

Measuring Internet Resilience through BGP

Nicolas Vivet & Guillaume Valadon
firstname.lastname@ssi.gouv.fr

August 7, 2015

Abstract

This submission is an extended version of the work that was presented during the PacSec and NSC conferences in 2014 ¹.

The main goal of these presentations was to raise awareness of BGP routing security issues, and the detection of specific routing events called IP prefixes hijacks. For RAIM, we would like to take the opportunity to present our work related to the Internet French observatory that we have been conducting since 2011. More specifically, we want to emphasize on both technical and research challenges that must be tackled to address the efficient detection of prefixes hijacks.

1 The Internet French Observatory

Introduced by the ANSSI ² in 2011, the Internet resilience observatory strives to improve knowledge of the Internet by studying the technologies that are vital for it to operate correctly. One of its objectives is to increase collective understanding of the Internet to have the most consistent and complete view as possible. In particular, about its resilience that can be characterised by a set of measurable technical indicators. Some of these indicators are directly derived from engineering rules, called best practices,

¹https://pacsec.jp/psj14/PSJ2014_Guillaum_presentation.pdf

²The French national authority for the defence and the security of information systems.

in particular defined by the technical and scientific community.

Thus, the observatory identify and measure indicators and publish the results and methodologies in a yearly report ³. We are thinking about publishing these on a different supports, like a website, to get better feedbacks from the operator and scientific community.

2 Measuring resilience

In order to assess the Internet resilience, the observatory perform several passive and active measurements. Our goal is to define technical *indicators* regarding two protocols that are essential for the Internet to function correctly: BGP and DNS.

Regarding BGP, the observatory uses the following indicators:

- Number of French Autonomous Systems
 - active
 - inactive
- Autonomous Systems connectivity
- Registries conformity
 - IRR
 - RPKI

³http://www.ssi.gouv.fr/uploads/2014/10/rapport_observatoire_2013_en.pdf

- Routing anomaly detection
 - IP Prefix hijacks
 - Outages
 - Full view leaks

These analysis are based on public data ranging from raw BGP data (from RIPE RIS) to textual Internet Routing Registries (RIPE, APNIC, ...) or even RIPE Atlas probes.

The observatory also works on other measurements related to DNS, TLS as well as DDoS.

3 Challenges

We developed a solution to detect potential hijacks on every prefixes announced on the Internet in near real-time. This solution is part of a larger infrastructure allowing the observatory's researchers to share network data and enable collaboration on network anomalies analysis.

However, we also face several difficulties. For example in classifying the events as legitimates or malicious automatically. While a lot of these potential hijacks can be validated using declarative registries, we often rely on more complex algorithms.

We have implemented such classification algorithms for example by establishing relationship between Autonomous Systems in order to know if two Autonomous Systems a business relation or if they belong to the same company. This proved to reduce significantly the number of potential hijacks. However, about a fifth of the anomalies remain unclassified and must be processed manually by someone who knows the Internet ecosystem. We think there might be rooms for improvements in this field especially with supervised classification (such as machine learning).

Last year, we tried to correlate data-plane path measurements (traceroutes) with control-plane

AS_PATH during prefix hijacks and detect traffic misdirection in order to characterise malicious attacks. But while we were able to characterize a malicious hijack using this technique, it seems difficult to adapt as an automatic classification.

Some work is also being done regarding full view leaks which is one of the main cause of prefix hijack. Their detection might also improve the classification of legitimate and malicious hijacks.

Moreover, we have seen emerging more sophisticated attacks using Autonomous Systems hijacks that are more difficult to detect because of a lack of reliable detection algorithm.

4 Conclusion

We are looking forward to share our work and results with the community hoping to give an interesting overview of the challenges we face in the detection of IP routing anomalies.