ISPs, Backbone Providers, and Hacking

Alex Horejsi
Bowen Waugh
Kit Ha
Richard Balbuena

What is an ISP?

Internet Service Provider

“Cable Company”

Connection to servers, companies, friends, family, etc.

Google vs Verizon

What is a Backbone Provider?

Different from ISPs

- Supplies access to other ISPs

T1 and T3 Lines

- 1.544 Mbps and 43 Mbps

Sprint, MCI, Level 3, etc.

Bowen

What is a Hacker?

Typical “Users”

Company relations

Professional Hackers

Black Hats

Bowen

Common types of malicious activity on the web

- Malicious internet robots (bots) infect a host to connect to a remote server owned by the hacker to steal sensitive information such as passwords, financial information, launch DDOS attacks and capture and analyze data packets.
- Email spam- Emails that may contain viruses and also log email replies to see if you are active as to send more spam/ Phishing to take you to fake site pretending to be something else to steal credentials.
- Distributed denial of service (DDOS)-Shutting down major sites with high amounts of requests to prevent users from accessing it
- Viruses and spyware distributed through download links (scare/download tactics----> “your pc has a virus” , multiple download buttons), torrented files, trojan horses

Richard Balbuena

Bots and their prominence

- Malicious bots can be placed on your computer through downloads. Can instruct an infected computer to connect to a hackers server. Most people do not realize that their computer is being used this way.
- Multiple bots connected to the same server form a “botnet” (robot network) which can be sold or rented for use of malicious intent (DDOS, information stealing, fake traffic for revenue)
- Bots can overload servers with multiple requests in a small amount of time to crash the site
- Bots send spam on emails, are present in video games, social media (twitter, tinder)

Richard Balbuena

Notable attacks on the internet

- 2017 Equifax data breach that affected 150+ millions of users. Hackers stole social security numbers, bank information, and personal information over 76 days, slowly retrieving information from their databases.
- 2015 Ashley Madison dating site hack by “The Impact Team” exposed emails, names, addresses leaked , exposing people having extramarital affairs. Hackers claim to have attacked the AM website to expose that AM didnt really delete user data after charging 19$ to delete it.
- 2011 Playstation Network DDOS attack that lasted over a month, making players unable to play online and have personal and credit card information exposed

Richard Balbuena

How ISPs and backbone providers prevent hacking

- Users are both victims and perpetrators of hacking. Internet companies need to both protect their customers from hacking and prevent them from hacking
- What these companies do to prevent hacking
  - Protecting customers from malware and attacks,
    - Example: Blocking means of attacks from hackers, viruses and worms
  - Preventing outgoing attacks from users who are hacking,
    - Example: Scanning for and blocking compromised hosts
  - Making the use of networks more transparent so that internet companies can monitor traffic more effectively and therefore identify attacks more easily
    - Example: “Calling records” from IPs to see the kind and amount of traffic travelling to and from a host

Alex Horejsi

What more could be done?

- Unfortunately, it does not seem like most ISPs are doing much in the way of security because there are few incentives for these companies to pursue greater security
- Many have focused on implementing security to protect users from being hacked, but very little to protect against outgoing attacks or to make network use more transparent

Alex Horejsi

Ethical Issues of doing more (Post Office Example)

- Dale Drew (Chief Security Officer of Level 3* communications) compares the process of stopping malicious activity on the Internet to running a post office.
  - “While they can’t look at the contents of an envelope, they do know who is sending what and to whom.” - csonline.com
- Being able to stop malicious activity in real time would mean being able to open these “envelopes” to determine if it’s bad or not. This would be a HUGE invasion of privacy.
- Preventative measures are done instead that rely on heuristics to determine if an envelope could “potentially” contain malicious activity.
  - This is not 100% accurate

*Level 3 is one of the major backbone providers for the Internet

Kit Ha

Ethical Issues of Preventative Measures

- **Even if** ISPs and backbone providers had a 99% success rate of predicting malicious activity, it would mean 1 in every 100 users would be flagged falsely.
  - In order to be absolutely correct, backbone providers have to work with
    - ISPs to connect IP addresses to actual customers and
    - law enforcement to ensure that it is actual malicious activity that is in progress
- The potential for false negatives.
  - Of the millions of IP addresses that Level 3 predicts to be a part of malicious activity
    - - 60% are estimated to be part of a botnet
    - - 22% are estimated to be victims of phishing
  - Level 3 can't block these IP addresses because most of these users don't even know their machines are doing something illegal.
  - Potential customers and transactions could be lost, if IP addresses were blocked.

Kit Ha

References

https://help.campaignmonitor.com/how-why-isps-block-emails

https://privacy.google.com/businesses/security/#!?modal_active=none

https://whatismyipaddress.com/isp

https://the-parallax.com/2017/08/31/hackers-love-wi-fi-protect/

https://www.nanog.org/meetings/nanog26/presentations/ispsecure.pdf

www.cs.cmu.edu/~dwendlan/personal/docs/isp_security_incentives.ppt

https://www.ncta.com/positions/protecting-consumer-privacy

References (Continued)

https://us.norton.com/internetsecurity-malware-what-are-bots.html

http://www.phishing.org/what-is-phishing

https://www.cybrary.it/0p3n/types-of-hackers/

https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

https://www.csoonline.com/article/3173274/amid-cyberattacks-isps-try-to-clean-up-the-internet.html

https://www.sciencenewsforstudents.org/article/botnets-malware-cyberattack-increase