CE0973a - Issues in Network Security
10: ISP Infrastructure

James A Sutherland

Abertay University

Monday, 14th March 2016

Threat Models 1

Think about who is out to get you, and why – back to CIA

BNP	Knock them offline (A), dox them (C)
Bank	Conduct unauthorised transactions (I)
Business	Blackmail, ID/CC theft, graffiti (A,C,I)
Government	Sabotage, espionage, infiltration (A,C,I)

Threat Models 2

Then think about *how* an attack might take place.

- DoS
- Infiltration
- Human factors: kidnap, torture, bribery/blackmail

Terminology

Phishing is surprisingly effective, usually as a variant of **Social Engineering** attack.

Phishing Email tricking recipient into disclosing credentials

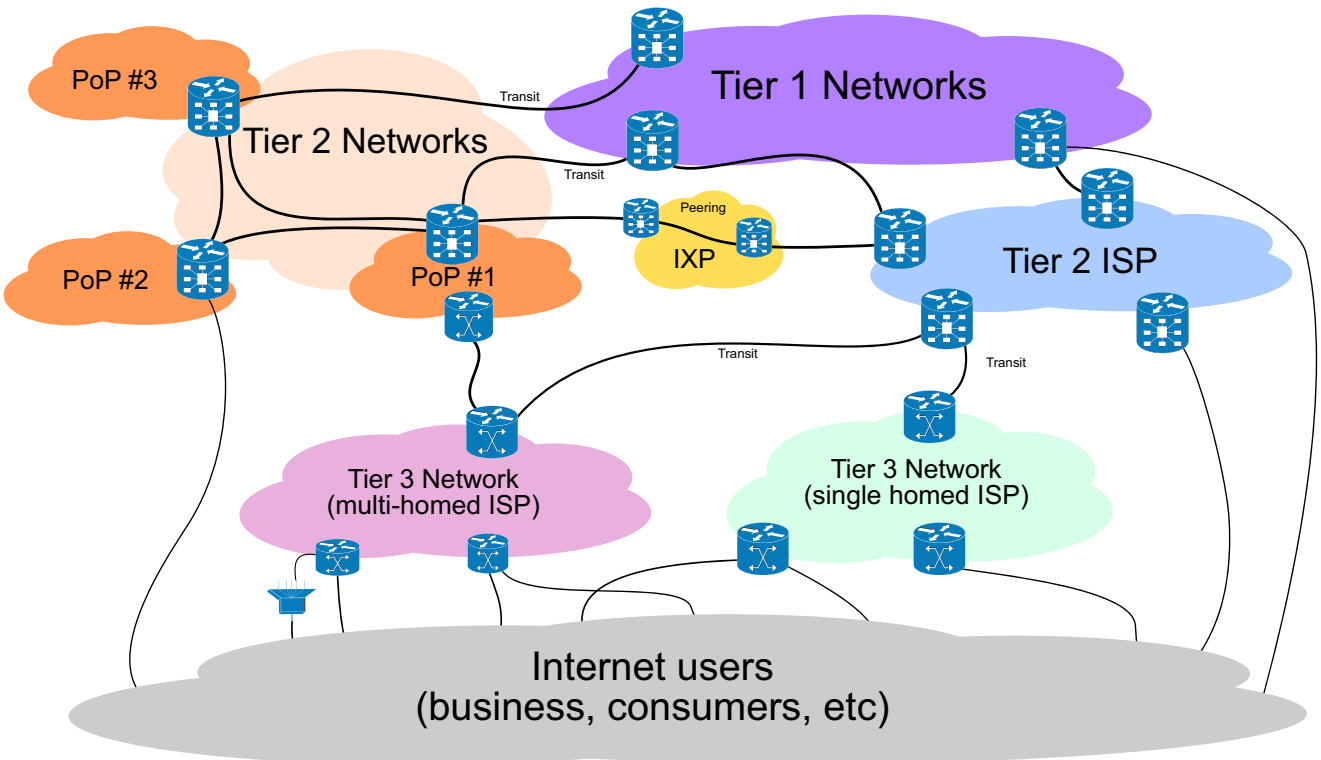
Spear Phishing Targeted phishing, usually specific individuals

Whaling Spear phishing when targeted against senior staff such as the CEO

Public information such as LinkedIn and Facebook profiles or interviews with senior figures can be very valuable in whaling attacks in particular.

Internet Routing Basics

Each network has an Autonomous System Number, ASN. For example, Janet (the UK university network) is AS 786.



From https://commons.wikimedia.org/wiki/File:Internet_Connectivity_Distribution_%26_Core.svg

Peering Versus Transit

Peering When two networks connect to each other.

- BT and Sky both generate lots of traffic (various video on demand services) and consume it too (millions of broadband customers each).
- Peering points such as LINX and LoNAP exist to support this: basically some Ethernet switch ports for ISPs to rent and exchange traffic through.

Transit When one network provides the other with a route to other networks

- Janet pays TeliaSonera

Peering Disputes

Peering isn't always free (when it is, that's called **Settlement Free Peering**). The volume, direction and value of traffic exchanged affect the pricing and politics.

- Cogent – controversial for cheap, disruptive pricing
- Netflix – large volume of outbound traffic, Comcast etc demanded payment

De-peering can be disruptive: without a route between client and server, the site appears offline!

Network Types

Single homed You! Just pay for "an Internet connection"

Dual homed Big enough to have two different connections at once

BGP connected Probably an ISP, or larger business: fancy dynamic routing

ISP Sizes

Tier 1 An ISP so big that it doesn't pay *anybody* for transit, just peering

- Level3, Cogent, TeliaSonera

Default Free Have an explicit route to every IP address

- Currently, that's about half a million routes

BGP: Border Gateway Protocol

Connects ISP networks (more specifically, routers) together, exchanging routing information.
"Hi, I'm AS786, I host 193.60.0.0/16 and 194.80.0.0/16"
Receiving router can pass this on to others, and/or use it[1]:
"That's a good route to 786, I'll use that and offer it to my friends/clients too.".

[1] This can be restricted by the sender using no-advertise and no-export codes. Of course, Janet actually use rather more networks than that!

BGP for defence

Under a DoS attack, it's possible to use BGP to block traffic: "discard all traffic from 6.6.6.0/24 to my network" — or if under a spoofed attack from a wide variety of sources all aimed at your DNS server 8.8.8.8: "discard all traffic for 8.8.8.8"[2]. Hopefully you can be quite specific there, identifying the origin network and target: for example, someone on BT's broadband network flooding your primary DNS server, so only block that particular combination.

[2] That's Google's primary public DNS server. If they ever have to block all its traffic, the Internet is having a bad day!

BGP for offence

DoS: no routing $\rightarrow$ no Internet access

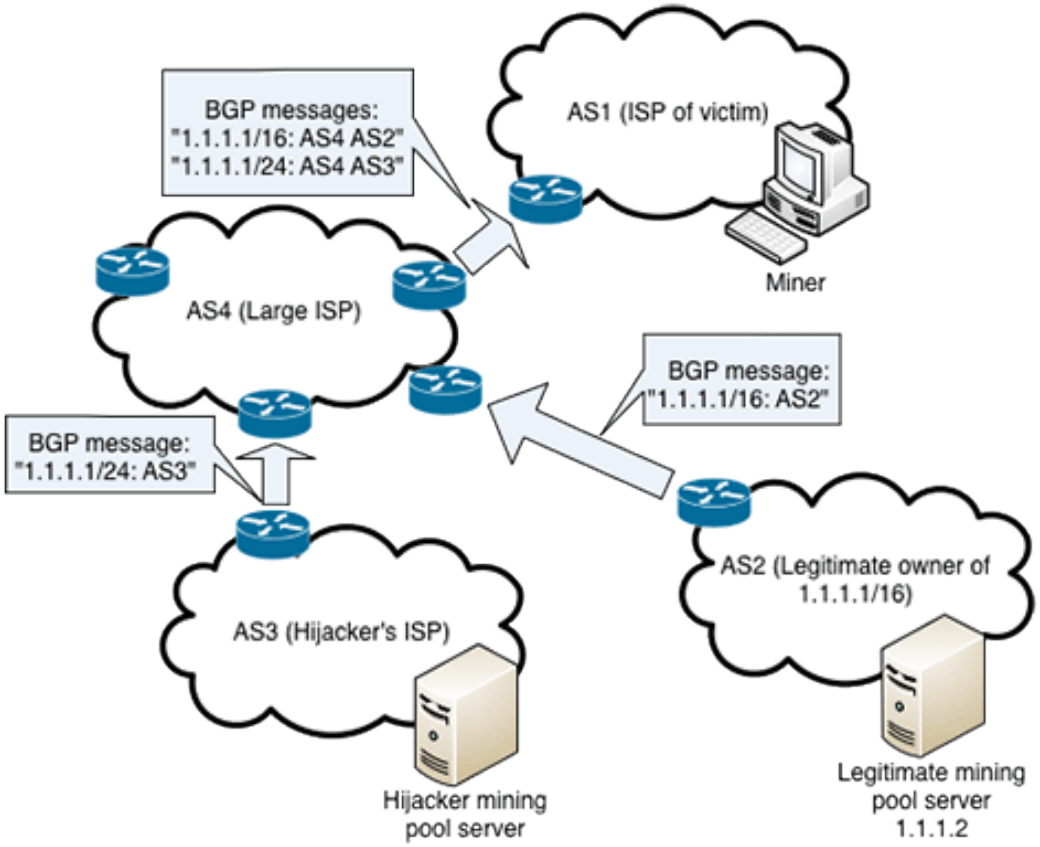
`https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit`

August 2014:

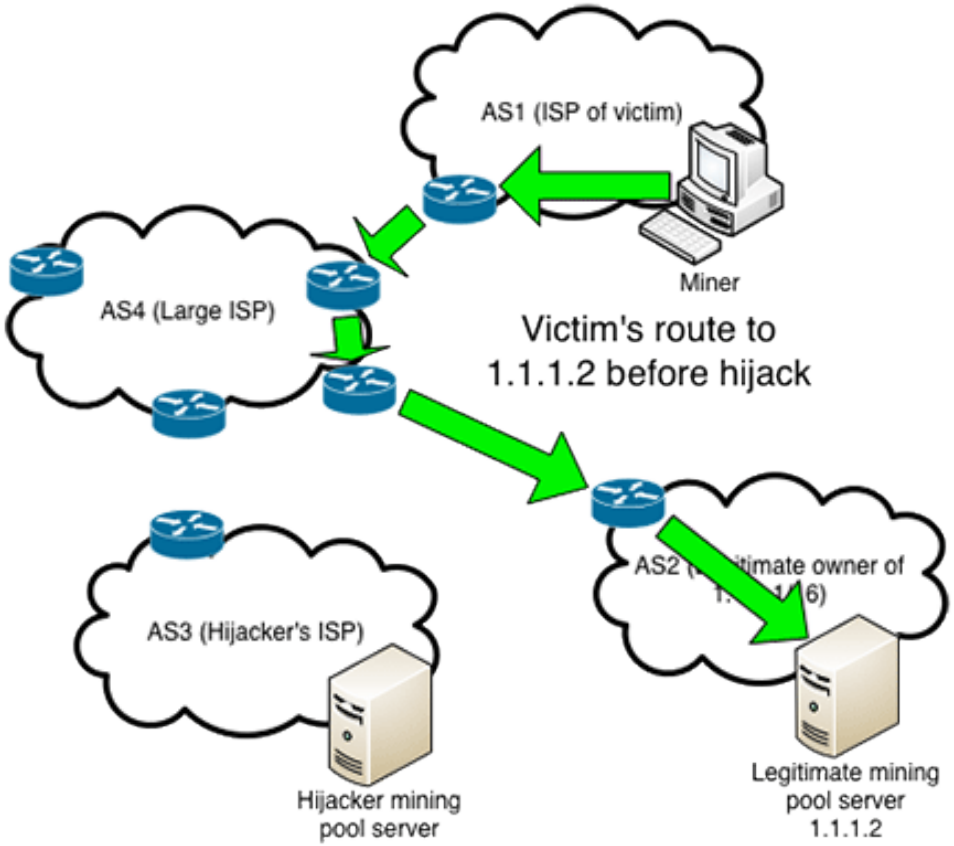
- Verizon add 15,000 new routes ...
- Pushing the default-free routing table over 512k prefixes ...
- Networks including both Ebay and Microsoft go offline

BGP can also be used to hijack traffic: just announce that the best way to reach the target address is through you!

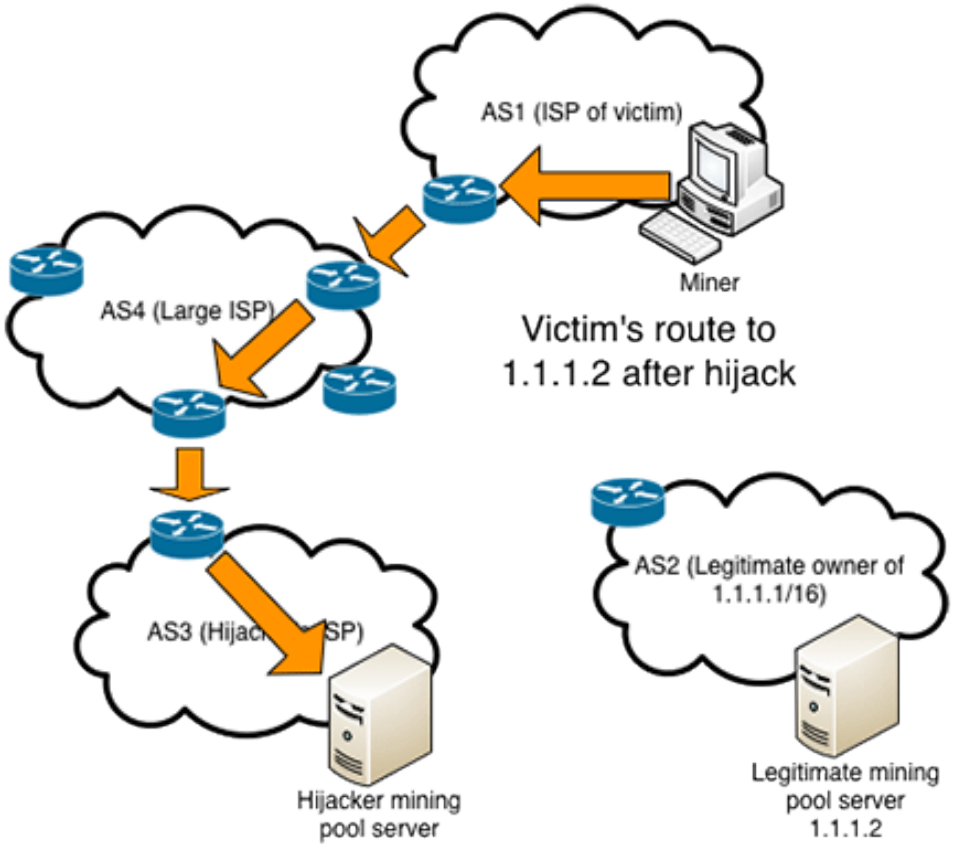
BGP Hijacking 1



BGP Hijacking 2



BGP Hijacking 3



BGP Defences

Status quo:

- Hijacking still happens, by accident and design
- Pakistan blocked YouTube . . . globally!

Countermeasures:

- TTL Security: `http://packetlife.net/blog/2009/nov/23/understanding-bgp-ttl-security/`
- Some crypto ideas: RPSL, SIDR
- Route analytics: identify 'bad' routes
- Manually!
- But SSL makes it all OK, because just seizing an IP doesn't give you an SSL certificate – right?

BGP Defences

Deadline Weeks 5,6,8,9 lab work portfolios to be in Blackboard by Friday night

BGP hijacking Look at your earlier network diagrams and think about the impact

Detect How would you know if it happened to you?

Resolve How would you fix it?

Prevent How would you stop it happening in the first place?

Mitigate What measures could you take to reduce the impact if it did?