Shield-BGProtect: IP Hijack Detector

Know when your data takes a detour after it leaves your network

Our unique IP address monitoring solution, Shield-BGProtect, is built upon data gathered by numerous software agents that we call “sentinels”. These “sentinels” are installed worldwide to perform active route monitoring by sending probes toward our client’s networks. The sentinel’s measurements are controlled to millisecond accuracy using a patented algorithm. The data they gather is sent, in real time, to cloud servers where advanced big-data analytics is performed.

Shield-BGProtect provides continuous active and passive monitoring of a customers' sensitive IP address space. We immediately inform customers about network security and network performance related incidents. Our dashboard allows them to investigate and mitigate these incidents.

The main features of Shield-BGProtect are:

- Uses 100s of “senitels” map the Internet routes upon which client data travels
- Incoming traffic monitoring
- Detects data-plane hijack attacks
- Dashboard allows study of an attack in real time as well as perform forensic analysis of past events
- Sends reports about malicious attacks
- Not limited to identifying attacks using BGP hijacks

How it works:

Shield-BGProtect enables organizations to accurately monitor their data as it travels over the Internet to ensure that if it takes a detour they are aware and can take immediate action to remediate the potential theft etc.

The Internet is a complex network, comprised of thousands of interconnected Autonomous Systems (AS). Considerable research is done in order to infer the undisclosed commercial relationships between ASes. These relationships dictate the routing policies between ASes. These policies are a crucial part in understanding the Internet’s traffic and behavior patterns. This work leverages Internet Point of Presence (PoP) level maps to improve AS Type of Relationship (ToR) inference.

We employ a method which uses PoP level maps to find complex AS relationships and detect anomalies on the AS relationship level. We present results of this method on ToR reported by CAIDA and report several types of anomalies and errors. The results demonstrate the benefits of using PoP level maps for ToR inference, requiring considerably fewer resources than other methods theoretically capable of detecting similar phenomena.

Better Geolocation mapping of the Internet:

Our solution uses a proprietary algorithm that crawls the Internet Point of Presence (PoP) level graph to improve the accuracy of geolocation, combining information from both geolocation databases and delay measurements. We aggregate IPs to PoPs before localization, and we aggregate IP links to PoP edges to

clean delay errors for multi-lateration. The input from multiple Geolocation databases helps in cleaning noise, and so does the comparison between the location of collocated anchor PoPs.

We constantly validate mapping performance using ground truth data from various sources. This improves geo-location and is helped by additional validation data collect from our “sentinels”.

***What do Attackers do*?**
It is difficult for an attacker to know which BGP hijack attacks will be noticed by today’s monitoring systems. The attacker must assume that his attack will be noticed, so he will keep his hijack attack very short – probably no more than a few hours. This is enough time to create significant damage to the attacked network, but may not be suitable for cases when there is a need for a long-lasting attack.

To make stealth attacks, attackers have started using data-plane hijack attacks. Instead of using the BGP protocol to divert packets towards the attacker, the attacker directly changes the forwarding table in the relevant routers on the way. Gaining access to ISP routers can be accomplished in one of several ways:

Running a penetration attack on the routers
Gaining the router password from an inside collaborator
Using backdoors in routers

***Isn’t BGP monitoring good enough*?**
No. BGP hijacks can be detected by listening to BGP announcements. In recent years, hundreds of malicious attacks have been detected on the Internet every month. To monitor the attacks, it is necessary to connect to an AS with a dedicated communication channel. This requires approval of the AS. Since an AS is reluctant to let an outside source connect with a dedicated communications channel, only a small portion of the BGP announcements can be monitored, and many hijack events go unnoticed.

Shield-BGProtect Solution:

As discussed above, most current solutions are based on small scale BGP monitoring which is limited in its ability to identify attacks and is also limited only to attacks using BGP hijacks. Our solution can identify all hijacks, regardless of the technique that is used. In addition to attack alerts, our customers have access to a dashboard that enables them to study the attack in real time, as well as to perform forensic analysis of past events. The dashboard gives our customers valuable network performance data, in addition to hijack protection.

We offer two independent services which complement each other but can be purchased separately:

1. Incoming real-time traffic monitoring - warns the network administrator about hijack attacks on its IP space or DNS, and identifies network performance problems. There is no need to install any SW or HW in the company network. Alarms can be sent via e-mail, SMS, or syslog/STIX messages.

2. Outgoing real-time traffic monitoring - warns the network administrator about hijack espionage attacks and blocks the targeted outgoing traffic. Installation of a low-profile agent on the company Internet gateway is required. The agent can be installed on any machine.

We supply a web interface (dash board) that enables real-time performance monitoring of the network leading to the monitored sites. In addition, we supply periodic reports about malicious attacks and reports about the company site performance as seen from the Internet.

Optional Requirements:

A sentinel (software monitoring agent) can be installed in the client's colo or local network. This can help add more detail to the existing geo-location graph. The sentinel's requirements are very minimal:
CPU: 1 Cores
Memory: 1 GB
Storage Space: 20 GB
Network: 1Gbe
Ports need to be opened: PING & TRACEROUTE

Further details:

The 'glue' holding the Internet together uses two protocols:

The Internet Protocol (IP)
The Border Gateway Protocol (BGP)

IP defines how information is exchanged between end systems at the network level, and requires that every device connected to the Internet (such as a computer or router) has a unique global address - the IP address. The source and destination IP addresses are placed in each packet of information sent, similar to the addresses on letters sent with by mail.

IP addresses are assigned in blocks of consecutive numbers to Autonomous Systems (if the AS is an ISP, it assigns individual IP addresses to home customers, or chunks of an address block to business customers). Information packets propagate through the Internet individually. Each router in the network looks at the destination IP address in the packet and forwards it according to a forwarding table.

The forwarding tables are built with the Border Gateway Protocol (BGP), the Internet routing protocol. With BGP, each AS announces to its neighbors the IP address blocks that it owns. These announcements ripple through the network. If AS1 announces that it owns an IP block that actually is owned by network AS2 (due to an error or as a result of malicious intent), traffic from a portion of the Internet destined for AS2 will actually be routed to AS1. This is called a BGP hijack. The amount of traffic routed from AS1 to AS2 depends on a variety of factors, but the amount can be very large.