SpamTracer: How Stealthy Are Spammers?

Pierre-Antoine Vervier
Eurecom
Sophia Antipolis, France
Pierre-Antoine.Vervier@eurecom.fr

Olivier Thonnard
Symantec Research Labs
Sophia Antipolis, France
Olivier_Thonnard@symantec.com

Abstract—**The Internet routing infrastructure is vulnerable to the injection of erroneous routing information resulting in BGP hijacking. Some spammers, also known as fly-by spammers, have been reported using this attack to steal blocks of IP addresses and use them for spamming. Using stolen IP addresses may allow spammers to elude spam filters based on sender IP address reputation and remain stealthy. This remains a open conjecture despite some anecdotal evidences published several years ago.**

In order to confirm the first observations and reproduce the experiments at large scale, a system called SpamTracer has been developed to monitor the routing behavior of spamming networks using BGP data and IP/AS traceroutes. We then propose a set of specifically tailored heuristics for detecting possible BGP hijacks.

Through an extensive experimentation on a six months dataset, we did find a limited number of cases of spamming networks likely hijacked. In one case, the network owner confirmed the hijack. However, from the experiments performed so far, we can conclude that the fly-by spammers phenomenon does not seem to currently be a significant threat.

I. Introduction

The current Internet routing infrastructure is built upon several legacy protocols that rely on the concept of trust among the interconnected entities. Cybercriminals now appear to take advantage of this vulnerability to perform BGP hijacking [1]. This attack consists in taking control of blocks of IP addresses owned by a given administrative entity without their authorization. This enables an attacker to disrupt or eavesdrop on the communications related with these addresses or to use the stolen block of IP addresses to perform other malicious activities, e.g., spamming, phishing or malware hosting.

Different well known BGP hijack incidents have already been observed in the Internet. The most famous one is probably the hijack by the Pakistani government of part of the Youtube network [2] on February 24th, 2008 in a clumsy attempt to block access to the website. While being non malicious, these incidents highlight the feasibility of such attacks.

In [3], [1], the authors show that cybercriminals are able to misuse the BGP routing protocol to hijack blocks of IP addresses for limited periods of time during which they could launch spam campaigns from, apparently, legitimate IP blocks. Those spammers are referred to as *fly-by spammers*. To the best of our knowledge, nobody else could demonstrate, until now, to which extent this assumption can be verified. However, if this claim is true, such techniques would clearly defeat the spam blacklists that anti-spam tools use as a first layer of defence against spammers. This work thus aims at reproducing the first experiments at large scale in order to confirm or not the existence of fly-by spammers.

Despite the fact that several techniques and deployed environments exist to monitor the routing infrastructure and detect hijacks, existing BGP monitoring systems have currently several drawbacks, described later, which seriously limit their use for solving the problems described here above.

In this paper, we present an environment called SpamTracer meant to study the fly-by spammers phenomenon. SpamTracer uses `traceroutes` and BGP routes to monitor the routing behavior of spamming networks identified by Symantec.cloud [4]. Routing anomalies extracted from the collected data plane and control plane routes are leveraged to identify cases of malicious BGP hijacks. The contribution of the paper is threefold: (i) we propose an environment for the study of the *fly-by spammers phenomenon*, (ii) we provide a methodology to detect *abnormal routing behaviors* from the collected `traceroute` and BGP data to help identify malicious BGP hijacks and, (iii) we provide a first report on the *real prevalence* of fly-spammers based on the first results obtained. Furthermore, by making the data set available through Symantec's Worldwide Intelligence Network Environement (WINE) [5], we invite the community to (in)validate our results by applying other analysis techniques.

II. Related Work

Several works and studies [6], [7], [1], [8], [9], [10], [11] have already been done on the detection of BGP hijacks as well as on solutions to bring authentication and integrity into BGP [12], [13] usually using cryptography. Solutions to securing BGP induce a heavy computational load on routers when using cryptography and require important changes in the protocol or the infrastructure, which currently slow down their large scale deployment.

Current BGP hijack detection techniques leverage anomalies in the routing infrastructure generated when a hijacker injects erroneous routing information. Existing techniques can be classified into two categories according to the type of information used to perform the detection: *control plane* or *data plane* information. Methods like PHAS [6] and others described in [10], [7] rely only on control plane information to assess the legitimacy of a BGP advertisement. Such techniques monitor

Version: February 01, 2013. Copyright IEEE. Authors version for personal use. Not to be offered for sale or otherwise re-printed, re-published or re-used without permission. A version of this paper will appear in IEEE TMA 2013.

BGP updates and triggers an alert when a new advertisement conflicts with their model of the Internet topology. However, they usually suffer from the high similarity between routing anomalies resulting from BGP hijacks and those resulting from benign BGP practices or misconfigurations.

Other methods leverage also information from the data plane to perform the detection. This allows collecting information about the different hosts and networks along the forwarding path from a vantage point to a monitored network. Characterizing the hosts and the networks is important as it can help distinguish between benign and malicious routing changes, e.g., a network becomes unreachable as a result of a blackhole. In iSPY [8], authors use AS-level traceroutes to detect a hijack. In Light-weight Probing [9], they trigger an alert when a significant change is observed in the distance between a set of vantage points and a monitored network. In Ping Test [11] and Argus [14], ICMP ping is used upon reception of an abnormal BGP update to verify that the network reachability is not modified by the new BGP advertisement. We extend previous approaches by leveraging many different features of the traceroutes like the IP/AS paths, the route length, the host and AS reachability. Moreover, we use an extended set of heuristics to help determine whether observed routing changes are benign or malicious. In [1], the system detects BGP anomalies and triggers routines that further check AS relationships and ping and nmap data plane fingerprints. Like many other systems, it does not deal with the hijack of unused IP space. However, this scenario is precisely the technique described in [3] that fly-by spammers presumably use. Finally, existing distributed systems like [15] already perform traceroute measurements towards a large portion of the Internet. We decided however to build our own data collection environment to be able to traceroute spamming hosts as soon as spam is received from them and thus discover possible short-living routes. Also, the authors in [16] suggests that collecting data specific to the problem we study is usually preferable to using existing datasets which may have been built for a different application.

III. Methodology

A. Overview

A BGP hijack can always be observed in BGP because this is where the routing process takes place. However, due to the lack of ground-truth data, relying only on control plane information to detect and analyse routing changes is challenging. However, data plane measurements can be leveraged to determine the impact of a routing change on the forwarding paths towards a monitored network. A tool called SpamTracer, illustrated in Figure 1, has been developed to monitor the routing behavior of spamming networks by collecting BGP routes and performing traceroute measurements repeatedly for a certain period of time after spam is received. Based on the short-lived nature of hijacks performed by fly-by spammers (no more than one day), we set the monitoring period to one week. IP-to-AS mapping of traceroutes is performed using live BGP feeds from RouteViews [17]. By performing multiple measurements on consecutive days for one week, traceroutes and BGP routes towards a given host or network can be compared and analysed in depth to find indications of a BGP hijack performed by a spammer. Because we monitor a spamming network just after spam is received, we expect to observe the change as soon as the hijack ends.

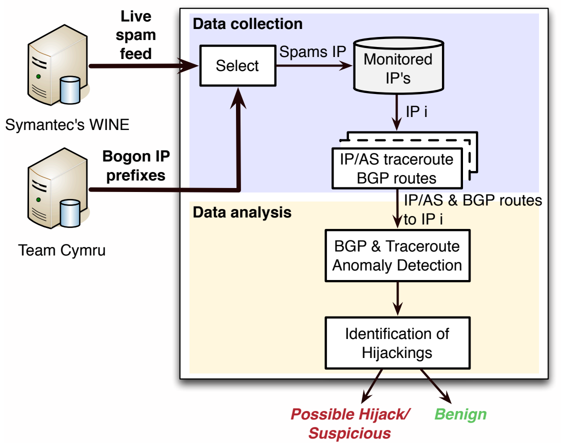
Live spam feed
Symantec's WINE
Bogon IP prefixes
Team Cymru
Data collection
Select
Spams IP
Monitored IP's
IP i
IP/AS traceroute BGP routes
IP/AS & BGP routes to IP i
Data analysis
BGP & Traceroute Anomaly Detection
Identification of Hijackings
Possible Hijack/ Suspicious
Benign

Fig. 1: **SpamTracer**: Collection and analysis of routing data for spamming networks

B. Data Collection

The data collection module of SpamTracer is based on a linear data flow where a feed of IP addresses to monitor is given as input and a series of enriched traceroutes and BGP routes are produced as output from which routing anomalies can be uncovered. The feed consists of IP addresses which were used to send spam in the last hour to Symantec.cloud spamtraps [4]. Because the spam feed consists of around 4M spam messages per day, a sampling is performed and around 10K IP addresses are tracerouted every day. Bogon prefixes (unallocated or reserved IP blocks) seen originating spam are automatically selected for monitoring as they represent unused IP space that spammers may have hijacked. Building the AS-level routes allows looking at network routes from the same perspective as BGP, which matters when studying IP prefix hijacking. The IP-to-AS mapping is performed using live BGP feeds from six RouteViews [17] servers which are worldwide distributed. The view of the routing in the Internet can differ from one location to another so geographic distribution of BGP collectors is important. The BGP AS paths from the BGP collectors to the monitored networks are also collected. Finally, further information is collected on the monitored networks and the different IP hops and ASes traversed (e.g., geolocation [18], whois [19], allocation status [20]).

C. Data Analysis

We now introduce a set of novel heuristics to identify abnormal routing behaviors from the routing data collected about spamming networks to find cases likely resulting from a malicious BGP hijack. For this task, the following data features are available for each monitored network for a period of seven days following a received spam:

- The set of daily IP/AS `traceroute`s from our vantage point to the network;
- The set of daily BGP AS paths from six RouteViews servers to the network;
- The registration and geolocation information of IP and AS hops in `traceroute`s.

The *data analysis* module of SPAMTRACER is depicted in Figure 2. It takes as input the collected data about a network and gives as output the degree of suspiciousness of the routing behavior of the analysed network. Our routing anomaly detection and analysis technique is based on two assumptions: (i) the routing anomalies must be observed by one of the six RouteViews servers and (ii) provided that they are impacted by the routing anomalies, the `traceroute`s provide the required input data to assess the suspiciousness of the routing anomalies detected in BGP.

In the remainder of this section we describe the BGP Anomaly and Traceroute Anomaly detection sub-modules depicted in Figure 2. We also introduce the set of heuristics used to *compute the suspiciousness* of the routing behavior of the analysed network based on the routing anomalies uncovered in the previous two sub-modules.

1) BGP Anomaly Detection: The first step of the routing anomaly detection is the extraction of BGP anomalies from the BGP AS paths collected daily during one week from the six RouteViews servers to the monitored networks.

Based on the attack model of BGP hijacking presented in [6], the trust-based nature of BGP allows an attacker to hijack an IP prefix (or part of it) by

Type 1: Advertising the same prefix, a subnet prefix or a supernet prefix from its own ASN which is different from the legitimate origin ASN (prefix ownership subversion);

Type 2: Advertising the same prefix, a subnet prefix or a supernet prefix using its own ASN and prepending one or more ASNs (including the legitimate origin ASN) to the AS path (AS path subversion).

(1.A) Multiple Origin AS (MOAS): this anomaly consists in an IP prefix being advertised from more than one origin AS (hijack of type 1). However, BGP engineering practices like aggregation and multihoming may introduce a legitimate MOAS [1]. The definition of a MOAS states that a *single* IP prefix is originated by multiple ASes [21]. In our case, we consider a MOAS any situation where a monitored spamming IP address is originated by multiple ASes no matter how many prefixes are involved.

We detect the following three BGP practices introducing MOAS conflicts:

(i) IP space advertised by a (single or multihomed) customer and by one of its providers (aggregated or not).
(ii) IP space advertised by multiple ASes owned by a single organisation (also known as sibling ASes);
(iii) IP anycast addressing (with multiple origin ASes);

As described in [1], other BGP engineering practices exist, including, for example, multihomed networks using a static link with one provider or using a private AS number. In the first BGP practice (i) described here above, the conflicting ASes have a customer/provider relationship so they are direct neighbours in the AS path. We detect this BGP practice by extracting customer/provider relationships from the collected BGP AS paths, from a daily AS-level Internet topology providing business relationships between ASes available at [22] and from the routing policies published in Internet Routing Registries (IRRs) provided by the Regional Internet Registries (RIRs) [23]. In the BGP practices (ii) and (iii), the conflicting ASes usually belong to the same organisation, e.g., AS20940 ”Akamai Technologies European AS” and AS21342 ”Akamai Technologies AS”. We detect such BGP practices by measuring the similarity between conflicting ASes owner names. We use the Levenshtein distance between owner names to assess their similarity.

(1.B) BGP AS Path Deviation: this anomaly consists in observing a significant change in the AS paths from one or more BGP collectors to a monitored network possibly resulting from a hijack of type 2. Instead of trying to assess the legitimacy of AS paths changes by looking at the inter-AS relationships like in [10], our approach leverages the AS paths from topologically distributed BGP collectors to detect major routing changes. We detect the anomaly by measuring the similarity between any two consecutive AS paths in the set of daily AS paths from each BGP collector individually. We use the Jaccard index between two sets of elements to compute the amount of overlap between two AS paths.

2) Traceroute Anomaly Detection: The extraction of routing anomalies from the data plane aims at determining how a routing change observed in BGP impacted the forwarding paths towards a monitored network.

(2.A) Network/Host Reachability Anomaly: this anomaly consists in observing a sudden and permanent change of reachability of the monitored network (AS) or host. Note that the Network/Host Reachability Anomaly consists of two values computed individually at the network and host levels. This anomaly suggests a major routing change altered the configuration of the monitored network, e.g., due to a blackholing hijack.

(2.B) Hop Count Anomaly: this anomaly consists in observing an important and permanent change in the length (in number of IP hops) of the `traceroute`s. This situation suggests that a major routing change occurred that permanently changed the forwarding paths. A major change in the IP `traceroute`s length can also result from a routing change only at the IP-level, e.g., a forwarding loop. Thus, upon detection of a Hop Count Anomaly, we seek to correlate this anomaly with an AS-level Traceroute Deviation.

(2.C) AS-level Traceroute Deviation: this anomaly consists in observing a significant change in the ASes traversed by `traceroute`s. The similarity between the AS-level paths is computed using the Jaccard index between each consecutive pair of AS-level paths.

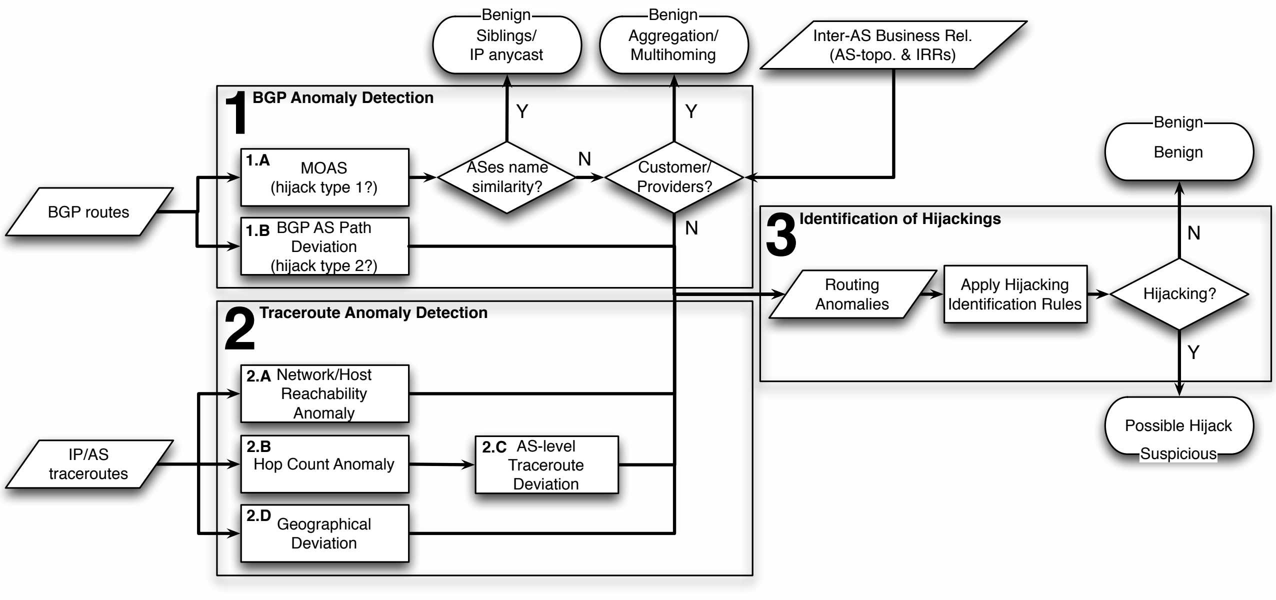

Fig. 2: **SpamTracer Data Analysis**: Detection and analysis of routing anomalies

(2.D) Geographical Deviation: this anomaly consists in observing significant discrepancies in the sequence of countries (mapped from IP hops) traversed by `traceroutes`. The assumption behind this anomaly is that country-level `traceroutes` more likely remain constant even when routing changes occur at the IP or AS levels. The similarity between country-level paths is computed using the Jaccard index.

3) Identification of Hijackings: This step aims at determining whether a monitored network exhibits a routing behavior likely resulting from a BGP hijack based on the outcome of the BGP and Traceroute anomaly detection. The BGP and Traceroute anomaly detection assigns a score between 0 and 1 to each anomaly type. So far we have applied a rather conservative threshold to each score to eliminate clearly benign cases. Then, we identify routing behaviors likely corresponding to hijackings based on the type and the number of suspicious anomalies detected. The combinations of anomalies representing the hijacking routing behaviors are thus computed based on the binary score of each anomaly. We are planning to relax this constraint in the future by removing the intermediate thresholds applied to each anomaly and identify hijackings by aggregating the score of each anomaly and computing a suspiciousness score.

In theory, the different combinations of the six routing anomalies described here above yield 64 different routing behaviors each of which can be assigned a degree of suspiciousness. However, based on our analysis, we consider certain combinations are not associated with any kind of suspicious behavior. Hence, only a subset of combinations are considered potential cases of hijackings. In order to identify the hijacking routing behaviors and use them to build hijacking identification rules, we make the following assumptions:

- the routing behavior should exhibit BGP and Traceroute anomalies so that they complement each others;
- the routing behavior should exhibit a BGP AS Path Deviation (1.B) indicating that a major routing change occurred;
- the Network/Host Reachability Anomaly (2.A) is considered the most suspicious Traceroute Anomaly as, when correlated with a BGP Anomaly, it provides a very strong indication that the routing change in BGP affected the connectivity of the victim network;
- the Hop Count Anomaly (2.B) correlated with an AS-level Traceroute Deviation (2.C) are more suspicious than the Geographical Deviation (2.D) as, when correlated with a BGP Anomaly, it indicates that a major topological change occurred which modified the AS- and IP-level forwarding routes.

The seven rules for the identification of hijackings provided in Table I corresponds to the 12 most suspicious combinations of anomalies. The degree of suspiciousness of a hijacking, indicated in the Table by the number of ”*”, is then assigned based on (i) the *number* of BGP Anomalies and (ii) the *number and type* of Traceroute Anomalies.

We also indicate in Table I using ”*” the likelihood of a hijacking corresponding to a fly-by spammer routing behavior as described by Ramachandran et al. in [3]. First, in this scenario, the hijack is assumed to be short-lived (no more than one day in Ramachandran’s observations) so we expect to observe the change from the hijacked state to the normal state of the network. Second, such a spammer is assumed to hijack unused, hence unannounced, IP space which results in a temporary route to the network being injected in BGP. As a consequence, we should observe a BGP AS Path Deviation (1.B) resulting from the difference between the temporary route (during the hijack) and the absence of route (after the hijack). Similarly, a Network/Host Reachability Anomaly (2.A), a Hop Count Anomaly (2.B), an AS-level Traceroute Deviation (2.C) and a Geographical Deviation (2.D) should be observed due to the change in the reachability as well as the major change in the forwarding paths between the hijacked state and the normal state of the network. Finally, a MOAS conflict (1.A) can be observed if the unused IP space is hijacked by advertising a less specific (covering) prefix than a prefix already advertised.

IV. Experimental Results

In this section we present the experimental results of the analysis of data collected between April 2011 and September 2011. We applied the BGP and `traceroute` anomaly detection heuristics on the SPAMTRACER dataset. We then applied the hijacking identification rules of Table I on the uncovered routing anomalies.

Out of 31,642 spamming networks involved in one or more routing anomalies, 81 cases were flagged as hijackings showing that considering many different routing anomalies and combining them is necessary to reduce the number of alarms generated. While it is hard to assess the false negatives resulting from the heuristics, it is unlikely that fly-by spammers would exhibit fewer anomalies than we consider. The second noticeable fact is that no serious hijacking and no serious case of fly-by spammer hijacking (rules 6 and 7) were found. No network thus exhibited a strong abnormal routing behavior.

Rules 1 and 3 identified 3 networks that exhibited a major change in the BGP AS paths (1.B) and an anomaly in the Hop Count (2.B) and the AS-level `traceroutes` (2.C). Two networks were also involved in a MOAS conflict (1.A). Rules 2 and 4 identified 78 networks for which a BGP AS Path Deviation (1.B) and a Network/Host Reachability Anomaly (2.A) were detected. Among those networks, 27 networks exhibited a MOAS conflict (1.A).

A. Investigating Hijackings

In order to determine whether the identified hijackings were real cases of malicious hijackings and possibly fly-by spammers, we verified the different cases using information from Internet Routing Registries (IRRs) provided by Regional Internet Registries (RIRs), external routing information databases [24], [25] as well as network owner feedback on mailing lists like NANOG [26]. We searched in the `whois` databases for possible links between the conflicting ASes in MOAS. We also used external routing information databases to identify routing anomalies that were stable over time.

Using our validation approach we classified 61 hijackings out of 81 as benign for the following reasons:

- a relationship between ASes in MOAS could be found in the `whois` databases (e.g., same contact and address, merged companies, provider/customer);
- our system misclassified some routing changes as anomalies due to incomplete `traceroutes`, inaccuracies in the IP-to-AS mapping or in the IP hops geolocation.

The 20 remaining hijackings exhibited the following routing behaviors:

- no relationship between ASes in non stable MOAS could be found in the `whois` databases;
- a major change in the BGP AS paths that impacted the reachability of the network/host. As we could not verify the legitimacy of those changes, we considered them as suspicious. We could correlate some of these hijackings with a hijack report on NANOG [27].

B. Case study

For five months from April to August 2011, the network of the Russian company Link Telecom (AS31733) was hijacked by a spammer [27], [28]. The spammer carried out the hijack by providing the US ISP Internap (AS12182) with a fake proof of ownership of the Linktel network, which then allowed them to advertise the victim's prefixes using the origin ASN 31733. It is noteworthy that by the time the network was stolen, the victim company had suspended its activity, thus leaving its blocks of IP addresses *unused* and making them a target of choice for the hijacker.

SPAMTRACER monitored some prefixes of Link Telecom after spam was received from them and observed the change resulting from the network administrator regaining control over his network.

While this case is a validated malicious hijacking performed by a spammer, it is worth noting that it does not correspond to our assumption about the behavior of fly-by spammers as described in [3] in which the hijack is short-lived.

V. Discussion

From the investigation of the identified hijackings, it turns out that only a few cases could not be explained by any legitimate BGP practice or misclassification by the system. So far, there are some evidences of hijacked spamming networks but it does not currently seem to be a commonly used practice by spammers. Because our system monitors a selected set of spamming networks observed everyday by Symantec.cloud spamtraps, it is possible that we do not have a complete visibility of hijacking spammers. We are working on improving the system scalability to extend its monitoring capability and thus its visibility. Also, as explained in [16], the routing information extracted from BGP and `traceroute` can provide an incomplete and inaccurate view of the Internet routing. We consider these limitations in the design of our system.

We could not observe any hijacking strictly matching the behavior described by [3] in which spammers hijack unused IP space for no more than one day. Instead we did observe different long-lived hijackings. This suggests that spammers may not currently need to repeatedly perform short-lived hijacks but can instead hijack an unused network and use it until the legitimate owner or an ISP figures out and takes appropriate actions to stop the hijack.

Investigating a case of BGP hijack is a difficult task mainly due to the fact that routing policies are usually set up and

Rule	(1.A) MOAS	(1.B) BGP AS Path Dev.	(2.A) Net./Host Reachability	(2.B) Hop Count & (2.C) Tr. AS-lvl Dev.	(2.D) Geo. Dev.	Hijack?	Fly-by spammer?
1	✗	✓	✗	✓	✓/✗	*	*
2	✗	✓	✓	✗	✓/✗	*	*
3	✓	✓	✗	✓	✓/✗	**	*
4	✓	✓	✓	✗	✓/✗	**	*
5	✗	✓	✓	✓	✗	**	**
6	✗	✓	✓	✓	✓	***	***
7	✓	✓	✓	✓	✓/✗	***	***

TABLE I: Rules for identifying hijackings and fly-by spammers based on BGP and `traceroute` anomalies. The number of ”*” indicates the suspiciousness of the hijacking

kept private by network owners. We are planning to automate getting feedback from the operators of networks involved in identified hijackings to facilitate the validation process. We could also check in the slowly emerging RPKI [12] for Route Origin Authorisations (ROAs) in case of MOAS conflicts.

In the analysis of the data we performed so far, we applied thresholds to each anomaly score to eliminate clearly benign cases. We are thus considering to use fuzzy logic to aggregate anomaly scores and thus improve the hijacking identification process thanks to a more accurate calculation of the suspicious cases.

VI. Conclusion

In this paper we have motivated the need for and presented a new environment to study the fly-by spammers phenomenon. We have collected BGP and `traceroute` data related to spamming networks and further applied heuristics to identify hijackings. While we could identify a limited number of hijacks correlated with spam, one of which validated by the network owner, we could not conclude that fly-by spammers is currently a significant nor a really prevalent phenomenon. Finally, we invite the community to analyse our dataset made available through Symantec’s WINE [5] using other analysis approaches.

Acknowledgments

We would like to thank *Symantec.cloud* for providing us with the spam dataset. This research work has been carried out in the context of the FP7 European project VIS-SENSE (http://www.vis-sense.eu/) under the grant agreement nr. 257495.

References

[1] X. Hu and Z. M. Mao, “Accurate Real-Time Identification of IP Prefix Hijacking,” in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP ’07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 3–17.

[2] “Pakistan hijacks YouTube,” http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml.

[3] A. Ramachandran and N. Feamster, “Understanding the network-level behavior of spammers,” in *SIGCOMM ’06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*. New York, NY, USA: ACM, 2006, pp. 291–302.

[4] “Symantec.cloud,” http://www.symanteccloud.com/.

[5] “Symantec’s Worldwide Intelligence Network Environment (WINE),” http://www.symantec.com/about/profile/universityresearch/sharing.jsp.

[6] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, “PHAS: A prefix hijack alert system,” in *Proc. USENIX Security Symposium*, 2006.

[7] H. Ballani, P. Francis, and X. Zhang, “A study of prefix hijacking and interception in the Internet,” in *Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM ’07. New York, NY, USA: ACM, 2007, pp. 265–276.

[8] Z. Zhang, Y. Zhang, Y. Charlie, H. Z. Morley, and M. R. Bush, “iSPY: Detecting IP Prefix Hijacking on My Own,” in *Proc. ACM SIGCOMM*, 2008.

[9] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, “A light-weight distributed scheme for detecting IP prefix hijacks in real-time,” in *Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM ’07. New York, NY, USA: ACM, 2007, pp. 277–288.

[10] J. Qiu and L. Gao, “Detecting Bogus BGP Route Information: Going Beyond Prefix Hijacking,” in *In Proc. SecureComm*, 2007.

[11] M. Tahara, N. Tateishi, T. Oimatsu, and S. Majima, “A Method to Detect Prefix Hijacking by Using Ping Tests,” in *APNOMS ’08: Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 390–398.

[12] R. Bush and R. Austein, “The RPKI and Origin Validation,” http://www.nanog.org/meetings/nanog46/presentations/Monday/Bush_security_N46.pdf, June 2009.

[13] S. Kent, “Securing the Border Gateway Protocol: A Status Update,” in *In Seventh IFIP TC-6 TC-11 Conference on Communications and Multimedia Security*, 2003, pp. 2–3.

[14] X. Shi, Y. Xiang, Z. Wang, X. Yin, and J. Wu, “Detecting prefix hijackings in the internet with argus,” in *Proceedings of the 2012 ACM conference on Internet measurement conference*, ser. IMC ’12. New York, NY, USA: ACM, 2012, pp. 15–28. [Online]. Available: http://doi.acm.org/10.1145/2398776.2398779

[15] “iPlane: An Information Plane for Distributed Services,” http://iplane.cs.washington.edu/.

[16] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush, “10 Lessons from 10 Years of Measuring and Modeling the Internet’s Autonomous Systems,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, pp. 1810–1821, 2011.

[17] “University of Oregon RouteViews Project,” http://www.routeviews.org/.

[18] “Maxmind,” http://www.maxmind.com/.

[19] “Team Cymru IP to ASN,” https://asn.cymru.com/.

[20] “Team Cymru IPv4 Fullbogons,” http://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt.

[21] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, “An analysis of BGP multiple origin AS (MOAS) conflicts,” in *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, ser. IMW ’01. New York, NY, USA: ACM, 2001, pp. 31–35.

[22] “Internet Topology Collection,” http://irl.cs.ucla.edu/topology/.

[23] “IRR.net,” http://www.irr.net/.

[24] “Huricane Electric Internet Services,” http://bgp.he.net/.

[25] “Ripestat,” http://www.stat.ripe.net.

[26] “NANOG (North American Network Operators’ Group),” http://www.merit.edu/nanog/.

[27] “Prefix hijacking by Michael Lindsay via Internap,” http://mailman.nanog.org/pipermail/nanog/2011-August/039381.html, August 2011.

[28] “Symantec Internet Security Threat Report: Future Spam Trends: BGP Hijacking. Case Study - Beware of ”Fly-by Spammers”,” http://www.symantec.com/threatreport/, April 2012.