SPAMTRACER: HOW STEALTHY ARE SPAMMERS?

TRAFFIC MONITORING AND ANALYSIS (TMA) 2013
PIERRE-ANTOINE VERVIER, OLIVIER THONNARD
Motivation

• CONJECTURE
  – Spammers would use BGP hijacking to send spam from the stolen IP space and remain untraceable
  – [Ramachandran and Feamster 2006]
  – [Hu and Mao 2007]

• POTENTIAL EFFECTS
  – Hijackers can steal someone else’s IP identity
  – Spam filters heavily rely on IP reputation as a first layer of defense
The Eurecom network 193.55.112.0/24 is originated by AS2200 (Renater, Eurecom’s ISP).
BGP Hijacking ::
Or the Art of Breaking the Internet

• CAUSE
  – The injection of **erroneous** routing information into BGP
  – No widely deployed security mechanisms yet
    • Ex.: RPKI, BGPsec

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

• EXPLANATIONS
  – Router misconfiguration, operational fault
    • Ex.: Hijack of part of Youtube network by Pakistan Telecom
  – Malicious intent?
BGP Hijacking :: Example

AS2200 originates 193.55.112.0/25. Very stealthy! Selected route to 193.55.112.0/25 = route through AS1904.
Fly-by Spammers :: Myth or Reality?

• STARTING POINT
  – Anecdotal evidences of spammers sending spam from unused IP space hijacked for a short period of time (< 1 day)

• OBJECTIVE
  – Validate or invalidate on large scale the conjecture about fly-by spammers

• IMPLEMENTATION
  – SPAMTRACER: collect routing information about spamming 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
- Bogon IP prefixes
- 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

Symantec.cloud
Team Cymru

Live spam feed

Symantec.cloud
Team Cymru
Data Analysis

• DATA SET
  – IP/AS Traceroutes and BGP routes from SPAMTRACER

• OBJECTIVE
  – Uncover abnormal routing behaviors
  – Classify them as benign/malicious

• REMARKS
  – BGP engineering practices are similar to BGP hijacks
  – Inter-AS routing is mainly governed by private routing policies ➔ no ground-truth!
Routing Anomaly Detection & Analysis

1. BGP Anomaly Detection
   - 1.A MOAS (hijack type 1?)
   - 1.B BGP AS Path Deviation (hijack type 2?)

2. Traceroute Anomaly Detection
   - 2.A Network/Host Reachability Anomaly
   - 2.B Hop Count Anomaly
   - 2.C AS-level Traceroute Deviation
   - 2.D Geographical Deviation

3. Identification of Hijackings
   - Benign
   - Suspicious
   - Possible Hijack

- Benign
- Sample
1. BGP Anomaly Detection

A. Multiple Origin ASes (MOASes)

B. BGP AS Path Deviation

Provider-customer or sibling relationship → BGP engineering = legitimate
2. Traceroute Anomaly Detection

A. Network/Host Reachability Anomaly

B. Hop Count Anomaly
2. Traceroute Anomaly Detection

C. AS-level Traceroute Deviation

D. Geographical Deviation
3. Identification of Hijackings

- Hijacking signatures correspond to specific combinations of routing anomalies
  - A hijacking must exhibit a BGP AS Path deviation
  - A MOAS highly increases the suspiciousness of the routing behavior
  - A Host/Network Reachability anomaly moderately increases the suspiciousness
  - A Hop Count anomaly, Traceroute AS-level path or Country-level path deviation slightly increase the suspiciousness

- Uncovered hijackings are manually investigated
  - Collected data, IRR’s, looking glasses, mailing lists
Results

• 81 identified **hijackings** in the **SPAMTRACER** data set from April 2011 to September 2011

• 61 **benign** cases
  – Customer-provider or sibling relationship between ASes in MOAS (e.g., merged companies)
  – Misclassification because of inaccurate traceroutes/IP-to-AS mapping/IP geolocation
Results

• 20 suspicious/malicious cases
  – No explanation for MOAS
  – No explanation for a major AS path change combined with other routing anomalies
  – One hijack case validated thanks to feedback from the owner

• No hijack of unused IP space for no more than one day as described in [Ramachandran 2006]
Link Telecom Hijack Case Study ::
The Story of a Sophisticated Spammer

• The network of the Russian ISP Link Telecom was hijacked for 5 months by a spammer in the U.S.

• By the time their network was hijacked, Link Telecom had suspended their activity

• The hijacker provided the U.S. ISP Internap with a fake proof of ownership of the network blocks by registering the expired linktelecom.biz domain
Link Telecom Hijack Case Study :: The Story of a Sophisticated Spammer

- Traceroutes collected by **SPAMTRACER** towards Link Telecom’s IP blocks during (AB) and after (CD) the hijack.
Conclusion

• Several hijackings were identified in the SPAMTRACER data set, one of them confirmed by the network owner.

• From the results obtained, the fly-by spammers phenomenon does not seem to currently be a significant and prevalent threat.

• Short-lived hijacks by spammers: conjecture or reality?
Future Work

• Improve the visibility of hijacks by deploying SpamTracer at large scale

• Refine the anomaly scoring system by leveraging fuzzy logic

• Improve the hijacking validation process by
  – Asking feedback from victim network owners
  – Correlating different data sources
Thank you!

Time for Q&A!
Some references


