Chapter 4

SYSTEM ARCHITECTURE

4.1 Scalable Architecture

Since, DNS and BGP together produce several Billions of data events per minute, a highly scalable framework has been developed that can collect and process the data in real-time. The framework consists of DNS and BGP sensors that collect the data in a distributed manner. These sensors receive data directly from the DNS servers and BGP enabled routers. To ensure that, the introduction of this system does not impact the functionality of the DNS and BGP systems, they are designed to collect the passive information in the form of out-of-band mode. A system has been developed that can detect both suspected prefix and path announcements in an efficient way. Features are selected based on thorough study on the protocols and recent real-world hijack incidents.

The collected data is parsed and aggregated and then sent to real-time and non-real-time analysis engine that runs highly scalable distributed machine-learning algorithms. The query-router (standalone) services that controls the communication between different modules. The query-router also provides an interface with the message broker. A
Figure 4.1: Framework Architecture
subsystem known as Front-End Message Router controls the communication between the Interactive Visualization and analysis engine on the processed data. The Figures 4.1 and 4.2 below depict the standalone and scalable architecture of the framework respectively.

The present research work proposes to deploy the standalone architecture in individual Tier-1 ISPs. Each standalone system is capable of handling few millions of DNS and BGP data per second without any stability issues. Hence, several Terabytes (TB) of data were able to collect within a day. However, monitoring a single ISP might not be enough to get an overall situational awareness of a malware propagating through a zone or country, thus resulting in monitoring and correlating the network activity of several Tier-1 ISPs. The proposed scalable architecture in this research work employs distributed and parallel algorithms with various optimization techniques that make it capable of handling huge volume of data. The scalable architecture also leverages the processing capability of the General Purpose Graphical Processing Unit (GPGPU) cores for faster and parallel analysis of DNS and BGP data. The framework architecture contains two types of analytic engines - real-time and non-real-time analytic engines. The purpose of analytic engine is to detect malicious activities thereby generate an alert in case of threat.

4.2 Supporting Services

The important supporting services needed for this project are explained in this section.

- **Passive Sensor:** The Passive Sensor collects DNS Query/Response from the
Figure 4.2: High-level architecture correlating data from multiple ISPs

DNS Servers (Any DNS Server). The passive sensor captures Network Traffic from DNS Servers and passes it to an application. The parser inspects the DNS Response Packet, converts it into human readable format and forwards it to DNS Log Collector. The Passive Sensor could be installed inside the DNS Server itself or any mirrored traffic could be sent to the sensors. Each Sensor could process the data from multiple DNS Servers if needed. It collects data passively from DNS Servers without affecting the DNS Server.

- **Active Sensor:** This sub-system performs an active DNS Query related to the
given sources, to collect data and perform various analysis. It’s main sources are: DNS server, WHOIS server, application programming interfaces such as Google Safe browsing API, and other DNS databases.

- **WHOIS Server:** This will provide information associated with a Domain or IP Address. Queries will be forwarded to corresponding WHOIS server for that particular Domain/IP address. The information related to domain and IP are explained below: For a domain, query is sent to retrieve the following information:
  
  - Registrant name, address, email, phone.
  - Registrar name, address, email, phone.
  - Administrator name, address, email, phone.
  - Domain registered date, expiration date, authoritative name server etc.

For an IP address the fields are:

  - Owner
  - Prefix (Network)
  - ASN
  - Location
  - Expiration Date

- **Online API’s:** Some of the analysis results could be correlated with the online external systems for validation and cross-correlation.
• **Log Collector and Parser:** This subsystem collects the parsed DNS Responses from distributed sensors and forwards it to the collector. The collector looks up the Geo-Location and details of ASN of each IP address (Client IP, DNS Server IP, and A Records in Resource records) in the DNS Responses. The parser uses the Geo IP database to find Geo-location (city, country, latitude, longitude) of an IP Address. ASN database is used for finding details of ASN (AS Number, AS Name) of an IP Address. This data will be appended with original data coming from sensors and publish to queue for real-time and batch analysis.

• **Query Router Service:** It is a standalone service, which controls the communication between different modules. It also interfaces with public message broker.

• **Front-End MessageRouter:** As a standalone service, this subsystem controls all the communication to-and-from the front-end UI. It also interfaces with the respective back end subsystems.

• **Internal Router:** Internal router software is peered with the BGP Router to get BGP Updates in a configurable time interval such as 5 minutes etc.

• **BGP Monitor:** The BGP monitor subsystem is responsible for collecting BGP Update-messages in real-time. It gets updates from the TCP port as a stream and stores them in an XML file format. The parsers will produce BGP update-messages in one single format, after extracting the data from two different sources. A Distributed Log Aggregator collects this parsed data to store it in a distributed
4.3 Data Collection

DNS data are collected in a passive manner by reading from the mirrored traffic using promiscuous mode on DNS communication information between the DNS server and the DNS clients. The data consists of DNS queries and the corresponding DNS answer made by the DNS client and DNS server respectively. The extracted data is analyzed for malicious events. The BGP data is collected by adding a read-only peer to a BGP speaking router. The read-only peer collects the data that occurs in the form of BGP updates, announcements, neighbor information etc. The BGP data consists of the route and prefix information. By analyzing the behavior of prefix announcements, route announcements and updates and comparing them with their previous historical behavior, this research aims to identify the malicious announcements, malware propagation and activities.

4.4 Conclusion

For this research, a real-time distributed Big Data framework was developed for analyzing large volumes of network data events. This framework focuses on providing situational awareness by analyzing and correlating DNS and BGP logs. The developed framework is capable of analyzing more than 2 Million events per second and it could detect the malicious activities within them in real-time. The developed framework can be scaled out to analyze even larger volumes of network event data by adding...
additional computing resources. The scalability and real-time detection of malicious activities from early warning signals makes the developed framework stand out from any system of similar kind.