is the domain name?
• How do I get a domain name?
• Where is it hosted?
• What does it do?
• SPOOFING!
What is a domain name and who hosts it?

- **Domain Name System**, or DNS, is the friendly naming system for giving addresses to web servers and web pages. Somewhat like international phone numbers, the domain name system gives every server a memorable and easy-to-spell address. Simultaneously, the domain names hide the really technical **IP address** which most viewers aren’t interested in.

Examples of Internet Domain Names
- google.com
- nytimes.com
- navy.mil
- harvard.edu
- monster.ca
- wikipedia.org
- japantimes.co.jp
- dublin.ie
- gamesindustry.biz
- spain.info
- sourceforge.net
- wikipedia.org
How do I get a domain name?

The registration of domain names is usually administered by domain name registrars who sell their services to the public.

A domain name registrar is an organization or commercial entity that manages the reservation of internet domain names. A domain name registrar must be accredited by a generic top-level domain (gTLD) registry and/or a country code top-level domain (ccTLD) registry. The management is done in accordance with the guidelines of the designated domain name registries.

- Network Solutions
- Go Daddy
- Register.com
What does a domain do?

• Domain names were created to make IP, or Internet Protocol, addresses more end user-friendly.

• Domain names tell computers where to go for web addresses, email and much more.
  • A Records
  • MX Records
  • CNAME
  • Etc....
Domain and IP’s

- 17.142.160.59
- Cheddercheese.com
- Would you rather type in the name or the numbers?
- Which one would you remember better?
Domain and IP’s

What does your domain do?

www.whatsmydns.net
Types of Spoofing

Email Spoofing:

• Mimicking a trusted email address or domain by using alternate letters or numbers to appear only slightly different than the original

• Disguising the ‘From’ field to be the exact email address of a known and/or trusted source

IP Address Spoofing:

• Attackers may use IP (Internet Protocol) spoofing to disguise a computer IP address, thereby hiding the identity of the sender or impersonating another computer system. One purpose of IP address spoofing is to gain access to a networks that authenticate users based on IP addresses.
Types of Spoofing

Website Spoofing:

• Website spoofing refers to when a website is designed to mimic an existing site known and/or trusted by the user. Attackers use these sites to gain login and other personal information from users.

IP Address Spoofing:

ARP Spoofing:

• Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to Media Access Control (MAC) addresses for transmitting data. ARP spoofing is used to link an attacker’s MAC to a legitimate network IP address so the attacker can receive data meant for the owner associated with that IP address. ARP spoofing is commonly used to steal or modify data but can also be used in denial-of-service and man-in-the-middle attacks or in session hijacking.
Spoofing

Yes. Send me the confirmation once complete.

on Feb 12, 2014 wrote:

Can I send this to you? I normally approve the wires, not initiate.

From: Steinkopf, Timothy
Sent: Wednesday, February 12, 2014 9:58 AM
To:

Subject: Re: Wiring Instruction

Process a wire of $357,493.41 to the attached account information. Let it be coded admin expense. Send me the confirmation when completed.

Thanks

Tim
Spoofing

From: Tom Kemp [mailto:tom.kemp@centrify.com]
Sent: Friday, September 11, 2015 9:55 AM
To: Tim Steinkopf
Subject: Wire Payment

Tim

Are you at your desk? I need you to process a wire transfer

Tom

Sent from my iPhone
Dear User,

Your Mail version is outdated, Failure to Upgrade to the newest my McGill University Mail 7.1 now will result to a permanent account closure.

To upgrade click the link below and accept our new terms and conditions.

[Update Server]

Thanks,
McGill University Team

Privacy Policy | Customer Support
©2017 Office365 McGill University Support Team. All Rights Reserved.
Spoofing
Spoofing

Bad guys often troll companies for months to gather the data necessary in pulling off a successful attack.

THE START
Attackers see if they can spoof your domain and impersonate the CEO (or other important people)

THE PHISH
Spoofed emails are sent to high-risk employees in the organization

To: Finance Department
Urgent wire transfer request! Please send $100,000 to new acct #987654-3210

To: CFO
Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

To: Human Resources
I need a PDF copy of ALL employee W-2s for the IRS ASAP!

THE RESPONSE
Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

It's from the CEO, I'll take care of this for him!

Sounds important, I'll send these right away!

THE DAMAGE
Social engineering was successful, giving hackers access to what they were after

Causing fraudulent wire transfers and massive data breaches

THE RESULT
The fallout after a successful attack can be highly damaging for both the company and its employees

Resulting damage:

- Money is gone forever in most cases and only recovered 4% of the time
- CEO is fired
- CFO is fired
- Lawsuits are filed
- Intangibles - tarnished reputation, loss of trust, etc.

So... Think Before You Click!
Spoofing

It’s not just about wire transfers. It’s about reputation.
Spoofing

How to stop it!
Secure your domain and monitor activity to keep secure.
Spoofing

Record checks:

**SPF** (sender policy framework)
Spoofing

Record checks:

**DKIM** (domain keys identified mail)
Spoofing

Monitoring!

And blocking!
Spoofing

Test your domain.
https://www.dmarcanalyzer.com/
Spoofing

• Use an anti-spam software like Barracuda

• Setup DKIM, SPF an PTR record for your domain names

• Make sure your website has firewall protection

• Train your employees to spot spoofing emails and not click on fake links
Now you know how a domain works!

www.augustetech.com
1.877.317.1077