Attack Pattern Discovery for Autonomous System

V. Sukanya

Dr.M.G.R Educational and Research Institute University, Chennai.

Abstract:

The Border Gateway Protocol is a most important component of the Internet's routing infrastructure .It is used to exchange the routing information between the Autonomous System. The BGP is the one which helps to verify the vulnerability, authenticity and also helps in prioritize the traffic .By analyzing the network traffic data, we can generate a malicious pattern and by deploying it in the BGP makes it to be more interoperable and to find the anomaly. The document proposes the need for the deployment that helps in the forensic investigation.

Keyword: Border Gateway Protocol, Autonomous System, External Border Gateway Protocol

1. Introduction:

The Internet is plagued by malicious activity, from spam and phishing to malware and denial-of-service (DoS) attacks. Much of it thrives on armies of compromised hosts, or botnets which are scattered throughout the Internet. Some network employ lax of security because of which there may exit malicious activity but some networks are highly secure and prevent malicious activity.

While many attacks are distributed across botnets, investigators and network operators have recently identified malicious networks through high profile autonomous system (AS) depeerings and network shutdowns. This paper also encloses a systematic pattern to identify the degree of autonomous system and it also helps the ISP to ensure that the necessary defense Mechanisms to be taken for preventing the malicious activity. In order to develop a systematic approach first the ISP has to mine the network and the clear metric is obtained by the BGP peers.

The main advantage of identifying the malicious network is that the peering agreement is automatically cancelled when it comes to the malicious network. It also helps in the priorities the traffic based on the cleanliness of the As.

2. Autonomous System:

On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator on behalf of a single administrative entity. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Networks within an autonomous system communicate routing information to each other using an Interior Gateway Protocol (IGP). An autonomous system shares routing information with other autonomous systems using the Border Gateway

Protocol (BGP). Previously, the Exterior Gateway Protocol (EGP) was used. In the future, the BGP is expected to be replaced with the OSI Inter-Domain Routing Protocol (IDRP).

3.Broder protocol gateway:

The Autonomous System exchanges the routing information between the gateway hosts using border gateway protocol. Internet gateway hosts uses BGP often. The BGP contains routing table which contains the address and the necessary information .The main Hosts using BGP communicate by means of Transmission Control Protocol and also send updated router table information but only when one host has detected a change.

The latest version of BGP-4 contains most administrative privilege and easy to configure. When the AS in local network communicate by means of IBGP and it doesn’t work well so it was replaced by EBGP which has its own limitation like fixed to tree topologies

Later emerged Border Gateway Protocol which replaced IBGP and EBGP. BGP overlays on both IBGP,EBGP and Open Shortest Path First(OSPF) interior gateway.

4. BGP peering:

The BGP-4 protocol uses a UPDATE message and rout propagation algorithm. The IP address is identified by a prefix which is identified by significant bits. An UPDATE message consists of three major parts. “Withdrawal” it means the prefix which are unreachable.” network layer reach ability information (NLRI)”- a list of IPV$ address prefixes that are reachable. “Path attributes”-the characteristics of NLRI path. These path attribute refer to the AS path. When propagating the UPDATE message is sent to the neighboring aS.

1. Each BGP speakers receives UPDATE message from the neighboring peer that contains routing information of all the destination peers.
2. The UPDATE was intended for the BGP speaker or AS that received it.
3. The peer actually sending the UPDATE was authorized to act on behalf of its AS to advertise the routing information in the UPDATE to BGP speakers in the recipient AS.
4. The AS that originates the route contain the BGP speaker which provides all the information of the reachable destination and the entire organisation that owns them.
5. The UPDATE message also provides the indicates the withdrawn route
6. Finally the BGP speaker sends and receives the UPDATE information to start processing.

5.DDoS Attack:

A denial of service (DDoS) attack occurs when a system is not providing services to authorized clients because of resource exhaustion by unauthorized clients. In wireless networks, DDoS attacks are difficult to prevent; it is also difficult to stop an ongoing attack, and the victim and its clients may not even detect it. The duration of such DDoS may range from milliseconds to hours. A DDoS attack against an individual station enables session hijacking.

6.Phishing Attack: Phishing

The process of attempting information such as usernames, password and credit card details by masquerading as a trustworthy entity by means of electronic communication. Many popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing sites may contain links to websites that are infected with malware. Phishing attack is done normally by means of e-mail spoofing, directed messages or redirecting to a website where the users enter all the personal information. Phishing incidents include legislation, public awareness and technical security.

7. Similarities:

The DDoS attack is the one where more no of request from different IP prefix which makes the server down. Similarly the Phishing sites are the one where more directed messages send to different IP prefix by means of electronic communication. So by grouping the network events rather than networks flow, we can generate an pattern to distinct the malicious attacker.

8.BGP Behaviour:

The BGP behavior can be viewed with the Routing Table. The prefix of particular AS appear to be disconnected more often, then it is said to be under malicious activity. The AS which is unreachable for longer amount of time then it is said to be in malicious activity. so overall by these behaviour and the prefix we can generate a pattern.

9. Attack Pattern Generation:

we now present the main pattern generation. By analyzing the existing routing events the candidate bubble are generated.

1.when ever the AS with the same prefix often tend to peer often then generate a bubble for that prefix

2.The AS with higher degree of peering is also included as a bubble.

3.Now a feedback loop is used the bubble is compared with the candidate bubble .if bubble is present then the connection is rejected.

4.And bubble is not present with the candidate bubble then the peer with the AS is established.

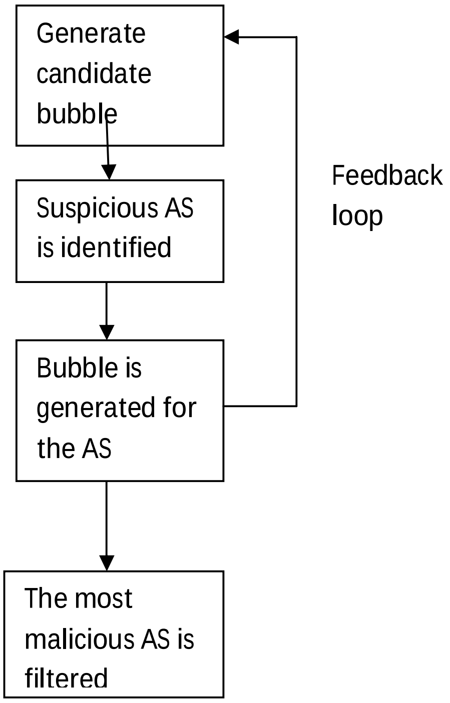
Generate candidate bubble
Suspicious AS is identified
Bubble is generated for the AS
The most malicious AS is filtered
Feedback loop

Fig.1.overview of algorithm

10.Conclusion:

In this paper , proposed the attack pattern generation for Autonomous System. Our analysis can be used to help increase ISP accountability and can become a mechanism to combat malicious activity. By providing a comparison to equivalently sized networks, we can highlight the ASs most in need of attention and which would

only offer diminishing returns. This information can also be used in peering agreements to place pressure on ISPs to respond to malicious activity.

11.References:

1] J. Hruska, "Bad seed ISP Atrivo cut off from rest of the Internet," 2008[Online].Available:http://arstechnica.com/security/news/2008/09/bad-seed-isp-atrivo-cut-off-from-rest-of-the-internet.ars

[2] B. Krebs, "Major source of online scams and spams knocked offline," 2008 [Online]. Available: http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html.

[3] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway
Protocol (S-BGP)," to appear in IEEE JSAC.

[4] S. Kent, R. Atkinson, "Security Architecture for the
Internet Protocol," RFC 2401, November 1998.

[5] D. Bizeul. Russian Business Network Study. http://www.bizeul.org/files/RBN study.pdf, 2007.