SPAMTRACER
TRACKING FLY-BY SPAMMERS
NANOG60

PIERRE-ANTOINE VERVIER
SYMANTEC RESEARCH LABS

Pierre-Antoine_Vervier@symantec.com
BGP hijacking

• CAUSES
  – The injection of erroneous routing information into BGP
  – No widely deployed security mechanism yet
    • E.g., ROA, BGPsec

• EFFECTS
  – Blackhole or MITM [Pilosof:Defcon’08] of the victim network

• EXPLANATIONS
  – Router misconfiguration, operational fault
    • E.g., Hijack of part of Youtube network by Pakistan Telecom
  – Malicious intent?
Where it all begins

• CONJECTURE
  – Spammers would use BGP hijacking to send spam from the stolen IP space and remain stealthy
  – Short-lived (< 1 day) routes to unannounced IP space + spam [Ramachandran:SIGCOMM’06] but...
  – …this does not necessarily imply hijacks [Vervier:ICC’14]
  – Anecdotal reports on mailing lists

• POTENTIAL EFFECTS
  – Misattribute attacks launched from hijacked networks due to hijackers stealing IP identity
  – Spam filters heavily rely on IP reputation as a first layer of defense
Fly-by spammers :: Myth or reality?
Your mission, should you accept it

• Validate or invalidate on a large scale the conjecture about fly-by spammers
• Assess the prevalence of this phenomenon

• SPAMTRACER [Vervier:TMA’13]
  – collect routing information about spam networks
  – extract abnormal routing behaviors to detect possible BGP hijacks
SpamTracer :: Presentation

• ASSUMPTION
  – When an IP address block is hijacked for stealthy spamming, a routing change will be observed when the block is released by the spammer to remain stealthy

• METHOD
  – Collect BGP routes and IP/AS traceroutes to spamming networks just after spam is received and during several days
  – Look for a routing change from the hijacked state to the normal state of the network
SPAMTRACER :: System architecture

Data collection
- Spams IP
- Monitored IP's
- IP i
- IP/AS traceroute
- BGP routes
- IP/AS & BGP routes to IP i

Data analysis
- BGP & Traceroute Anomaly Detection
- Identification of Hijackings
- Possible Hijack/Suspicious
- Benign

Live spam feed
- Symantec.cloud
- Team Cymru
- Bogon IP prefixes
29 hijacked IP prefixes from Jan. to Jul. 2013
Fly-by spammers :: Hijack signature

• Hijacked networks
  – were **dormant** IP address blocks, i.e., by the time the networks were hijacked they had been left **unadvertised** by their owner
  – advertised for a rather **short** period of time
  – advertised from an apparently **legitimate origin** AS but via a presumably **illegitimate upstream** AS
  – see [Huston:RIPE50]

• In practice, we observed
  – hijack **durations** between 30 minutes and 20 days
  – **unadvertised** periods between 1 month and 9 years
  – **illegitimate upstream** ASes were hijacked too
**Hijack duration**

Most hijacks were rather short-lived!

- **9/29 IP prefixes**
  - Hijack duration: $6 \text{ days} \leq \text{hijack duration} \leq 20 \text{ days}$

- **20/29 IP prefixes**
  - Hijack duration: $\leq 4 \text{ days}$

MIN = 30 minutes
Durations of unadvertised period of IP prefixes

Most hijacked IP prefixes were left unadvertised for a very long time!
Case studies ::
IP prefix routing history & Spam & DNSBLs

- IP prefixes have only been announced when spam was received!
- Few IP prefixes have spam sources blacklisted in Spamhaus SBL and DROP, Uceprotect or Manitu at the time of the BGP announcements!
Case studies ::
IP prefix routing history & Spam & DNSBLs

• Strong temporal correlation between
  – BGP announcements of IP prefixes and
  – spam
• BGP announcements are quite short-lived!
• No identified spam bot!
• Scam web sites advertised in spam mails hosted in the hijacked networks
How effective is this spamming technique?

• Out of 29 hijacked IP address blocks
  – 6 (21%) were listed in Uceprotect or Manitu
  – 13 (45%) were listed in Spamhaus SBL and DROP (Don’t Route Or Peer)
    • DROP is supposed to list hijacked IP address blocks
    • but little is known about their listing policy
  – 29 (100%) were observed only once during the time period of the experiment

• Fly-by spammers seem to manage to remain under the radar!
Which networks were targeted?

• All hijacked IP address blocks were assigned to a different organization (i.e., a different owner)

• Out of 29 organizations
  – 12 (41%) were found to be dissolved or very likely out of business
  – 17 (59%) were found to be still in business or no conclusive evidence of them being out of business could be found

• Fly-by spammers seem to simply target dormant IP address blocks regardless of their owner still being in business or not!
One timeline to bind them

• Several hijacks were performed in **groups of 2 to 4**, all hijacks in a group starting and ending at the **same time**

• During several days there were always **at least two** IP prefixes hijacked

• This **temporal pattern** suggests a common root cause to those hijacks!
One timeline to bind them
What about long-lived hijacks?

• We looked specifically for short-lived hijacks
  – each spam network was monitored for 1 week after spam was received
• But what about long-lived ones
  – it happens also, e.g., LinkTelecom hijack lasted 5 months [NanogML’11, Symantec:ISTR’12, Schlamp:CCR’13]
  – but they are less straightforward to detect
  – and it seems to defeat the assumed purpose of evading blacklisting
• We are working on updating our framework to better detect these cases
How to prevent fly-by spammers?

• In the observed hijack cases, spammers
  – did not tamper with the origin of the IP address blocks
  – but advertised the IP address blocks via illegitimate upstream ASes

• The RPKI is currently the most promising architecture for securing BGP
  – both Route Origination and Route Propagation must be secured to prevent fly-by spammers
  – secured Route Origination via ROAs is being more and more deployed
  – but secured Route Propagation with BGPsec is still at a too early stage

• The solution for now is thus to
  – return and help RIRs reclaim dormant IP space, and
  – use detection systems to mitigate the effects of these attacks, e.g., by feeding IP-based reputation systems with hijacked IP address blocks
Conclusion

• The observed fly-by spammer cases show that this phenomenon is happening though it does not currently seem to be a very prevalent technique to send spam, e.g., compared to botnets.

• However, it is important to detect those attacks because hijacking IP address blocks hinder traceability of attackers and can lead to misattributing attacks when responding with possibly legal actions!
Perspectives

• Provide an interface for network operators to query identified hijacks

• Collaborate with RIRs and ISPs to help mitigate hijacks

• Ongoing collaboration with Institut Eurécom (FRA) and TU München (GER) to build a comprehensive system for the detection and investigation of malicious BGP hijacks
Thank you!

Time for Q&A!
Some references


Spamhaus DNSBLs, http://www.spamhaus.org/
Uceprotect DNSBL, http://www.uceprotect.net/
Manitu DNSBL, http://www.dnsbl.manitu.net/