SPAMTRACER

TRACKING FLY-BY SPAMMERS

RIPE 67

PIERRE-Antoine VERVIER

SYMANTEC RESEARCH LABS

Pierre-Antoine_Vervier@symantec.com
Where It All Begins

• CONJECTURE
  – Spammers would use BGP hijacking to send spam from the stolen IP space and remain untraceable
  – Short-lived (< 1 day) routes to unused IP space + spam [Ramachandran2006, Hu2007]
  – 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?
BGP Hijacking

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

• EFFECTS
  – **Blackhole** or **MITM** [Pilosof 2008] of the victim network

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

Select

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

Symantec.cloud

Bogon IP prefixes

Team Cymru

Possible Hijack/Suspicious

Benign
29 hijacked prefixes from Jan. to Jul. 2013
Hijack duration between 1 and 20 days
Fly-By Spammers :: Hijack Signature

• Hijacked networks
  – were **dormant** address blocks, i.e., by the time the networks were hijacked they had been left **idle** by their owner
  – advertised for a **short** period of time
  – advertised from an apparently **legitimate origin** AS but via a **rogue upstream** AS
  – see [Huston2005]

• In practice, we observed
  – **idle intervals** between 3 months and 7 years
  – hijack **durations** between 1 day and 20 days, mostly < 5 days
  – rogue **upstream ASes** were hijacked too
Case Studies ::
Suspicious BGP Routes & Spam

![Graph showing suspicious BGP announcements and spam numbers over time.](image)

- **Suspicious BGP announcements**
- **Daily number of spam**

Data points indicate a correlation between specific BGP announcement prefixes and high spam activity.
Case Studies :: Suspicious BGP Routes & Spam

• Strong temporal correlation between
  – suspicious BGP announcements and
  – spam
• BGP announcements are quite short-lived!
• No identified spam bot!
• A lot of scam web sites advertised in spam mails were hosted in the hijacked networks
Case Studies :: Suspicious BGP Routes & DNSBLs

• Only 2 address blocks appeared in the Uceprotect* blacklist at the time of the suspicious BGP announcements

Notice: blacklist entries automatically expire after 7 days

*http://www.uceprotect.net
How Stealthy Were Spammers?

• Out of 29 hijacked address blocks
  – 6 (21%) were listed in Uceprotect
  – 13 (45%) were listed in Spamhaus DROP (Don’t Route Or Peer)
    • DROP is supposed to list hijacked 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 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 address blocks regardless of their owner still being business or not
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 [Nanog2011, ISTR2012, Vervier2013, Schlamp2013] lasted 5 months
  – 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 detect these cases
How To Prevent Fly-By Spammers?

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

• BGPsec 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 is still at a too early stage

• The solution for now is thus to
  – encourage the following of routing best practices and
  – use detection systems to mitigate the effect of these attacks, e.g., by feeding IP-based reputation systems with hijacked 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 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

• 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


