# Operations and Intelligence Report
# INSPIRA HEALTH NETWORK

## June 2016

BEST IN CLASS – INFORMATION SECURITY
INTELLIGENCE AND OPERATIONS

**Table of Contents**


**1. About This Report ..... 3**

**2. Confidentiality ..... 3**

**3. Scope of This Report ..... 4**

GLESEC Contracted Services ..... 4

**4. Executive Summary ..... 4**

Risk Value ..... 4

Attack Summary ..... 7

Geography ..... 8

Category Distribution ..... 9

Port Activity ..... 11

Known Threat Sources by Threat Type ..... 12

Vulnerability Summary ..... 13

Risk Distribution ..... 18

**5. Recommendations ..... 22**

**6. Security Intelligence ..... 40**

Known Threat Source Information ..... 43

Bandwidth Information ..... 54

Vulnerability Information ..... 62

**7. Security Operations ..... 69**

**8. Appendix 1 – Critical Attack Sources (WHOIS Information) ..... 74**

**9. Appendix 2 – Top Scanners Blocked (WHOIS Information) ..... 84**

**10. Appendix 3 – Glossary of Terms ..... 84**

## *1. About This Report*

The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the systems under contract. The information generated by these systems is then aggregated, correlated and analyzed. The more complete the set of systems under contract the more accurate and complete the results will be. The report is organized to provide an executive summary with recommendations (as necessary or applicable) followed by more detailed information.

We at GLESEC believe information security is a holistic and dynamic process. This process requires on-going research and follow up. Holistic since no single "device" can provide the security necessary for an organization. Technology alone cannot provide the security necessary, but people that understand the operations and information generated by the security devices are a key to proper security. The process is dynamic since due to the nature of Internet security given the constant discovery of new security vulnerabilities and exploits, the proliferation of hacking tools that make it easier for script-kiddies with minimal knowledge to cause damage. The increase in malware, phishing, insider threats, espionage, organized crime, intellectual property theft, and hacktivism are the very cause of information security exposure and are most commonly driven by financial gain.

## *2. Confidentiality*

GLESEC considers the confidentiality of client's information as a trade-secret. The information in this context is classified as:

a) Client name and contact information
b) System architecture, configuration, access methods and access control
c) Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

## *3. Scope of This Report*

## GLESEC Contracted Services

**MSS: Managed Security Service (full outsourcing)**

| Service | Manufacturer | Model | Update Expiration | Service Expiration |
|---|---|---|---|---|
| MSS-APS | Radware | DefensePro 516 ODS2-S1(Bridgeton) | 01/01/17 | 01/01/17 |
| MSS-APS | Radware | DefensePro 516 ODS2-S1(Elmer) | 01/01/17 | 01/01/17 |
| MSS-VME | Beyond Security | AVDS | 01/01/17 | 01/01/17 |

## *4. Executive Summary*

This report corresponds to the period from June 1, 2016 to June 30, 2016.

This month we see a decrease of 21% in the attack activity but an increase of 31% of critical attacks from prior month. The attacks this month are predominant of medium to large duration (less than 1 minute and ten to thirty minutes) and targeting multiple port sand port 23. Over 50 percent of the attacks are coming from known threat sources that GLESEC gathers and correlates with the information produced by the protection systems (DefensePro). The attacks are mostly from the**: USA, China, Netherlands, Japan, Russia, Brazil, France, Poland, Germany, Vietnam .** A significant number of attacks are scanning which can be considered reconnaissance and is what precedes further attacks.

In terms of vulnerabilities, this month we see 56 vulnerable systems out of 125 scanned with 298 vulnerabilities with three high, 40 medium and the remaining low. This is almost the same as prior month. It should be noted that the three critical vulnerabilities remain from prior month. The categories of vulnerable systems for this month are:

> Web Servers vulnerabilities are the most prevalent vulnerability category with **114** detected vulnerabilities followed by Encryption and Authentication with **102** , preliminary analysis with **68** , Server Side Scripts with **10**, Mail Servers with **2**, Simple Network Services with **2** for the report period.

We assume that systems 170.75.33.133 and 170.75.33.95 are web servers, since these have the 3 critical vulnerabilities and are catalogued as such by our monitoring. This indicates a more serious issue and should be addressed with high priority.

On the Operations side, the systems were available 100% of the time with good response time

(Bridgeton at 15.62 msec and Elmer at 11.05 msec) and no packet loss.
The categories for vulnerabilites this month is: Encryption and Authentication vulnerabilities are the most prevalent vulnerability category with **36** detected vulnerabilities followed by Web servers with **18** , preliminary analysis with **17** , SSH servers with **2** for the report period.

The systems have operated properly with **100%** up time and good performance. The round-trip delay to GLESEC IDC has remained **15.62 ms** and 11.05 ms for Bridgeton and Elmer respectively with no packet loss

## Risk Value

To provide a way to quantify the risk of a Company, GLESEC introduces a definition for a metric value to capture the exposure risk that allow to evaluate the objective vulnerabilities and also the record of change over time. This procedure to qualify can be used to evaluate the ROI in the security measures we have implemented.

It is important to mention that this metric considers a median value for the vulnerabilities classified as ¨high¨, ¨medium¨ and ¨low¨, given them a value of 100% 50% and 10% to each, so the factor of the total number of system that are vulnerable.

This takes into consideration all of the vulnerabilities, but is important to point out that this values (100, 50 and 10) are arbitrary chosen by us, so this measure can in time change as we understand more of the risk involved. We can use this metric to evaluate the progress in time and to compare one over the other using a common amount set.

| Total IP's Scanned | | | IP's Vulnerable |
|---|---|---|---|
| 125 | | | 56 |
| Risk Distribution | | | |
| High | Medium | Low | Total |
| 3 | 40 | 255 | 298 |
| **Risk Value** | | 0.073 | |
| **Vulnerabilities Weighted Sum** | | | 0.163 |

According to the metrics:

RV= 0.073

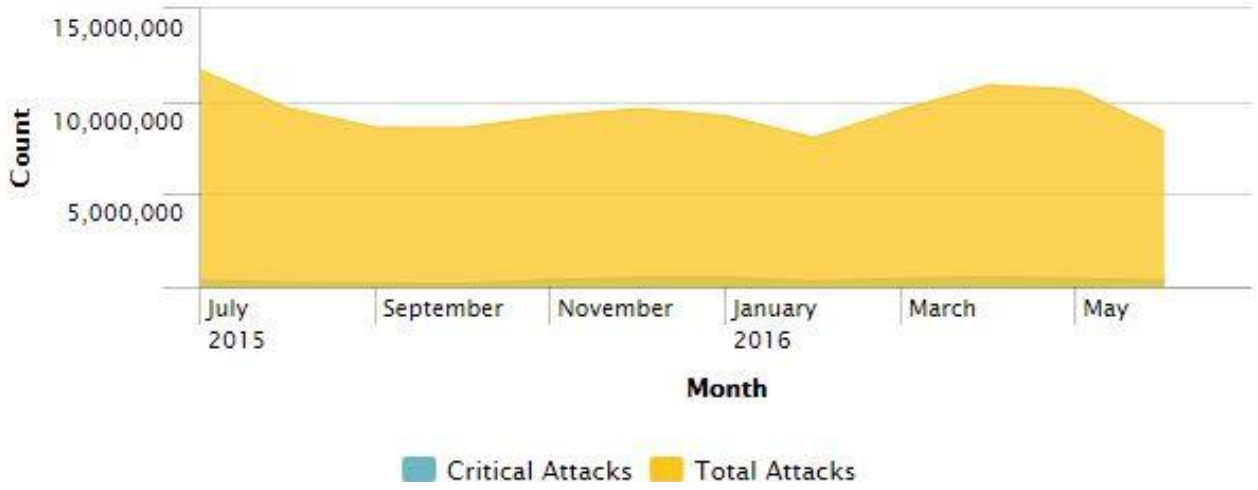
The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

## Attack Summary

Based on the information gathered from the DefensePro during this period **8,393,071** attacks on INSPIRA HEALTH NETWORK, **311,812** of which were considered critical were all stopped by the Radware devices.

INSPIRA HEALTH NETWORK receives an average of **10,449,536** total attacks and **322,144**critical attacks on a monthly basis which equates to an average of **412,045** total daily attacks and **14,047** critical daily attacks. As the graph illustrates total attack levels in relation to the previous report period totalled **10,624,005** total attacks and critical attacks in compared with a last period's total of **237,033**.

This statistical graph provides the count of critical and total attacks blocked per month calculated on a rolling 12 month period (Last 12 months)

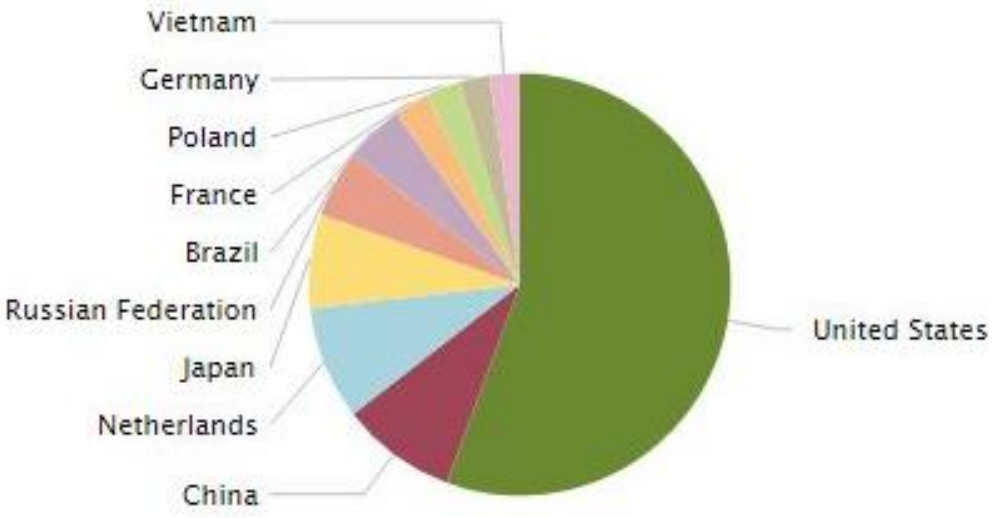



Comparison of previous month with current month.

| Description | May | June |
|---|---|---|
| **Total Attack** | **10,624,005** | **8,393,071** |
| **Critical Attacks** | **237,033** | **311,812** |
| **Monthly attack average** | **12,965,744** | **10,449,563** |
| **Daily Attack Average** | **437,033** | **322,144** |
| **Monthly Critical attack average** | **347,710** | **412,045** |
| **Daily Critical Attack Average** | **12,568** | **14,047** |

## Geography

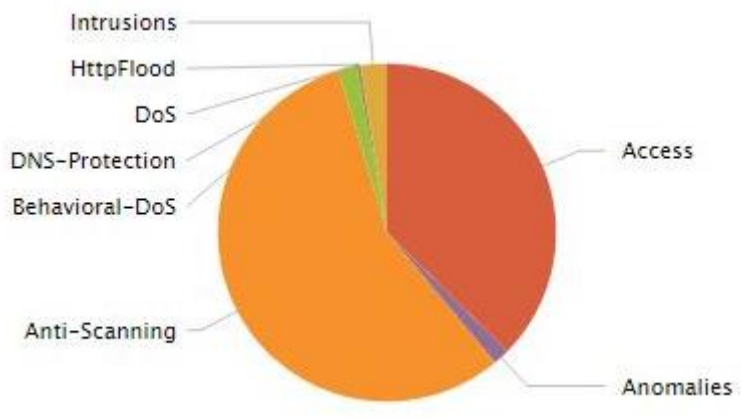
The vast majority of attacks on **INSPIRA HEALTH NETWORK** originated geographically from the following Top 10 countries: **USA, China, Netherlands, Japan, Russia, Brazil, France, Poland, Germany, Vietnam** listed in order of frequency. The attacks that we observed are happening to companies all around the world. Geographic borders offer little or no protection against cyber-attacks, in fact just the opposite is true offering more opportunity for anyone to carry out an attack.




*Please view the Maps, and **Graph: Top 10 Attacking Countries Blocked**, **Graph: Top 10 Attacking Countries Blocked by Attack Type**, **Graph: Top 10 Attacking Countries Blocked by Protocol** available in the Security Intelligence section of the report.

## Category Distribution

Category distribution for this report period is illustrated and detailed below.




### Scanning accounted for 24.0 % of attacks during this report period

Network-wide Anti-Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modelling, commonplace after the information gathering phase of a targeted or planned attack.

### Intrusions accounted for 6.5 % of attacks during this report period

These include vulnerability-based threats such as: Worms and Botnets; Trojan horses and the creation of backdoors; Vendor-specific exploitation vulnerabilities in products e.g., Microsoft, Oracle; Exploitation of vulnerabilities in applications such as web, mail, VoIP, DNS, SQL; Spyware, Phishing, anonymizes.

### Packet Anomalies accounted for 1.3 % of attacks during this report period

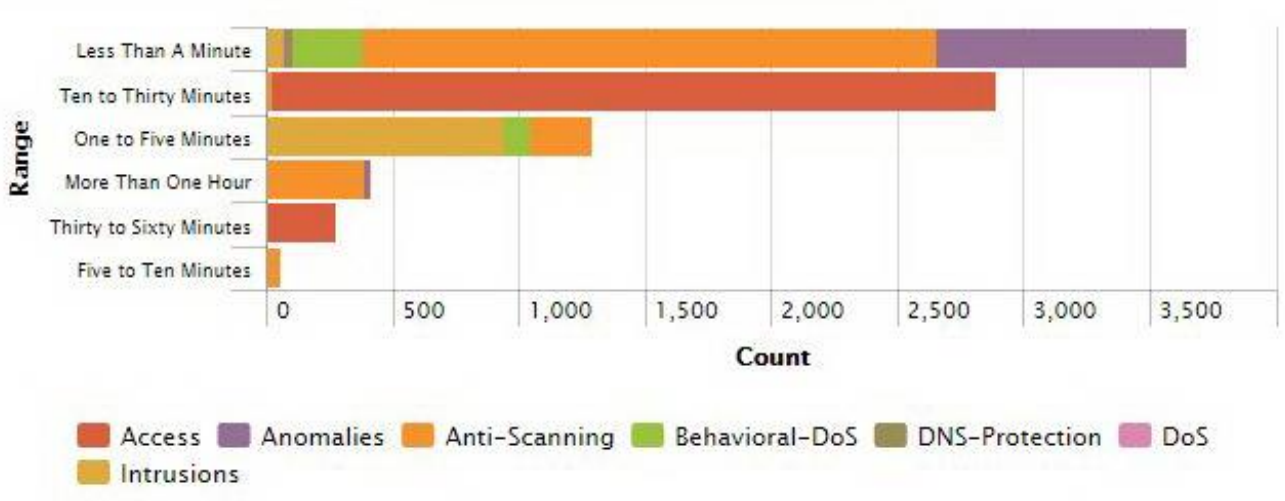
This anomalous traffic is usually caused by attacks or evasion tactics directed at the network devices such as firewalls in order to bypass their functions which if allowed to pass could permit scanning of the internal network or overloading the central processing unit of the device rendering it unusable and effectively causing a network bottleneck or DoS condition. They are also used as a method to collapse the underlying network infrastructure with packet crafting tools used by threat agents to interrupt services or distract security teams with volumetric attacks while more targeted attacks are directed at important assets to allow for data exfiltration. Packet Anomalies can also be caused by applications that do not adhere to RFC standards.

### Access accounted for 64.6 % of attacks during this report period

Access category relates directly to blacklists configured by GLESEC on the DefensePro for known threat sources.

## Duration

Attack duration for specific categories for this report period is illustrated below.




## Bandwidth

Access protection dropped **163.69 Gbps**, Anti-Scanning protection dropped **60.69 Gbps**, Dos Protection Dropped **0.04 Gbps,** Intrusion protection dropped **16.38 Gbps** of total traffic, Behavioral-DoS dropped **5.73 Gbps**, **4.39 Gbps** dropped by Packet Anomaly protection rules, DNS Protection dropped a total of **2.37 Gbps** of traffic, for a total of **253.29 Gbps** of alicious traffic was discarded this period.

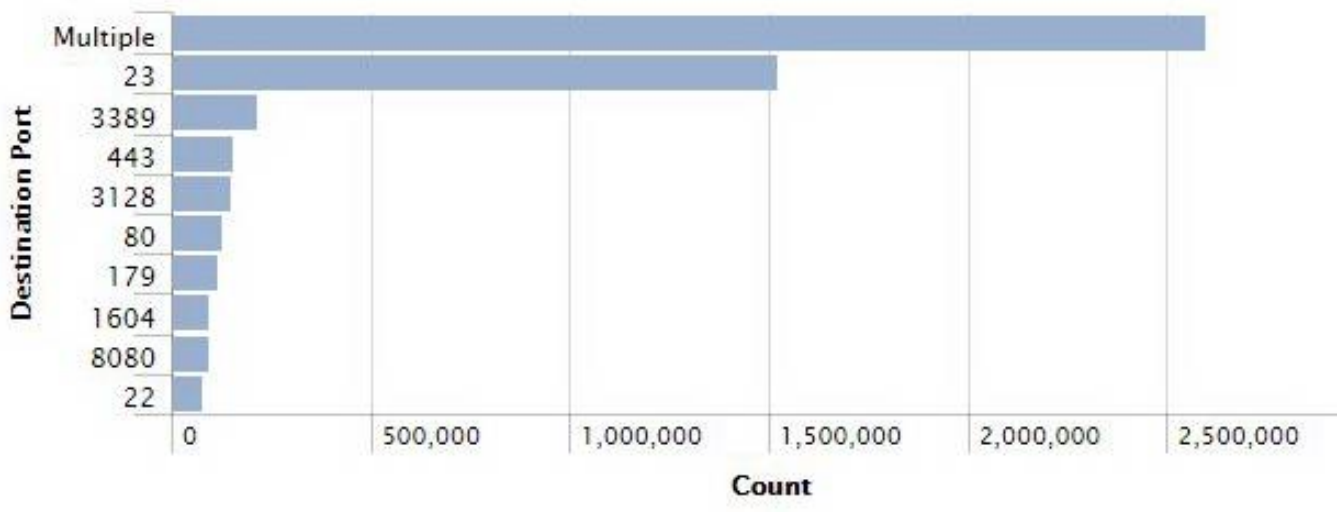
| Category | Gbps | Mbps |
|---|---|---|
| Access | 163.69 | 167614.06 |
| Anti-Scanning | 60.69 | 62142.35 |
| Intrusions | 16.38 | 16777.83 |
| Behavioral-DoS | 5.73 | 5871.74 |
| Anomalies | 4.39 | 4496.48 |
| DNS-Protection | 2.37 | 2423.68 |
| DoS | 0.04 | 40.96 |
| Total Bandwidth in Gbps/Mbps | 253.29 | 259367.10 |

*Please view the **Bandwidth Information**, and **Graph: Bandwidth by Blocked Threat Category by Hour of Day** and **Graph: Top Attacks Blocked by Bandwidth** and **Graph: Attack Categories Blocked by Bandwidth** available in the Security Intelligence section of the report.

## Port Activity

The advanced intrusion detection and prevention capabilities offered by the DefensePro IPS NBA, DoS and Reputation Service provides maximum protection for network elements, hosts and applications. It is composed of different application-level protection features to prevent intrusion attempts such as worms, Trojan horses and single-bullet attacks, facilitating complete and high-speed cleansing of all malicious intrusions.

The DefensePro assisted in preventing attacks directed at network and server level which were directed at well-known port numbers: **80** (http), **1433** (ms-sql), **8080** (http-alt), **4500** (ipsec-nat-t), **443** (https), **5060** (sip), **23** (telnet), **22** (ssh), **3306** (mysql) in order of frequency for this report period.

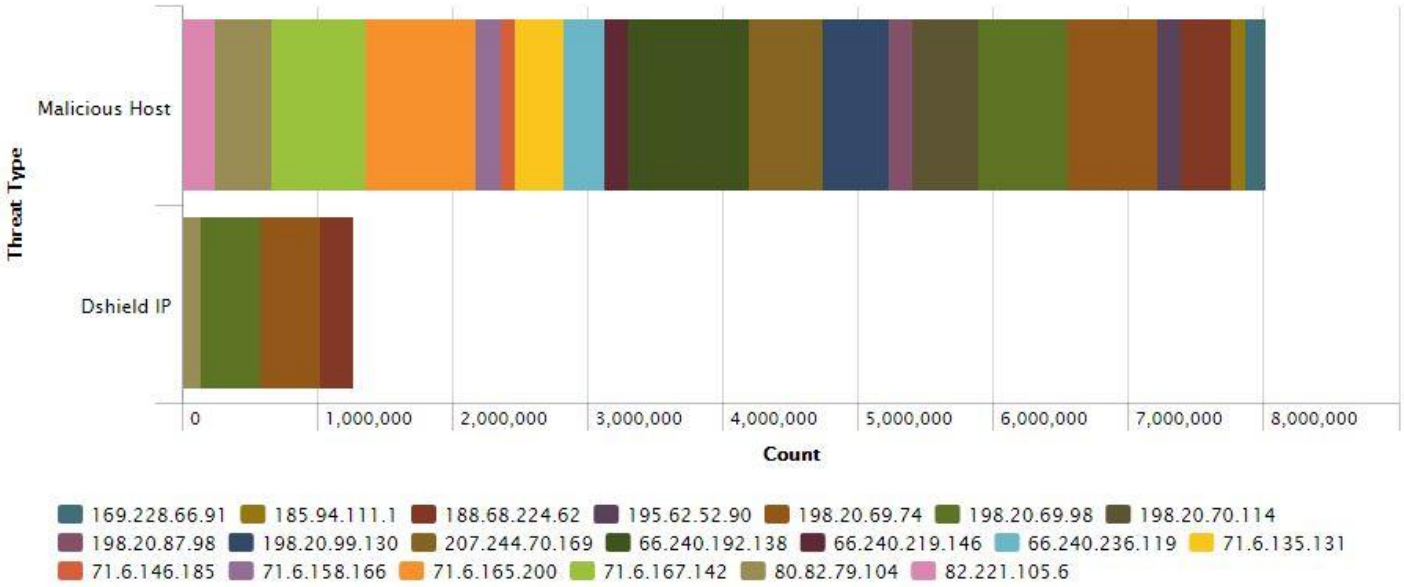



Port number information utilized is based on IANA Service Name and Transport Protocol Port Number Registry and additional outside sources are used to illustrate the relationship to commonly exploited attacks vectors.

*Please view the **Port Information**, and **Graph: Attacks Blocked by Destination Port** and **Graph: Top Probed Applications Blocked** available in the Security Intelligence section of the report.

## Known Threat Sources by Threat Type

**4,425,470** attacks on INSPIRA HEALTH NETWORK are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro attack logs and outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.



## Vulnerability Summary

The following network ranges for INSPIRA HEALTH NETWORKwas scanned for vulnerabilities.
**170.75.32.0/20 170.75.32.48.0/20**
A total of **125** hosts were scanned **56** of which were found to be vulnerable.
Vulnerabilities were detected for the following host IPs:

| Vulnerable Hosts | High | Medium | Low | Total |
|---|---|---|---|---|
| 170.75.48.3 | 0 | 0 | 1 | 1 |
| 170.75.48.2 | 0 | 0 | 1 | 1 |
| 170.75.48.1 | 0 | 0 | 1 | 1 |
| 170.75.33.217 | 0 | 1 | 2 | 3 |
| 170.75.33.216 | 0 | 1 | 2 | 3 |
| 170.75.33.190 | 0 | 0 | 6 | 6 |
| 170.75.33.163 | 0 | 1 | 7 | 8 |
| 170.75.33.162 | 0 | 1 | 9 | 10 |
| 170.75.33.142 | 0 | 1 | 8 | 9 |
| 170.75.33.141 | 0 | 1 | 7 | 8 |
| 170.75.33.140 | 0 | 1 | 6 | 7 |
| 170.75.33.138 | 0 | 1 | 3 | 4 |
| 170.75.33.137 | 0 | 1 | 2 | 3 |
| 170.75.33.135 | 0 | 1 | 2 | 3 |
| 170.75.33.134 | 0 | 1 | 2 | 3 |
| 170.75.33.133 | 0 | 0 | 3 | 3 |
| 170.75.33.132 | 0 | 1 | 7 | 8 |
| 170.75.33.131 | 0 | 0 | 7 | 7 |
| 170.75.33.130 | 0 | 0 | 2 | 2 |
| 170.75.33.129 | 0 | 1 | 8 | 9 |

| | | | | |
|---|---|---|---|---|
| 170.75.33.128 | 0 | 0 | 4 | 4 |
| 170.75.33.127 | 0 | 1 | 7 | 8 |
| 170.75.33.125 | 0 | 1 | 8 | 9 |
| 170.75.33.124 | 0 | 0 | 8 | 8 |
| 170.75.33.123 | 0 | 3 | 5 | 8 |
| 170.75.33.122 | 0 | 1 | 7 | 8 |
| 170.75.33.121 | 0 | 1 | 6 | 7 |
| 170.75.33.120 | 0 | 0 | 2 | 2 |
| 170.75.33.119 | 0 | 1 | 9 | 10 |
| 170.75.33.118 | 0 | 0 | 3 | 3 |
| 170.75.33.117 | 0 | 1 | 6 | 7 |
| 170.75.33.116 | 0 | 1 | 6 | 7 |
| 170.75.33.115 | 0 | 1 | 6 | 7 |
| 170.75.33.113 | 1 | 0 | 6 | 7 |
| 170.75.33.112 | 0 | 0 | 4 | 4 |
| 170.75.33.111 | 0 | 1 | 7 | 8 |
| 170.75.33.110 | 0 | 3 | 10 | 13 |
| 170.75.33.109 | 0 | 1 | 7 | 8 |
| 170.75.33.108 | 0 | 2 | 7 | 9 |
| 170.75.33.106 | 0 | 0 | 3 | 3 |

| Vulnerable Hosts | High | Medium | Low | Total |
|---|---|---|---|---|
| 170.75.33.105 | 0 | 0 | 3 | 3 |
| 170.75.33.104 | 0 | 0 | 3 | 3 |
| 170.75.33.98 | 0 | 0 | 2 | 2 |
| 170.75.33.97 | 0 | 0 | 4 | 4 |
| 170.75.33.95 | 2 | 0 | 2 | 4 |
| 170.75.33.58 | 0 | 1 | 4 | 5 |
| 170.75.33.55 | 0 | 2 | 4 | 6 |
| 170.75.33.53 | 0 | 1 | 2 | 3 |
| 170.75.33.51 | 0 | 3 | 5 | 8 |
| 170.75.33.35 | 0 | 0 | 4 | 4 |
| 170.75.33.4 | 0 | 1 | 6 | 7 |
| 170.75.32.15 | 0 | 1 | 5 | 6 |
| 170.75.32.10 | 0 | 0 | 1 | 1 |
| 170.75.32.3 | 0 | 0 | 1 | 1 |
| 170.75.32.2 | 0 | 0 | 1 | 1 |
| 170.75.32.1 | 0 | 0 | 1 | 1 |

**Vulnerability –Current Month and Previous Month**

A comparison of persistent vulnerabilities of the current month and previous month.

| | ip | Previous_Month | Current_Month |
|---|---|---|---|
| 1 | 170.75.32.1 | 1 | 1 |
| 2 | 170.75.32.10 | 1 | 1 |
| 3 | 170.75.32.15 | 5 | 6 |
| 4 | 170.75.32.2 | 1 | 1 |
| 5 | 170.75.32.3 | 1 | 1 |
| 6 | 170.75.33.104 | 3 | 3 |
| 7 | 170.75.33.105 | 3 | 3 |
| 8 | 170.75.33.106 | 3 | 3 |
| 9 | 170.75.33.108 | 8 | 9 |
| 10 | 170.75.33.109 | 8 | 8 |
| 11 | 170.75.33.110 | 12 | 13 |
| 12 | 170.75.33.111 | 9 | 8 |
| 13 | 170.75.33.112 | 8 | 4 |
| 14 | 170.75.33.113 | 10 | 7 |
| 15 | 170.75.33.115 | 6 | 7 |
| 16 | 170.75.33.116 | 7 | 7 |
| 17 | 170.75.33.117 | 7 | 7 |
| 18 | 170.75.33.118 | 9 | 3 |
| 19 | 170.75.33.119 | 10 | 10 |
| 20 | 170.75.33.120 | 2 | 2 |
| 21 | 170.75.33.121 | 2 | 7 |
| 22 | 170.75.33.122 | 8 | 8 |
| 23 | 170.75.33.123 | 6 | 8 |
| 24 | 170.75.33.124 | 9 | 8 |
| 25 | 170.75.33.125 | 9 | 9 |
| 26 | 170.75.33.127 | 8 | 8 |
| 27 | 170.75.33.128 | 10 | 4 |
| 28 | 170.75.33.129 | 9 | 9 |
| 29 | 170.75.33.130 | 2 | 2 |
| 30 | 170.75.33.131 | 9 | 7 |

| | ip | Previous_Month | Current_Month |
|---|---|---|---|
| 31 | 170.75.33.132 | 8 | 8 |
| 32 | 170.75.33.133 | 7 | 3 |
| 33 | 170.75.33.134 | 3 | 3 |
| 34 | 170.75.33.135 | 3 | 3 |
| 35 | 170.75.33.137 | 3 | 3 |
| 36 | 170.75.33.138 | 3 | 4 |
| 37 | 170.75.33.140 | 2 | 7 |
| 38 | 170.75.33.141 | 8 | 8 |
| 39 | 170.75.33.142 | 10 | 9 |
| 40 | 170.75.33.162 | 9 | 10 |
| 41 | 170.75.33.163 | 8 | 8 |
| 42 | 170.75.33.190 | 3 | 6 |
| 43 | 170.75.33.216 | 3 | 3 |
| 44 | 170.75.33.217 | 3 | 3 |
| 45 | 170.75.33.35 | 7 | 4 |
| 46 | 170.75.33.4 | 7 | 7 |
| 47 | 170.75.33.51 | 6 | 8 |
| 48 | 170.75.33.53 | 3 | 3 |
| 49 | 170.75.33.55 | 6 | 6 |
| 50 | 170.75.33.58 | 5 | 5 |
| 51 | 170.75.33.95 | 3 | 4 |
| 52 | 170.75.33.97 | 7 | 4 |
| 53 | 170.75.33.98 | 2 | 2 |
| 54 | 170.75.48.1 | 1 | 1 |
| 55 | 170.75.48.2 | 1 | 1 |
| 56 | 170.75.48.3 | 1 | 1 |

Please view **Recommendations** for more details.

## Risk Distribution

Category distribution for this report period is illustrated and detailed below.

Based on the information gathered from the GLESEC Automated Vulnerability Detection System (AVDS) a total of **298 Vulnerabilities** were found which consisted of **3 High Risk Vulnerabilities** during this period, **40 Medium Risk Vulnerabilities** and **255 Low Risk Vulnerabilities.**

| Scan Name | High | Medium | Low | Total |
|---|---|---|---|---|
| Inspira_Health_Network | 3 | 40 | 255 | 298 |

## High risk vulnerabilities accounted for 1.01 % of the discoveries during this report period

High are defined as being in one or more of the following categories: Backdoors, full Read/Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords).

## Medium risk vulnerabilities accounted for 13.42 % of the discoveries during this report period

Medium describes vulnerabilities that either expose sensitive data, directory browsing and traversal, disclosure of security controls, facilitate unauthorized use of services or denial of service to an attacker.

## Low risk vulnerabilities accounted for 85.57% of the discoveries during this report period

Low describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social-engineering or similar attacks.

## Vulnerability Categories

Most frequent type of vulnerabilities.

| | | | | | |
|---|---|---|---|---|---|
| 1 | Preliminary Analysis | 9 | Firewalls | 17 | Network Devices |
| 2 | SMB/NetBIOS | 10 | SSH Servers | 18 | Malformed Packets |
| 3 | Simple Network Services | 11 | Mail Servers | 19 | Proxy Servers |
| 4 | Policy Checks | 12 | SQL Servers | 20 | Wireless AP |
| 5 | Web Servers | 13 | FTP Servers | 21 | Webmail Servers |
| 6 | RPC Services | 14 | Server Side Scripts | 22 | NFS Services |
| 7 | Backdoors | 15 | SNMP Services | 23 | Printers |
| 8 | Encryption and Authentication | 16 | DNS Servers | | |

The list below indicate your vulnerability most frequent:

Web Servers vulnerabilities are the most prevalent vulnerability category with **114** detected vulnerabilities followed by Encryption and Authentication with **102** , preliminary analysis with **68** , Server Side Scripts with **10**, Mail Servers with **2**, Simple Network Services with **2** for the report period.

| Category | High | Medium | Low | Total |
|---|---|---|---|---|
| Web servers | 3 | 1 | 110 | 114 |
| Encryption and Authentication | 0 | 29 | 73 | 102 |
| Preliminary Analysis | 0 | 0 | 68 | 68 |
| Server Side Scripts | 0 | 10 | 0 | 10 |
| Mail servers | 0 | 0 | 2 | 2 |
| Simple Network services | 0 | 0 | 2 | 2 |

## Encryption and Authentication vulnerabilities accounted for 34.23 % of the discoveries during this report period

Authentication and encryption are two intertwined technologies that help to insure that your data remains secure. Authentication is the process of insuring that both ends of the connection are in fact who they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well.

While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications.

## Web Server vulnerabilities accounted for 38.25 % of the discoveries during this report period

Various high-profile hacking attacks have proven that web security remains the most critical issue to any business that conducts its operations online. Web servers are one of the most targeted public faces of an organization, because of the sensitive data they usually host. Securing a web server is as important as securing the website or web application itself and the network around it. If you have a secure web application and an insecure web server, or vice versa, it still puts your business at a huge risk. Your company's security is as strong as its weakest point.

## Preliminary Analysis vulnerabilities accounted for 22.82 % of the discoveries during this report period

Preliminary Analysis vulnerabilities are primarily information or service disclosures that can be gathered during footprinting/enumeration. Information disclosure is the unwanted exposure of private data. For example, a user views the contents of a table or file he or she is not authorized to open, or monitors data passed in plaintext over a network. Some examples of information disclosure vulnerabilities include the use of hidden form fields, comments embedded in Web pages that contain database connection strings and connection details, and weak exception handling that can lead to internal system level details being revealed to the client. Any of this information can be very useful to the attacker/threat agent.

## Simple Network Service vulnerabilities accounted for 0.67 % of the discoveries during this report period

Simple Network vulnerabilities affect protocols like NTP, ICMP and common network applications like SharePoint among others. This is not meant to be a comprehensive list.

## Mail Server vulnerabilities accounted for 0.67 % of the discoveries during this report period.

A mail server is the computerized equivalent of your friendly neighborhood mailman. Spammers sometimes send a flood of traffic that overwhelms an email server. The result is sluggish email delivery, delaying legitimate messages from reaching their intended recipients on your network.

## Server Side script vulnerabilities accounted for 3.36 % of the discoveries during this report period.

Is a technique used in website design which involves embedding scripts in an HTML source code which results in a user's (client's) request to the server website being handled by a script running on the server-side before the server responds to the client's request.

## *5. Recommendations*

**GLESEC recommends for INSPIRA HEALTH NETWORK to address the following vulnerabilities assigned a High Risk by the GLESEC AVDS.**

### Systems Affected

170.75.33.114

### Description

Apache Version Prior to 2.0.51

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

### Possible Solution

Limit the number of ranges allowed in the Range and Request-Range request headers, or disallow the use of Range and Request-Range request headers altogether. For more information, refer to Apache's advisory for CVE-2011-3192.

### Systems Affected

170.75.33.114

### Description

Apache HTTP Server 403 Error Page UTF-7 Encoded XSS

Cross-site scripting (XSS) vulnerability in Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.

### Possible Solution

Upgrade to Apache version 2.2.8, Apache version 2.0.63, Apache version 1.3.41 or newer.

### Systems Affected

170.75.33.114

### Description

Apache Running Version Prior to 2.0.63

Multiple vulnerabilities have been discovered in Apache:

* The date handling code in modules/proxy/proxy_util.c (mod_proxy) in Apache 2.3.0, when using a threaded MPM, allows remote origin servers to cause a denial of service (caching forward proxy process crash) via crafted date headers that trigger a buffer over-read.

* Cross-site scripting (XSS) vulnerability in the (1) mod_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod_imagemap module in

the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
* Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
* mod_proxy_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.== Apache Running Version Prior to 2.0 .59 ==
Off-by-one error in the ldap scheme handling in the Rewrite module (mod_rewrite) in Apache 1.3 from 1.3.28, 2.0.46 and other versions before 2.0.59, and 2.2, when RewriteEngine is enabled, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted URLs that are not properly handled using certain rewrite rules.== Apache Running Version Prior to 2.0.55 ==
Two security vulnerabilities have been discovered in Apache:
* The byte-range filter in Apache 2.0 before 2.0.54 allows remote attackers to cause a denial of service (memory consumption) via an HTTP header with a large Range field.
* Memory leak in the worker MPM (worker.c) for Apache 2, in certain circumstances, allows remote attackers to cause a denial of service (memory consumption) via aborted connections, which prevents the memory for the transaction pool from being reused for other connections

## Possible Solution

Upgrade to Apache version 2.0.63 or newer.

**GLESEC recommends for INSPIRA HEALTH NETWORK to address the following vulnerabilities assigned a Low Risk by the GLESEC AVDS.**

## Systems Affected

170.75.33.95, 170.75.33.102, 170.75.33.118

## Description

Microsoft Windows HTTP.sys Code Execution VulnerabilityThe remote host answers to an ICMP timestamp request. This allows an attacker to know the time and date on your host.

## Impact

HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."

## Possible Solution

See solution provided at: https://technet.microsoft.com/library/security/ms15-034

## Systems Affected

170.75.33.114

## Description

Apache Running Version Prior to 2.0.65

Multiple vulnerabilities have been found in Apache:

* The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

* The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of RewriteRule and ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

* Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

* scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

* protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a long or malformed header in conjunction with crafted web script.

* mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

## Possible Solution

Upgrade to Apache version 2.0.65 or newer.

**GLESEC recommends for INSPIRA HEALTH NETWORK to address the following vulnerabilities assigned a Medium Risk by the GLESEC AVDS.**

## Systems Affected

170.75.32.15

## Description

Cisco ASA Software Information Disclosure

The SSL VPN implementation in Cisco Adaptive Security Appliance (ASA) Software allows remote attackers to obtain potentially sensitive software-version information by reading the verbose response data that is provided for a request to an unspecified URL, aka Bug ID CSCuq65542.

## Impact

Successful exploitation will allow attacker to obtain sensitive information that may aid in further attacks.

## Possible Solution

See solution provided at:
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3398

## Systems Affected

170.75.33.58, 170.75.33.97, 170.75.33.101, 170.75.33.102, 170.75.33.107, 170.75.33.108, 170.75.33.109, 170.75.33.110, 170.75.33.111, 170.75.33.112, 170.75.33.113, 170.75.33.114, 170.75.33.115, 170.75.33.116, 170.75.33.117, 170.75.33.118, 170.75.33.119, 170.75.33.122, 170.75.33.123, 170.75.33.124, 170.75.33.125, 170.75.33.127, 170.75.33.128, 170.75.33.129, 170.75.33.131, 170.75.33.132, 170.75.33.133, 170.75.33.134, 170.75.33.135, 170.75.33.137, 170.75.33.138, 170.75.33.140, 170.75.33.141, 170.75.33.216, 170.75.33.217

## Description

Deprecated SSL Protocol Usage

The remote service accepts connections encrypted using SSLv2 and/or SSLv3, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

## Possible Solution

Consult the application's documentation to disable SSL 2.0 and SSL 3.0, and use TLS 1.0 or newer

## Systems Affected

170.75.33.104, 170.75.33.105, 170.75.33.106, 170.75.33.113

## Description

Microsoft IIS Tilde Character Information Disclosure Vulnerability

The remote host has Microsoft IIS installed and prone to information disclosure vulnerability. Microsoft IIS fails to validate a specially crafted GET request having a '~' tilde character, which allows to disclose all short-names of folders and files having 4 letters extensions.

## Impact

Successful exploitation will let the remote attackers to obtain sensitive information that could aid in further attacks.

## Systems Affected

170.75.33.110

## Description

Default Web Server Configuration

The web server's default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, a web server is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing

hackers with a convenient target that is not likely to trip any alarms.

## Possible Solution

Change the default page, or stop and disable the web server completely.
If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network.

## Systems Affected

170.75.33.110

## Description

Tomcat Documentation XSS Vulnerabilities

The remote web server includes an example JSP application that fails to sanitize user-supplied input before using it to generate dynamic content in an error page.

## Impact

An unauthenticated remote attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site.

## Possible Solution

Un-deploy the Tomcat documentation web application.

## Systems Affected

170.75.33.110

## Description

Tomcat snoop.jsp Cross-Site Scripting Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in certain JSP files in the examples web application in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote attackers to inject arbitrary web script or HTML via the portion of the URI after the ';' character, as demonstrated by a URI containing a "snp/snoop.jsp;" sequence.

## Systems Affected

170.75.33.110

## Description

Apache Tomcat Implicit Objects XSS

vulnerability in implicit-objects.jsp in Apache Tomcat 5.0.0 through 5.0.30 and 5.5.0 allows remote attackers to inject arbitrary web script or HTML via certain header values.

## Possible Solution

Remove the Apache Tomcat example web applications, or upgrade to Apache Tomcat version 5.0.SVN, Apache Tomcat version 5.5.18 or newer.

## Systems Affected

170.75.32.15

## Description

IPSEC IKE Detection

The remote host seems to be enabled to do Internet Key Exchange (IKE). This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.

## Possible Solution

You should ensure that:
1) The VPN is authorized for your Companies computing environment
2) The VPN utilizes strong encryption
3) The VPN utilizes strong authentication

## Systems Affected

170.75.32.15, 170.75.32.58, 170.75.32.97, 170.75.32.101, 170.75.32.102, 170.75.32.107, 170.75.32.108, 170.75.32.109, 170.75.32.110, 170.75.32.111, 170.75.32.112, 170.75.32.113, 170.75.32.114, 170.75.32.115, 170.75.32.116, 170.75.32.117, 170.75.32.118, 170.75.32.119, 170.75.32.122, 170.75.32.123, 170.75.32.124, 170.75.32.125, 170.75.32.127, 170.75.32.128, 170.75.32.129, 170.75.32.132, 170.75.32.133, 170.75.32.134, 170.75.32.135, 170.75.32.137, 170.75.32.138, 170.75.32.140, 170.75.32.190, 170.75.32.216, 170.75.32.217

## Description

SSL Verification Test

This test connects to a SSL server, and checks its certificate and the available ciphers. Weak (export version) ciphers are reported as problematic.

## Possible Solution

Usage of weak ciphers should be avoided.

## Systems Affected

170.75.32.15, 170.75.32.58, 170.75.32.97, 170.75.32.101, 170.75.32.102, 170.75.32.107, 170.75.32.108, 170.75.32.109, 170.75.32.110, 170.75.32.111, 170.75.32.112, 170.75.32.113, 170.75.32.114, 170.75.32.115, 170.75.32.116, 170.75.32.117, 170.75.32.118, 170.75.32.119, 170.75.32.122, 170.75.32.123, 170.75.32.124, 170.75.32.125, 170.75.32.127, 170.75.32.128, 170.75.32.129, 170.75.32.131, 170.75.32.132, 170.75.32.133, 170.75.32.134, 170.75.32.135, 170.75.32.137, 170.75.32.138, 170.75.32.140, 170.75.32.190, 170.75.32.216, 170.75.32.217, 170.75.33.141

## Description

Supported SSL Ciphers Suites

This test connects to a SSL server, and checks its certificate and the available ciphers. Weak (export version) ciphers are reported as problematic.

## Possible Solution

http://www.openssl.org/docs/apps/ciphers.html

## Systems Affected

170.75.32.15, 170.75.33.58, 170.75.33.95, 170.75.33.97, 170.75.33.98, 170.75.33.101, 170.75.33.102, 170.75.33.104, 170.75.33.105, 170.75.33.106, 170.75.33.107, 170.75.33.108, 170.75.33.109, 170.75.33.110, 170.75.33.111, 170.75.33.112, 170.75.33.113, 170.75.33.114, 170.75.33.115, 170.75.33.117, 170.75.33.119, 170.75.33.120, 170.75.33.121, 170.75.33.122, 170.75.33.123, 170.75.33.124, 170.75.33.125, 170.75.33.126, 170.75.33.127, 170.75.33.128, 170.75.33.129, 170.75.33.132, 170.75.33.133, 170.75.33.140, 170.75.33.190, 170.75.33.141

## Description

HTTP Packet Inspection

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.

## Systems Affected

170.75.33.58, 170.75.33.95, 170.75.33.97, 170.75.33.98, 170.75.33.101, 170.75.33.102, 170.75.33.104, 170.75.33.105, 170.75.33.106, 170.75.33.107, 170.75.33.108, 170.75.33.109, 170.75.33.110, 170.75.33.111, 170.75.33.112, 170.75.33.113, 170.75.33.114, 170.75.33.115, 170.75.33.116, 170.75.33.117, 170.75.33.118, 170.75.33.119, 170.75.33.120, 170.75.33.121, 170.75.33.122, 170.75.33.123, 170.75.33.124, 170.75.33.125, 170.75.33.126, 170.75.33.127, 170.75.33.128, 170.75.33.129, 170.75.33.130, 170.75.33.131, 170.75.33.132, 170.75.33.133, 170.75.33.140, 170.75.33.190, 170.75.33.141

## Description

Identify Unknown Services via GET Requests

This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

## Systems Affected

170.75.32.15

## Description

Cisco ASA SSL VPN Detection

The remote host is a Cisco Adaptive Security Appliance (ASA) running an SSL VPN server

## Possible Solution

Make sure the use of this device is authorized by your company policy.

## Systems Affected

170.75.33.114

## Description

Apache Version Prior to 2.0.48

The remote host appears to be running a version of Apache 2.x which is older than 2.0.48. This version is vulnerable to a bug which may allow a rogue CGI to disable the httpd service by issuing over 4K of data to stderr.

To exploit this flaw, an attacker would need the ability to upload a rogue CGI script to this server and to have it executed by the Apache daemon (httpd).

## Possible Solution

Upgrade to Apache version 2.0.48 or newer.

## Systems Affected

170.75.33.114

## Description

Apache Connection Blocking DoS

The remote web server appears to be running a version of Apache that is less that 2.0.49 or 1.3.31. These versions are vulnerable to a denial of service attack where a remote attacker can block new connections to the server by connecting to a listening socket on a rarely accessed port

## Possible Solution

Upgrade to Apache version 2.0.49, version 1.3.31 or newer.

## Systems Affected

170.75.33.114

## Description

Apache Input Header Folding and mod_ssl ssl_io_filter_cleanup DoS

There is denial of service in Apache HTTPd version 2.0.x by sending a specially crafted HTTP request. It is possible to consume arbitrary amount of memory. On 64 bit systems with more than 4GB virtual memory this may lead to heap based buffer overflow.
There is also a denial of service vulnerability in mod_ssl's ssl_io_filter_cleanup function. By sending a request to vulnerable server over SSL and closing the connection before the server can send a response, an attacker can cause a memory violation that crashes the server.

## Possible Solution

Upgrade to Apache version 2.0.50 or newer.

## Systems Affected

170.75.32.1, 170.75.32.2, 170.75.32.3, 170.75.48.1, 170.75.48.2, 170.75.48.3

## Description

ICMP Timestamp Request

The remote host answers to an ICMP timestamp request. This allows an attacker to know the time and date on your host.

## Impact

This may help attackers to defeat time based authentications schemes.

## Possible Solution

See solution provided at: http://www.beyondsecurity.com/faq/questions/54/how-can-i-mitigate-icmp-timestamp

## Systems Affected

170.75.33.97, 170.75.33.109, 170.75.33.117, 170.75.33.128, 170.75.33.141

## Description

Web Application Firewall Detection

By analysing error codes and messages returned from some web queries, we are able to determine that the remote web server is protected by a web application firewall.
Such protection may disrupt scan results. Countermeasures have been taken to make the scan as reliable as possible.

## Possible Solution

To get a more comprehensive set of scan results, either whitelist the scanner's IP address or scan from an unprotected location.

## Systems Affected

170.75.33.101, 170.75.33.105, 170.75.33.106, 170.75.33.107, 170.75.33.108, 170.75.33.110, 170.75.33.111, 170.75.33.112, 170.75.33.113, 170.75.33.114, 170.75.33.118, 170.75.33.119, 170.75.33.124, 170.75.33.125, 170.75.33.127, 170.75.33.129

## Description

IIS Content-Location HTTP Header

By default, in Internet Information Server (IIS), the Content-Location references the IP address of the server rather than the Fully Qualified Domain Name (FQDN) or Hostname.
This header may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.

## Impact

If this contains internal IP address information, attackers may gain critical information about the host.

## Possible Solution

See solution provided at: http://support.microsoft.com/kb/218180

## Systems Affected

170.75.33.101, 170.75.33.104, 170.75.33.105, 170.75.33.106, 170.75.33.107, 170.75.33.111, 170.75.33.114, 170.75.33.117, 170.75.33.119, 170.75.33.122, 170.75.33.123, 170.75.33.129

## Description

Directory Scanner

We found some common directories on the web server:

**170.75.33.101:**

```
The following directories were discovered:
/applets, /icons, /images, /includes, /scripts, /stylesheets, /tools
```

**170.75.33.104:**

```
The following directories were discovered:
/images, /include, /reports, /xml
```

**170.75.33.105:**

```
The following directories were discovered:
/images, /include, /reports, /xml
```

**170.75.33.106:**

```
The following directories were discovered:
/images, /include, /reports, /xml
```

**170.75.33.107:**

```
The following directories were discovered:
/css, /downloads, /help, /images, /includes, /reports
```

**170.75.33.111:**

```
The following directories were discovered:
/_notes, /documents, /upload
```

**170.75.33.114:**

```
The following directories were discovered:
/cgi-bin
```

**170.75.33.117:**

```
The following directories were discovered:
/en-US
```
**170.75.33.119:**
```
The following directories were discovered:
/Log, /exec, /log, /scripts, /utils
```
**170.75.33.122:**
```
The following directories were discovered:
/obj
```
**170.75.33.123:**
```
The following directories were discovered:
/Templates, /images, /java, /templates
```
**170.75.33.129:**
```
The following directories were discovered:
/archive
```
## Impact
This is usually not a security vulnerability, only an information gathering. Nevertheless, you should manually inspect these directories to ensure that they are in compliance with accepted security standards.
## Possible Solution
Check if those directories contain any sensitive information, if they do, prevent unauthorized access to them

## Systems Affected
170.75.33.102, 170.75.33.125
## Description
Microsoft IIS Default Page
The remote server appears to be an unconfigured IIS Server.

## Systems Affected
170.75.33.109
## Description
Non-compliant Strict Transport Security (STS)
The remote web server implements Strict Transport Security (STS). The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.
All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.
**170.75.33.109:**
```
The STS header line is:
Strict-Transport-Security: max-age=31536000
 includeSubDomains
```

## Systems Affected

170.75.33.109

## Description

Strict Transport Security (STS) Detection

The remote web server implements Strict Transport Security (STS). The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.
All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

**170.75.33.109:**

```
The STS header line is:
Strict-Transport-Security: max-age=31536000
 includeSubDomains
```

## Systems Affected

170.75.33.110

## Description

Apache Tomcat Servlet/JSP Container Default Files

WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server.

**170.75.33.110:**

```
The following directories are DAV enabled:
 - /webdav/
```

## Systems Affected

170.75.33.110

## Description

HTTP Server Backported Security Patches

Security patches may have been 'back ported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives.

## Systems Affected

170.75.33.114

## Description

Apache HTTP Server httpOnly Cookie Information Disclosure

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a long or malformed header in conjunction with crafted web script.

**170.75.33.114:**

```
We verified this by sending a request with a long Cookie header:
GET / HTTP/1.1

Host: lab.sjhs.com

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Accept-Language: en

Cookie: $Version="1"
 z9=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z8=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z7=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z6=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z5=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z4=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z3=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z2=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z1=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/
 z0=A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..A..$Path=/


Connection: Keep-Alive

Accept-Charset: iso-8859-1,*,utf-8

User-Agent: Mozilla/4.0 (compatible
 MSIE 6.0
 Windows NT 5.0)

Date: Sun, 27 Oct 2015 13:53:32 GMT

Pragma: no-cache

Which caused the Cookie header to be displayed in the default error page (the response
shown below has been truncated):
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: $Version=&quot
```

## Possible Solution

Upgrade to Apache version 2.2.22 or newer.

## Systems Affected

170.75.33.119

## Description

robot(s).txt Detection

Some webmasters use a file called robot(s).txt to supply information to search engines and other indexing tools. This file exists on your server: make sure it doesn't contain sensitive information.

**170.75.33.119:**

```
'robots.txt' contains the following:
User-agent: *

Disallow: /
```

## Impact

This file can be viewed by anyone, and it might contain sensitive information about the server. For example, specifying which directories shouldn't be indexed tells the attacker where the sensitive files are.

## Possible Solution

Make sure the file doesn't contain any sensitive information

## Systems Affected

170.75.33.122

## Description

Microsoft .NET Custom Errors Not Set

The remote ASP.NET web server is configured to show verbose error messages, which might lead into the disclosure of potential sensitive information about the remote installation (such as the path under which the remote web server resides) or about the remote ASP.NET applications.

**170.75.33.122:**

```
[HttpException]: The file '/aQnIczm7.ashx' does not exist.

   at System.Web.UI.Util.CheckVirtualFileExists(VirtualPath virtualPath)


   at
System.Web.Compilation.BuildManager.GetVPathBuildResultInternal(VirtualPath
 virtualPath, Boolean noBuild, Boolean allowCrossApp, Boolean
allowBuildInPrecompile)

   at
System.Web.Compilation.BuildManager.GetVPathBuildResultWithNoAssert(HttpContext
 context, VirtualPath virtualPath, Boolean noBuild, Boolean
allowCrossApp, Boolean allowBuildInPrecompile)

   at
System.Web.Compilation.BuildManager.GetVPathBuildResult(HttpContext
context, VirtualPath virtualPath, Boolean noBuild, Boolean
allowCrossApp, Boolean allowBuildInPrecompile)

   at
System.Web.UI.SimpleHandlerFactory.System.Web.IHttpHandlerFactory2.GetHandler(HttpContext
 context, String requestType, VirtualPath virtualPath, String
```

```
physicalPath)

   at
System.Web.HttpApplication.MapHttpHandler(HttpContext context, String
requestType, VirtualPath path, String pathTranslated, Boolean
useAppConfig)

   at
System.Web.HttpApplication.MapHandlerExecutionStep.System.Web.HttpApplication.IExecutionS
tep.Execute()
```

## Possible Solution

Configure your server such as the option 'customErrors mode' is set to 'On' instead of 'Off'.

## Systems Affected

170.75.33.122

## Description

Microsoft .NET Handlers Enumeration

It is possible to obtain the list of handlers the remote ASP.NET web server supports.

**170.75.33.122:**

```
 - .ashx
 - .aspx
 - .asmx
 - .rem
 - .soap
```

## Possible Solution

http://support.microsoft.com/kb/815145

## Systems Affected

170.75.33.124,170.75.33.128, 170.75.33.141

## Description

IIS Allows BASIC and/or NTLM Authentication

The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages.
That is, by requesting valid webpages with purposely invalid credentials, you can ascertain whether or not the authentication scheme is in use. This can be used for brute-force attacks against known UserIDs.

**170.75.33.124:**

```
- IIS Basic authentication is enabled
```

**170.75.33.128:**

```
- IIS Basic authentication is enabled
- IIS NTLM authentication is enabled
```

## Possible Solution

Follow this procedure:

1. Open Internet Information Service Manager
2. Choose the server
3. Choose master properties
4. Choose WWW Service
5. Choose Edit
6. Choose Directory Security
7. Under Anonymous access, choose edit
8. Deselect Integrated Windows Authentication

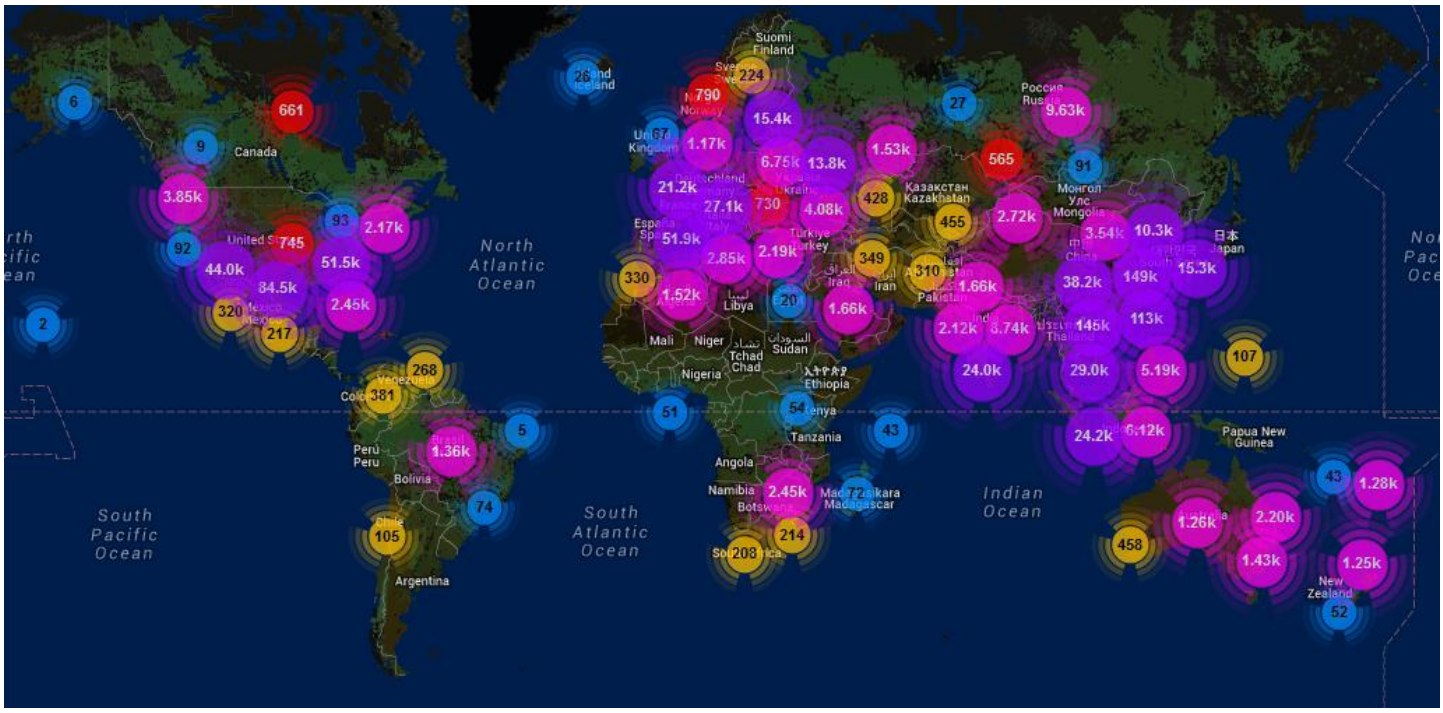
GLESEC recommends “Implementing the First Five Quick Wins” based on the Twenty Critical Security Controls for Effective Cyber Defense, Version 4.1 that were formulated as a joint effort from the NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities. These are readily available from GLESEC which has provided the following link: Top 20 Critical Security Controls
The Critical Controls represent the biggest bang for the buck to protect your organization against real security threats. Within Critical Controls 2-4 are five “quick wins.” These are subcontrols that have the most immediate impact on preventing the advanced targeted attacks that have penetrated existing controls and compromised critical systems at thousands of organizations.
The five quick wins are:

a) Application white listing (in CSC2)
b) Using common, secure configurations (in CSC3)
c) Patch application software within 48 hours (in CSC4)
d) Patch systems software within 48 hours (CSC4)
e) Reduce the number of users with administrative privileges (in CSC3 and CSC12)

## 6. Security Intelligence

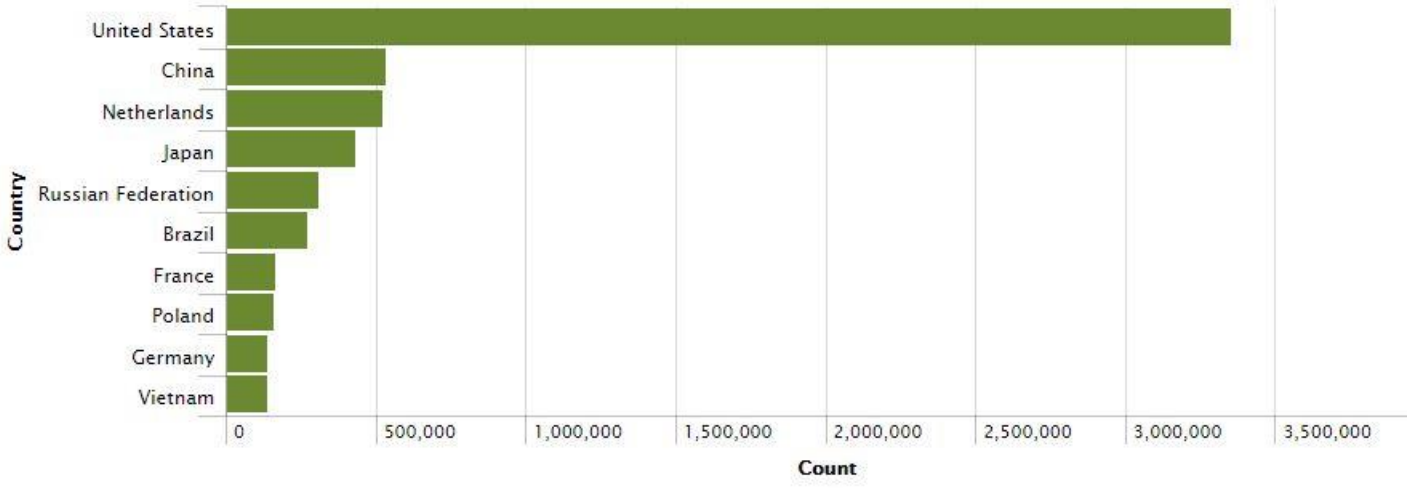
The purpose of this section is to highlight intelligence gathered from the devices under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

The vast majority of attacks on **INSPIRA HEALTH NETWORK** originated geographically from the following Top 10 countries: **USA, Netherlands, China, Germany, Russia, France, Sweden, Iceland, Poland, Korea** listed in order of frequency. The attacks that we observed are happening to companies all around the world. Some results do not include location information that allows map plotting.



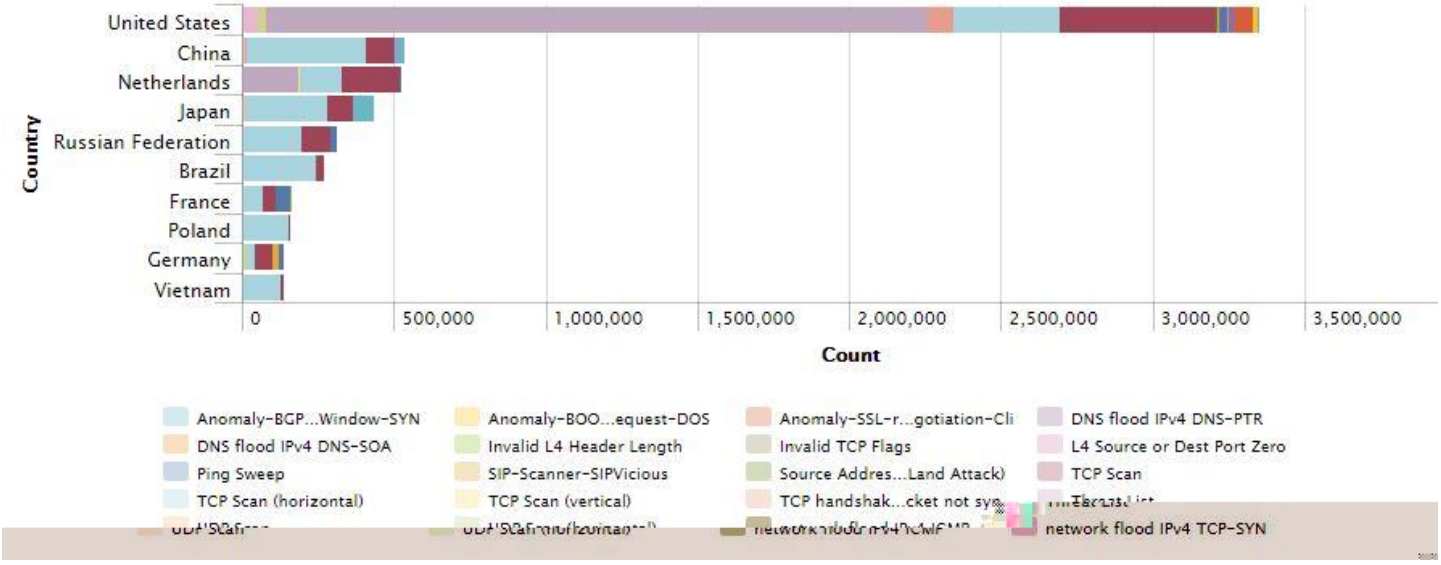
**Graph: Top 10 Attacking Countries Blocked**

This report provides the count of total attacks blocked by country




**Graph: Top 10 Attacking Countries Blocked by Attack Type**

This report provides the count of total attacks types blocked by country

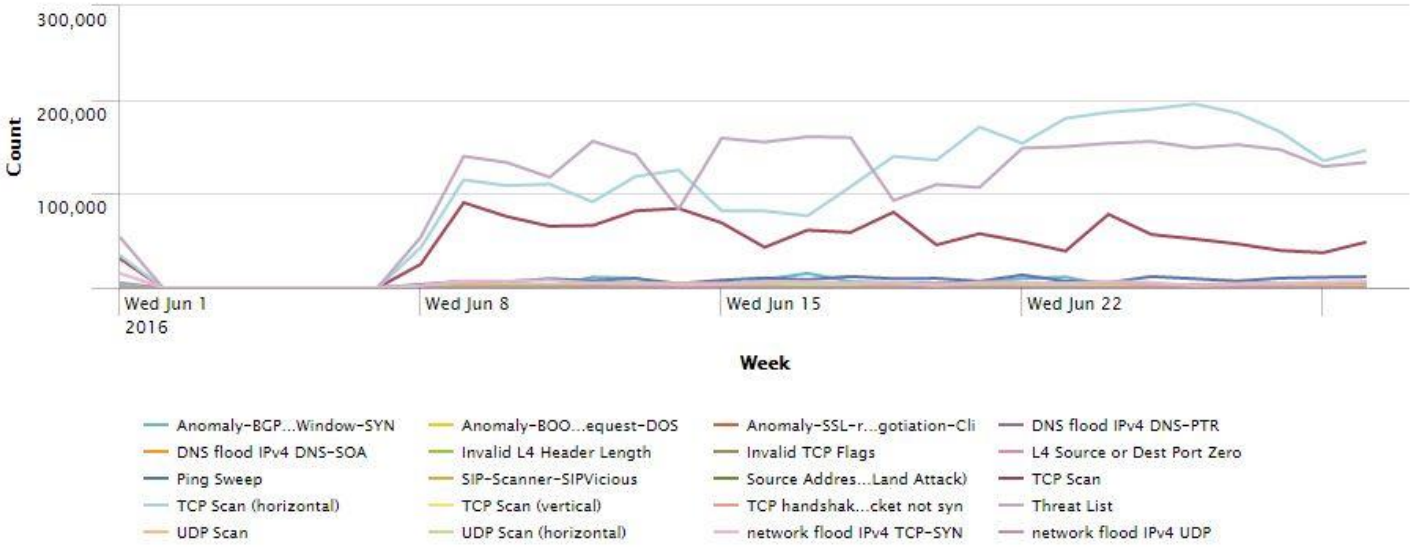


**Graph: Top 10 Attacking Countries Blocked by Protocol**

This report provides the count of attack protocols blocked by country

**Graph: Attacks Types Blocked by Week**

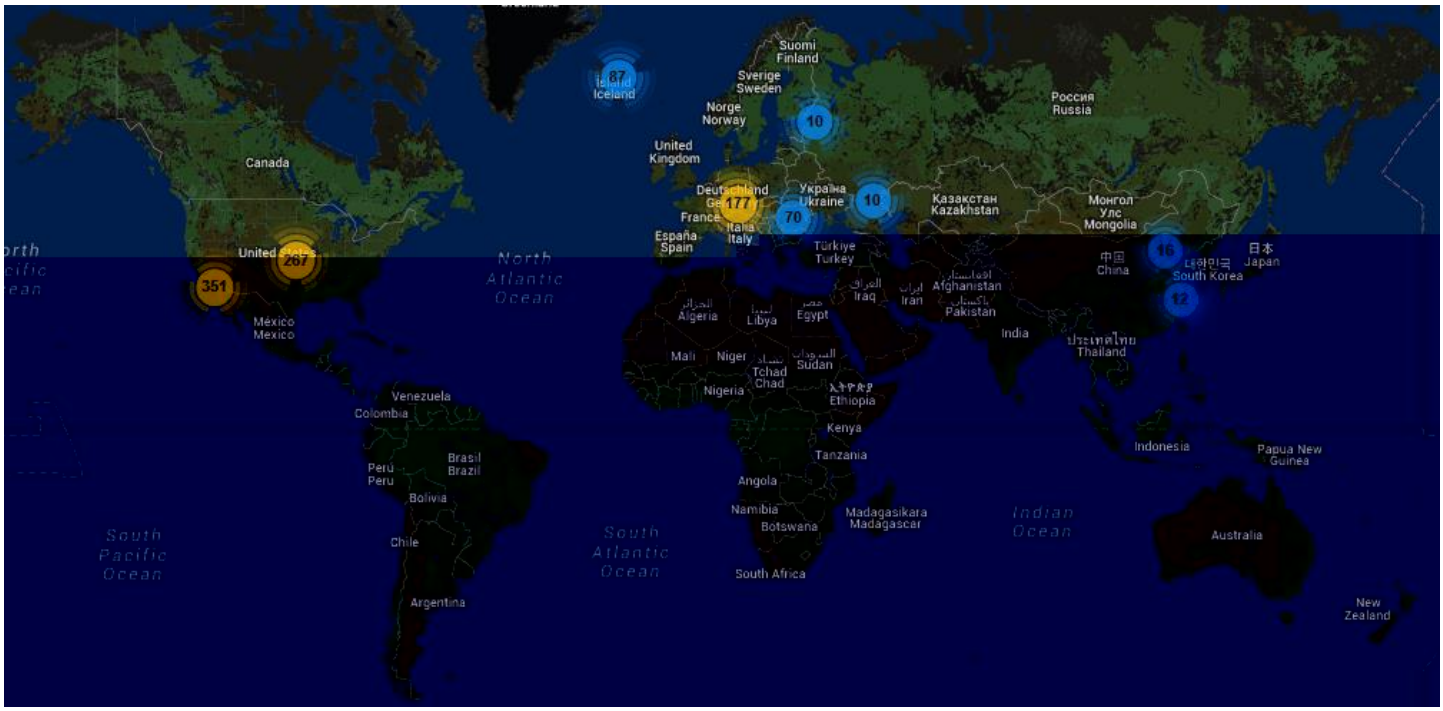
This report provides the count of attacks blocked by week



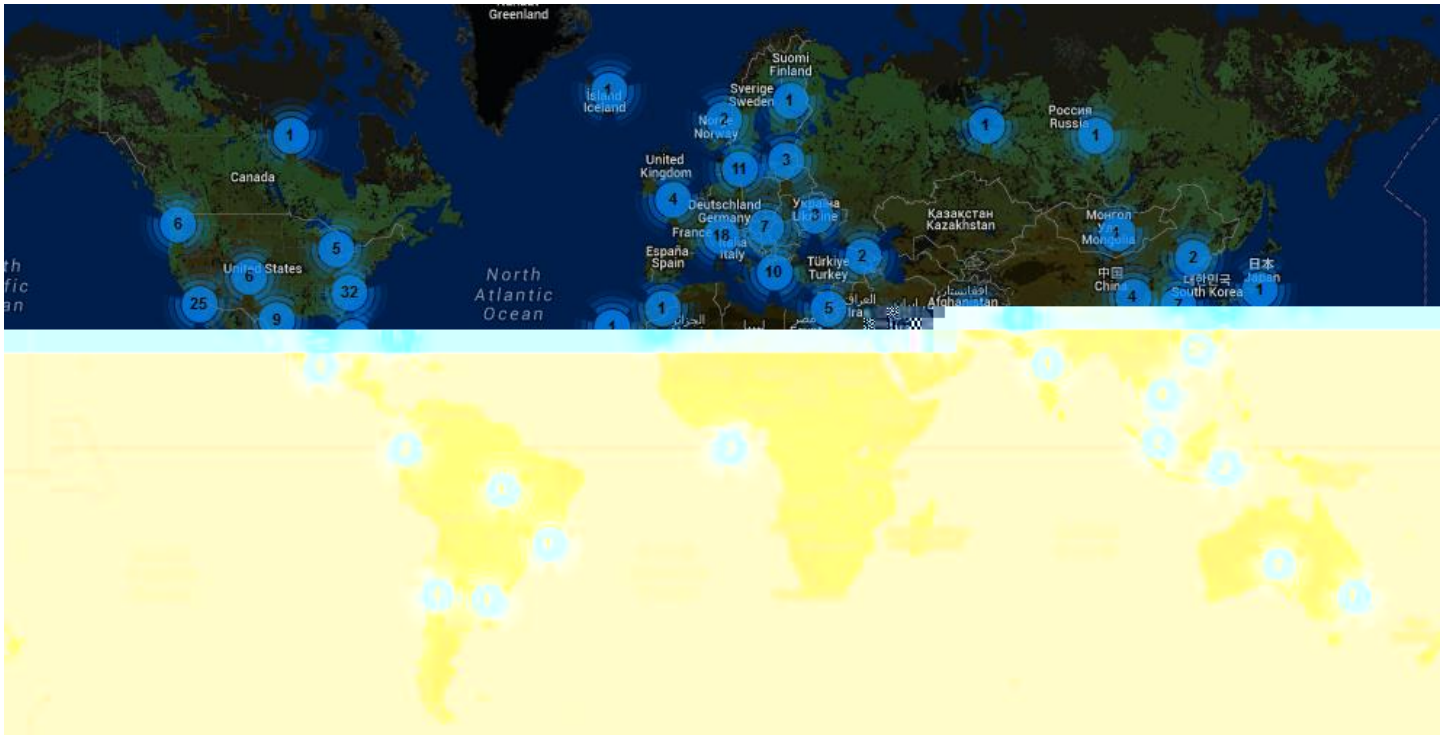
## Known Threat Source Information

**4,425,470** attacks on **INSPIRA HEALTH NETWORK** are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro attack logs and outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

**2,785,087** attacks on **INSPIRA HEALTH NETWORK** from the DNS Blacklist obtained by correlating values from the Project Honey Pot Database. Some results do not include location information that allows map plotting.

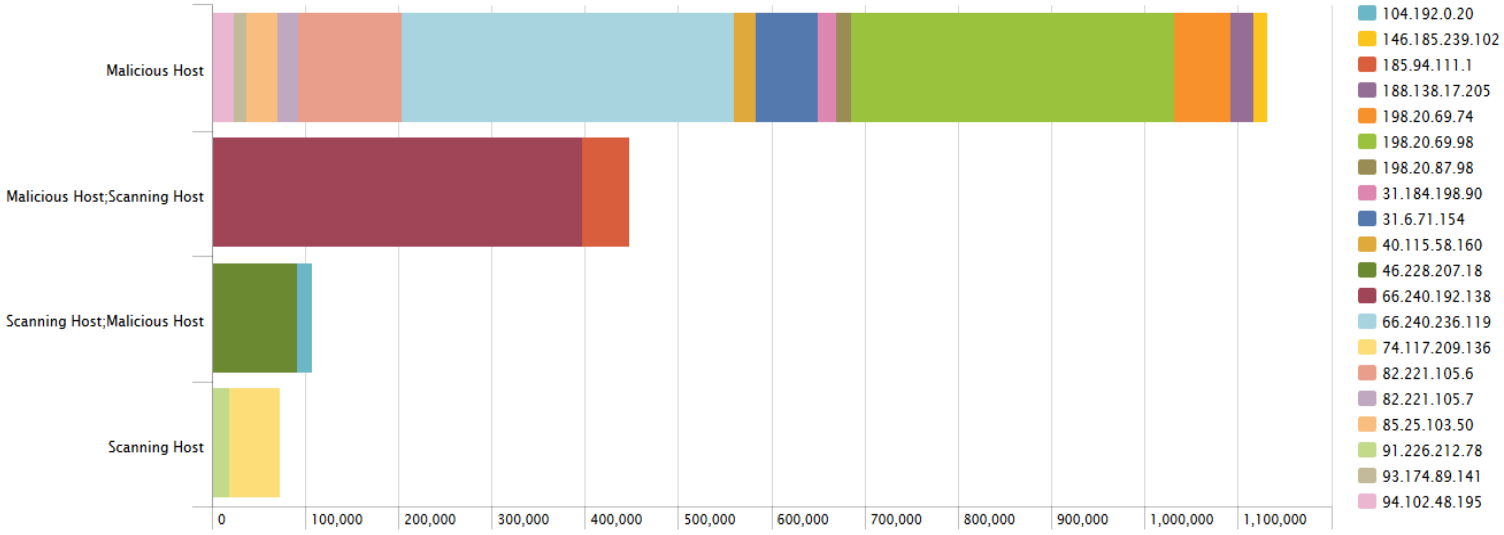


Map of geographic distribution on **INSPIRA HEALTH NETWORK** from known threat sources obtained by correlating values from AlienVault Labs; Emerging Threats; Zeus, Spyeye, and Palevo Tracker. Some results do not include location information that allows map plotting.



**Graph: Known Threat Sources by Threat Type**

This report provides the Top 20 known threat sources by IP and their respective infringing threat type.




**Graph: Attacks Denied**

This report provides the count of total denied attacks along with network security rule.

## Port Information

**Port Information:** Port **80** (http), Port **1443** (ms-sql), Port **8080** (https-alt), Port **3306** (mysql)

Commonly scanned in order to attack web servers. SQL injection is currently the most common form of web site attack in that web forms are very common, often they are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available online. This kind of exploit is easy enough to accomplish that even inexperienced hackers can accomplish mischief. However, in the hands of the very skilled hacker, a web code weakness can reveal root level access of web servers and from there attacks on other networked servers can be accomplished. Structured Query Language (SQL) is the nearly universal language of databases that allows the storage, manipulation, and retrieval of data. Databases that use SQL include MS SQL Server, MySQL, Oracle, PostgreSQL, MongoDB, Access and Filemaker Pro and these databases are equally subject to SQL injection attack.

Web based forms must allow some access to your database to allow entry of data and a response, so this kind of attack bypasses firewalls and endpoint defenses. Any web form, even a simple logon form or search box, might provide access to your data by means of SQL injection if coded incorrectly.

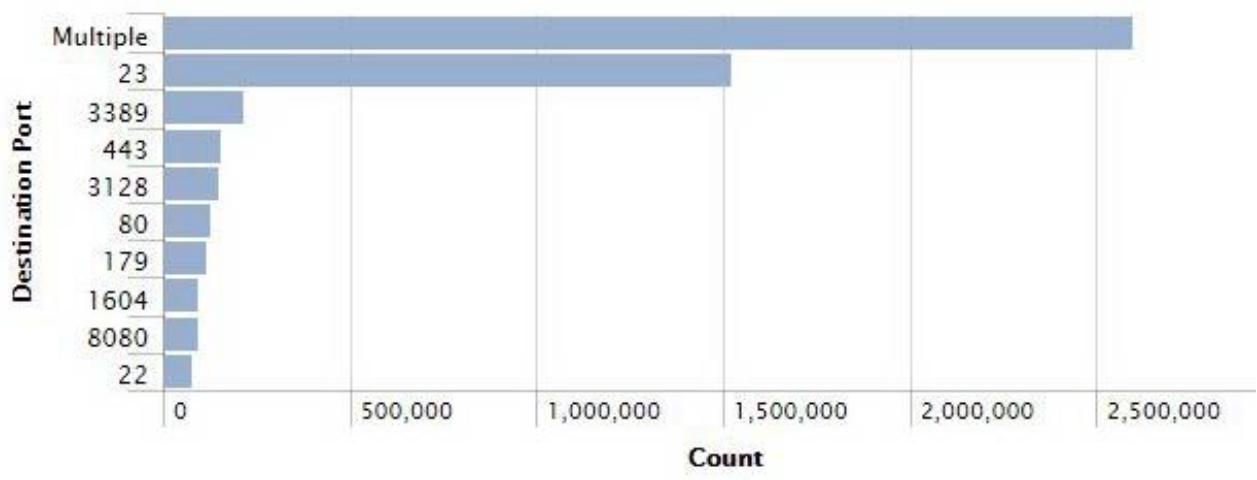
OWASP Top 10 for 2013 lists A1-Injection as the greatest threat and defines this category as:

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

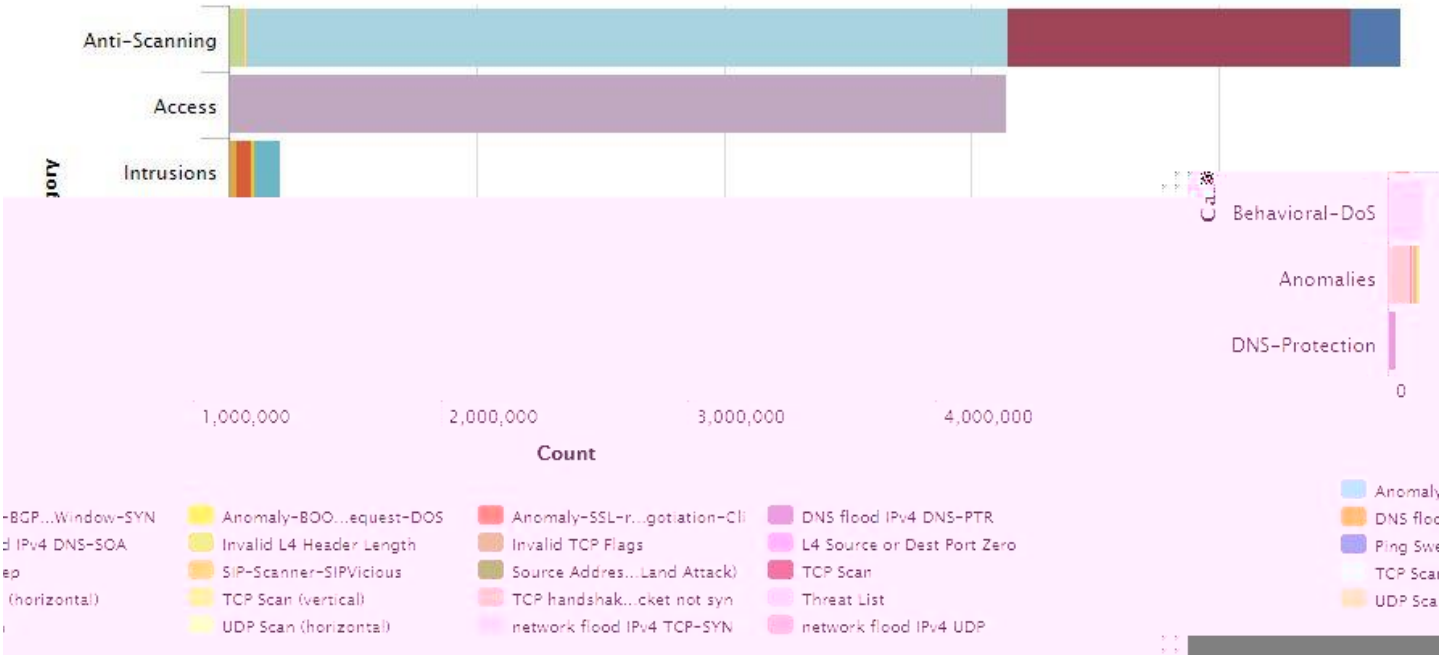
**Graph: Attacks Blocked by Destination Port**

This report provides information on the total number of attacks blocked that were attempted on which port and for how many times.



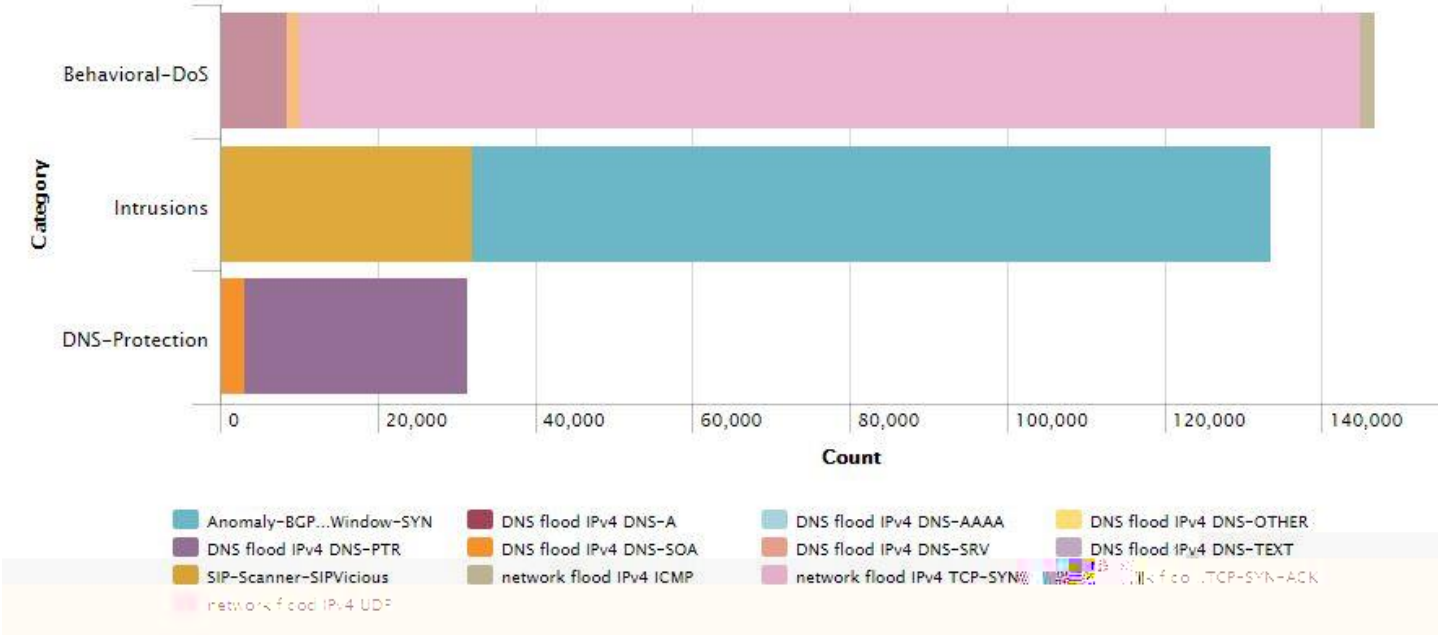

**Graph: Attacks Blocked By Threat Category**

This report lists the attacks blocked per Attack Category, listing the attack name.



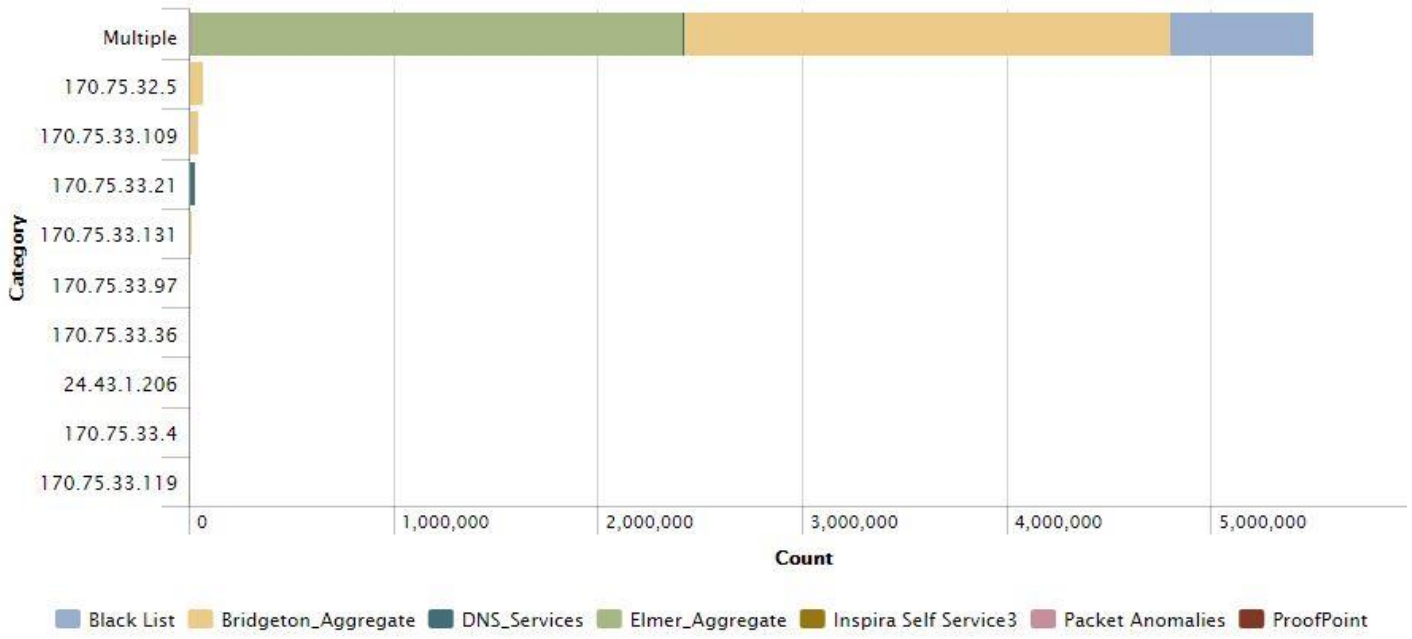
**Graph: Critical Attacks Blocked**

This report provides Critical Attacks information, attack name, network security rule along with the number of times the attack was launched



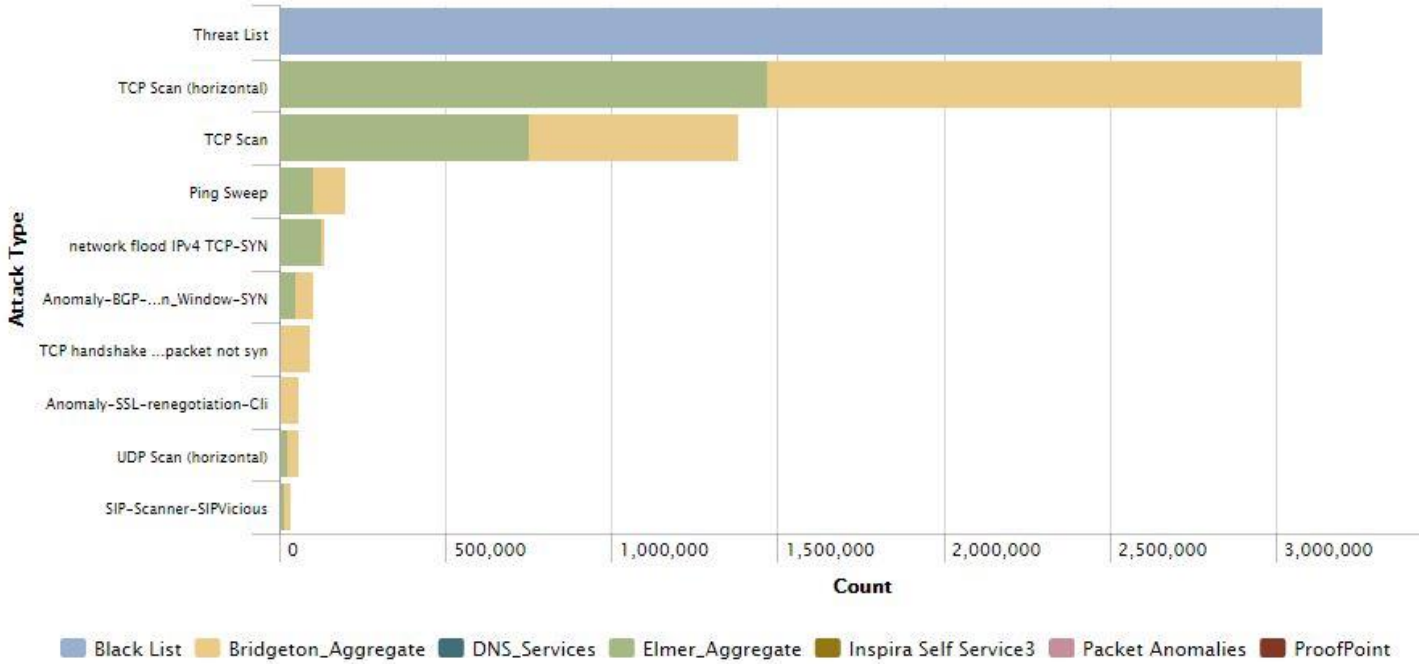
**Graph: Top Attacked Destinations Blocked**

This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



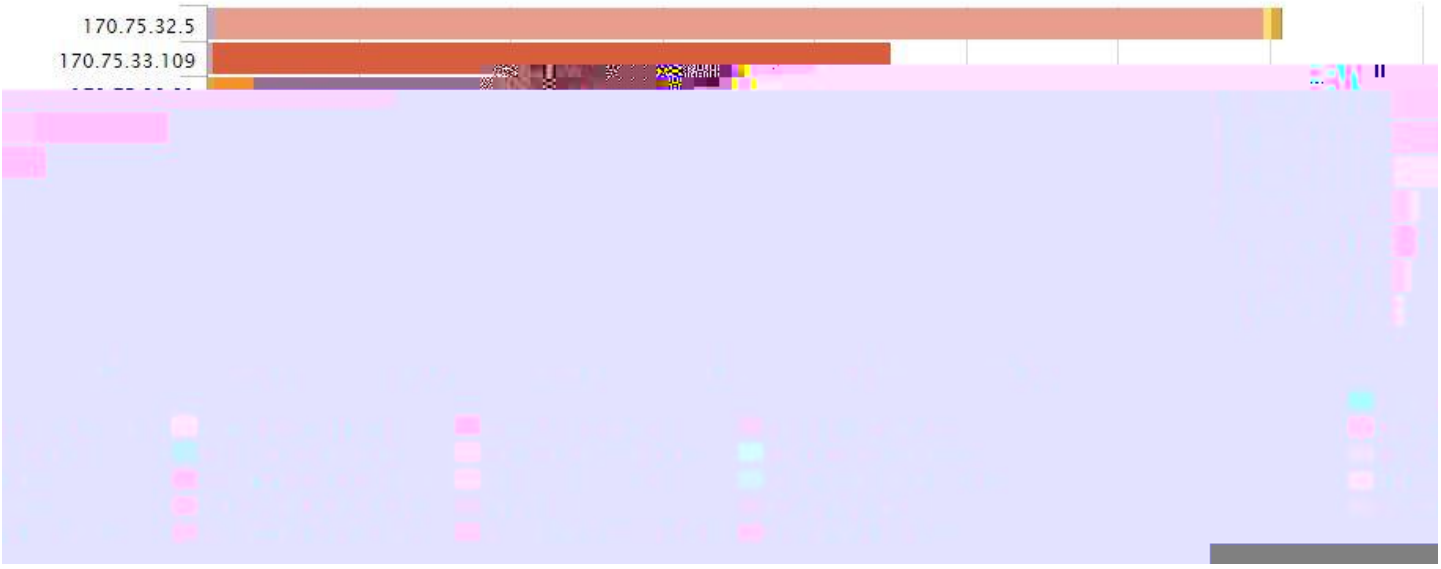

**Graph: Top Attacks Blocked**

This report provides information on the Top Attacks Blocked, the attack name, network security rule and the total number of attacks blocked with this combination.



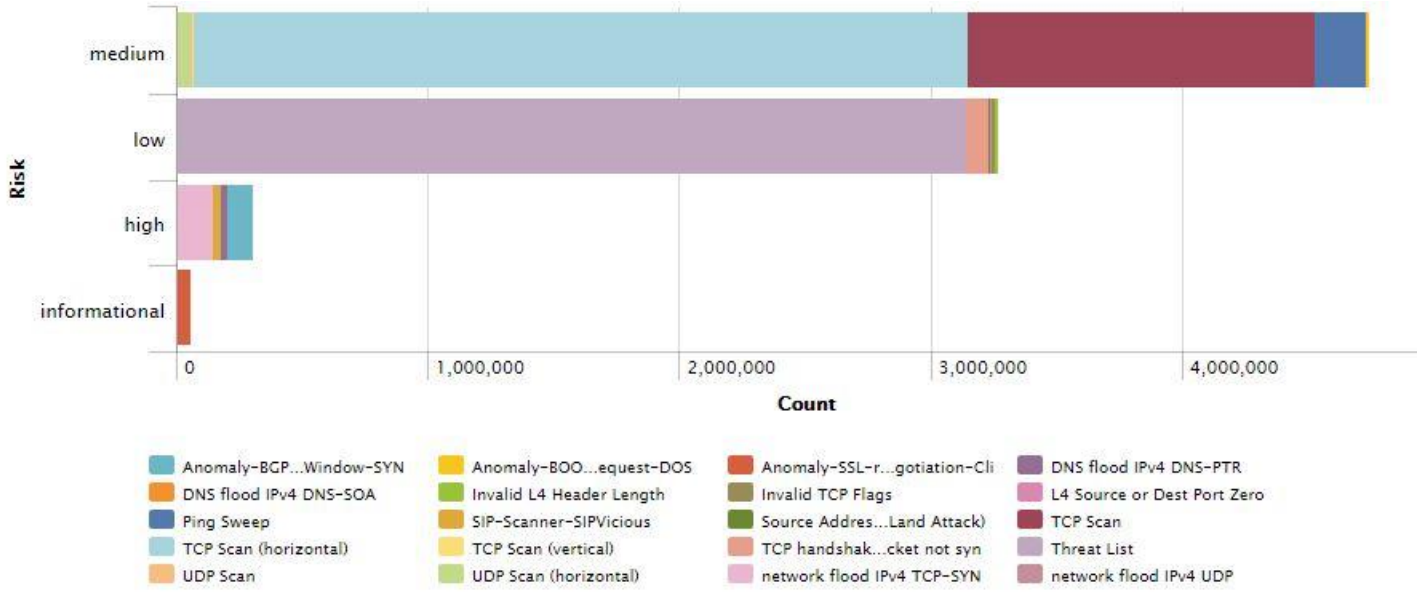
**Graph: Top Attacks Blocked by Destination**

This report provides information on the top attacks targeted at destinations that were blocked on the DP IPS. In this report the destination on which the attack was targeted, attack name, and count are shown.



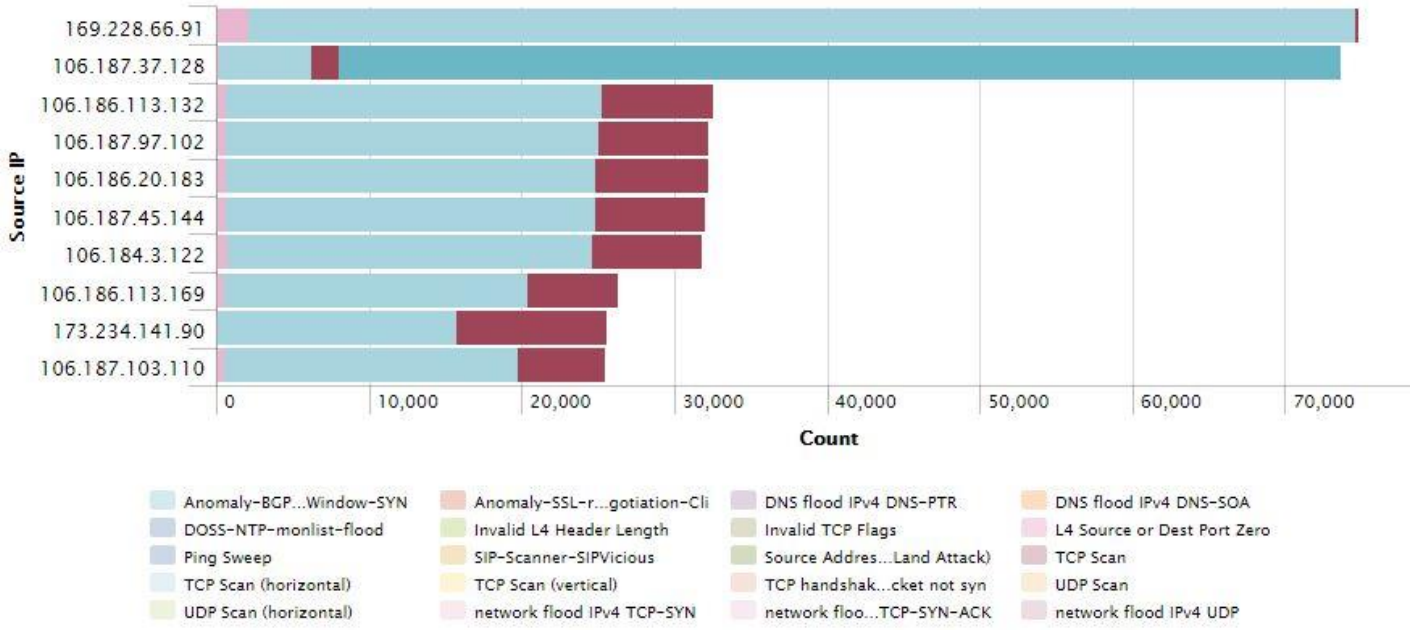

**Graph: Top Attacks Blocked By Risk**

This report provides information on the attacks, which were blocked on DP IPS based on their risk. In this report the risk of the attack and attack name are shown.



**Graph: Top Attacks Blocked by Source**

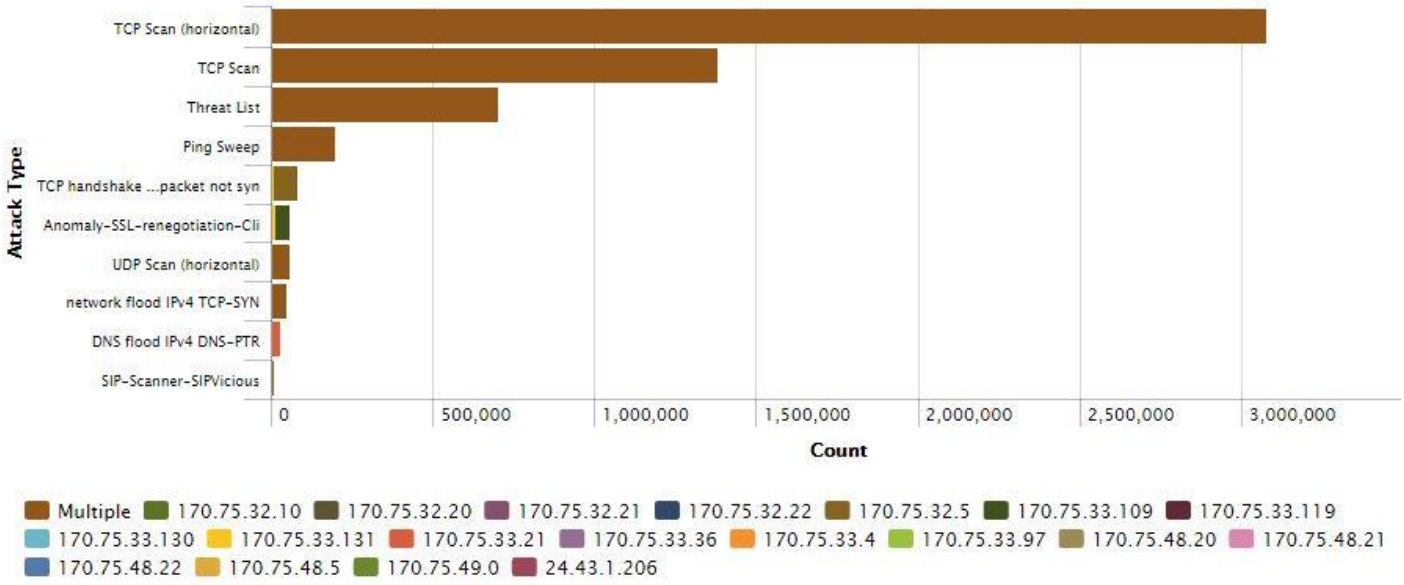
This report provides information on the top attacks blocked, categorized by attacks for each source that was the source of attacks along with the attack name and the number of attacks that triggered with this combination.




**NOTE:** See Appendix 1 – Critical Attack Sources (WHOIS Information)

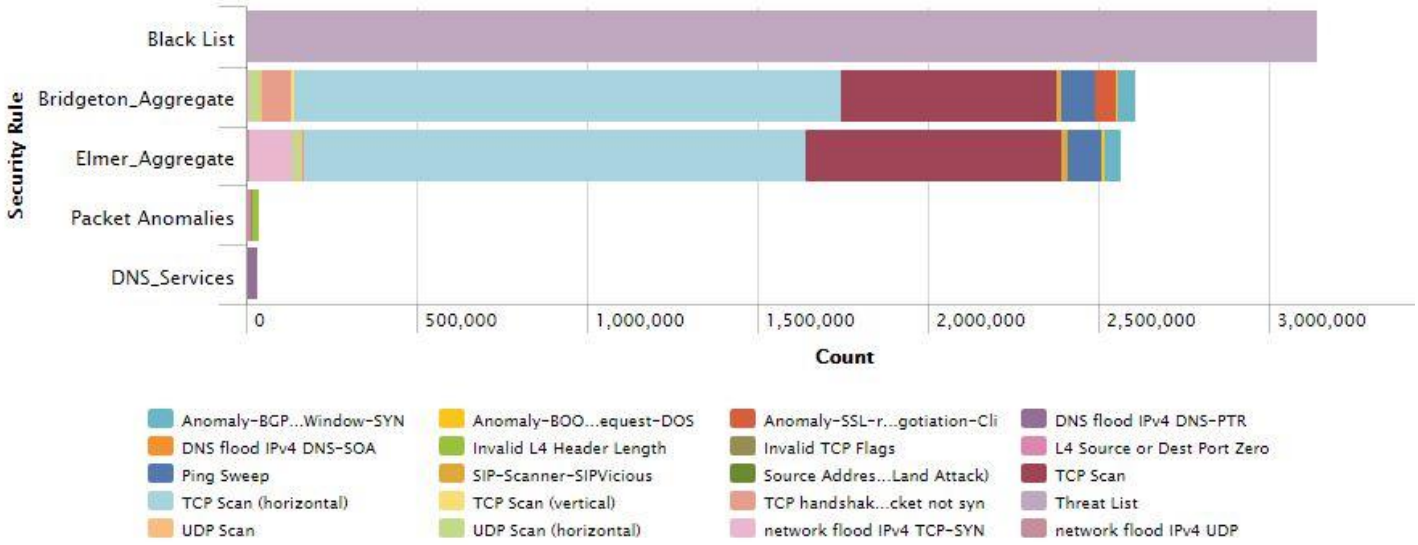
**Graph: Top Destinations by Attacks Blocked**

This report provides information on the attacks attempted for the most number of times on the destination protected system IPs.



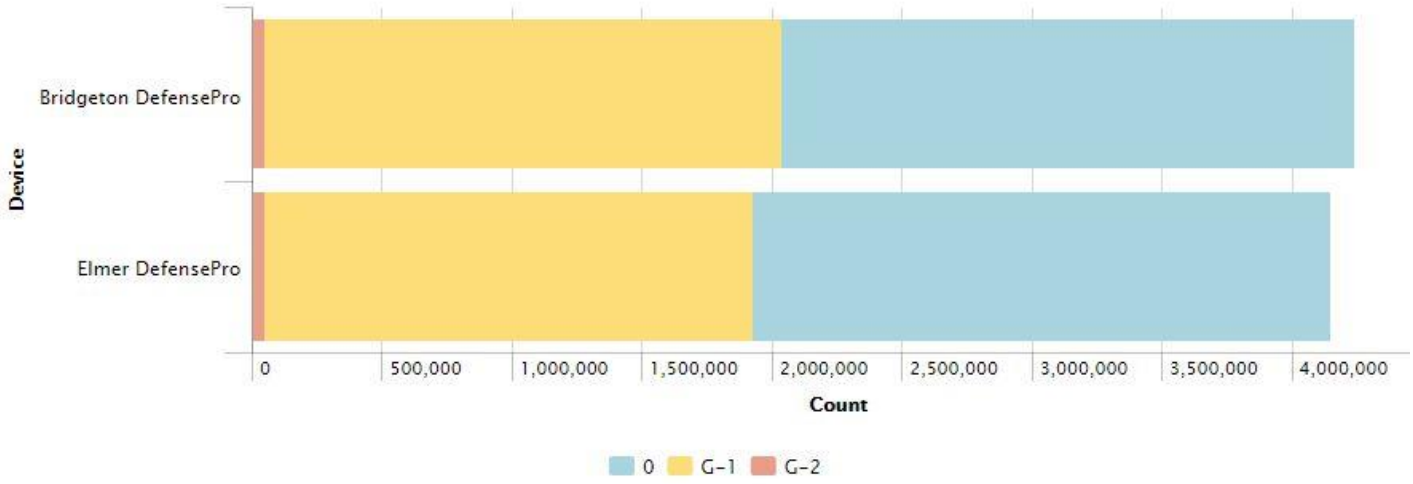

**Graph: Attacks Blocked by Network Security Rule**

This report lists the attacks per network security rule, listing the attack name.



**Graph: Attacks Blocked by Physical Port (per single IPS device)**

This report lists the attacks per physical port.



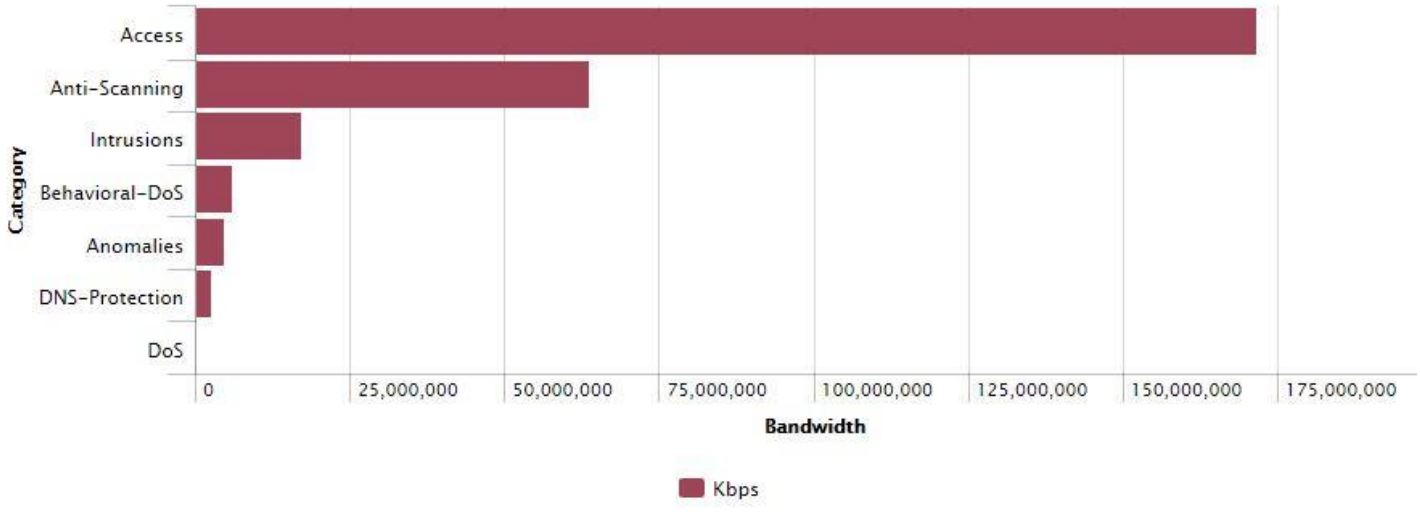
## Bandwidth Information

Access protection dropped **163.69 Gbps**, Anti-Scanning protection dropped **60.69 Gbps**, Intrusion protection dropped **16.38 Gbps** of total traffic, Behavioral-DoS dropped **5.73 Gbps**, **4.39 Gbps** dropped by Packet Anomaly protection rules, DNS Protection dropped a total of **2.37 Gbps** of traffic, Dos Protection Dropped **0.04 Gbps,** for a total of **253.29 Gbps** of malicious traffic was discarded this period.

| Category | Gbps | Mbps |
|---|---|---|
| Access | 163.69 | 167614.06 |
| Anti-Scanning | 60.69 | 62142.35 |
| Intrusions | 16.38 | 16777.83 |
| Behavioral-DoS | 5.73 | 5871.74 |
| Anomalies | 4.39 | 4496.48 |
| DNS-Protection | 2.37 | 2423.68 |
| DoS | 0.04 | 40.96 |
| Total Bandwidth in Gbps/Mbps | 253.29 | 259367.10 |

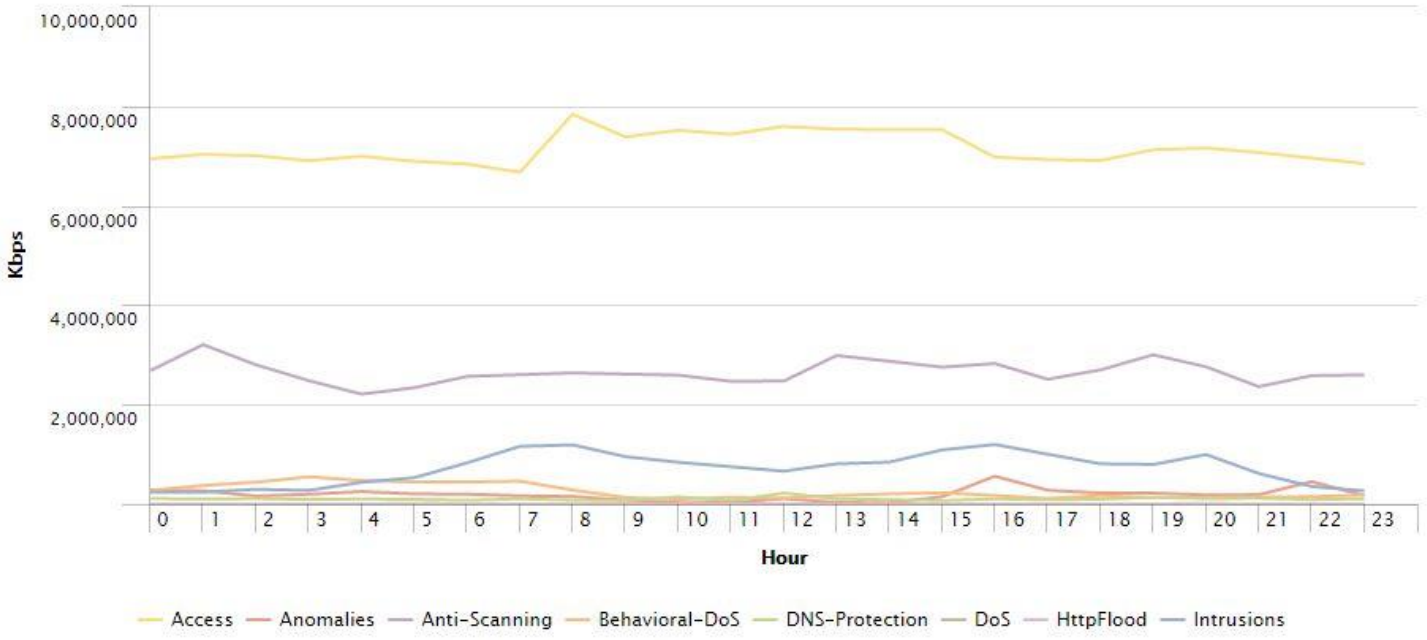
**Graph: Attack Categories Blocked by Bandwidth**

This report shows the attack categories based on the BW of the attacks sharing the same category including Kbps.



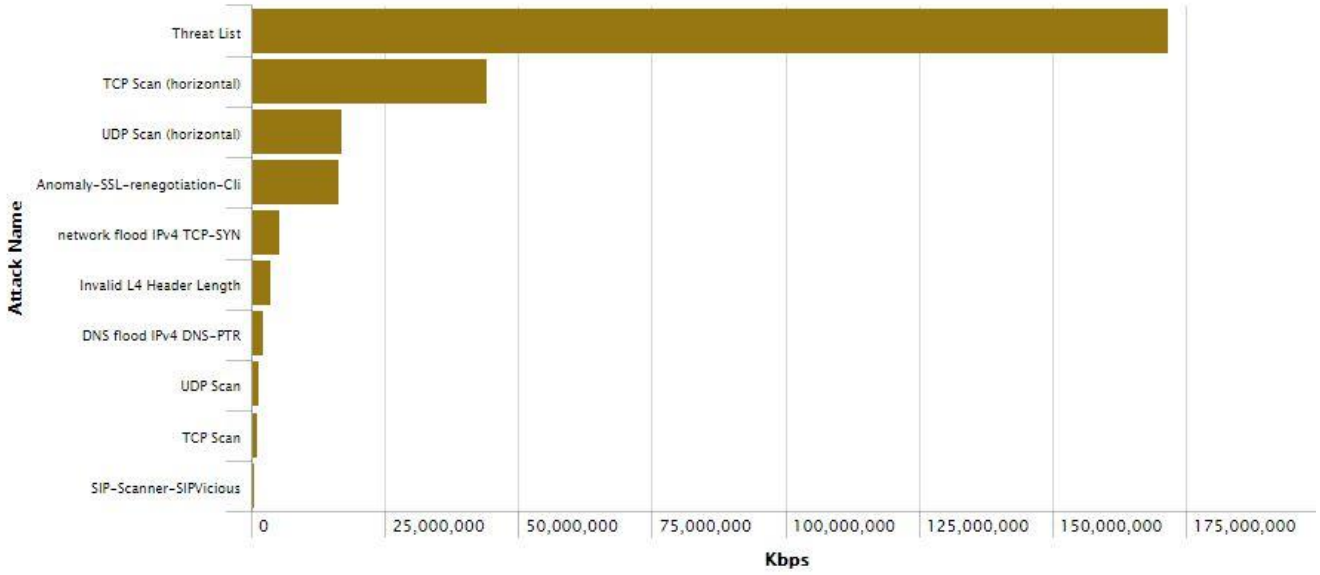
**Graph: Bandwidth by Blocked Threat Category by Hour of Day**

This report shows the most bandwidth consuming threat categories based on the bandwidth of the attacks sharing the same threat category for each hour of day.



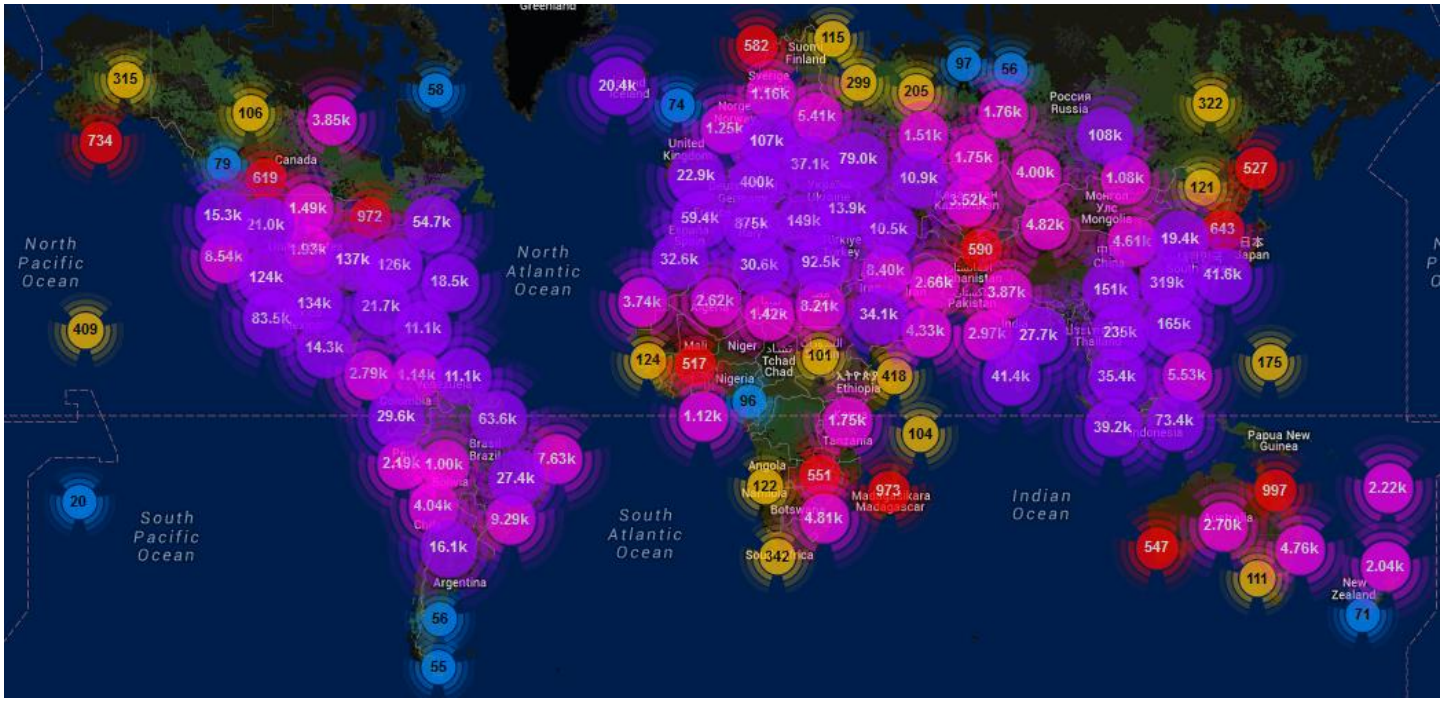

**Graph: Top Attacks Blocked by Bandwidth**

This report shows the most bandwidth consuming attacks based on the BW of the attack including Kbits.



## Scanning Information

Map of geographic distribution of **4,841,746** attacks on **INSPIRA HEALTH NETWORK** from scanning sources. Some results do not include location information that allows map plotting.




Network-wide Anti Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modeling, commonplace after the information gathering phase of a targeted or planned attack.

We have included some of the most important ports scanned this period which tend to be exploited frequently by attackers. **Port Information:** Port **80** (http), Port **443** (http-alt)

Commonly scanned in order to attack web servers. SQL injection is currently the most common form of web site attack in that web forms are very common, often they are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available online. This kind of exploit is easy enough to accomplish that even inexperienced hackers can accomplish mischief. However, in the hands of the very skilled hacker, a web code weakness can reveal root level access of web servers and from there

attacks on other networked servers can be accomplished. Structured Query Language (SQL) is the nearly universal language of databases that allows the storage, manipulation, and retrieval of data. Databases that use SQL include MS SQL Server, MySQL, Oracle, PostgreSQL, MongoDB, Access and Filemaker Pro and these databases are equally subject to SQL injection attack.

Web based forms must allow some access to your database to allow entry of data and a response, so this kind of attack bypasses firewalls and endpoint defenses. Any web form, even a simple logon form or search box, might provide access to your data by means of SQL injection if coded incorrectly.

**Port Information:** Port **1433** (ms-sql-s), **3306** (mysql)

OWASP Top 10 for 2013 lists A1-Injection as the greatest threat and defines this category as: Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

**Port Information:** Port **23** (telnet), **22** (ssh)

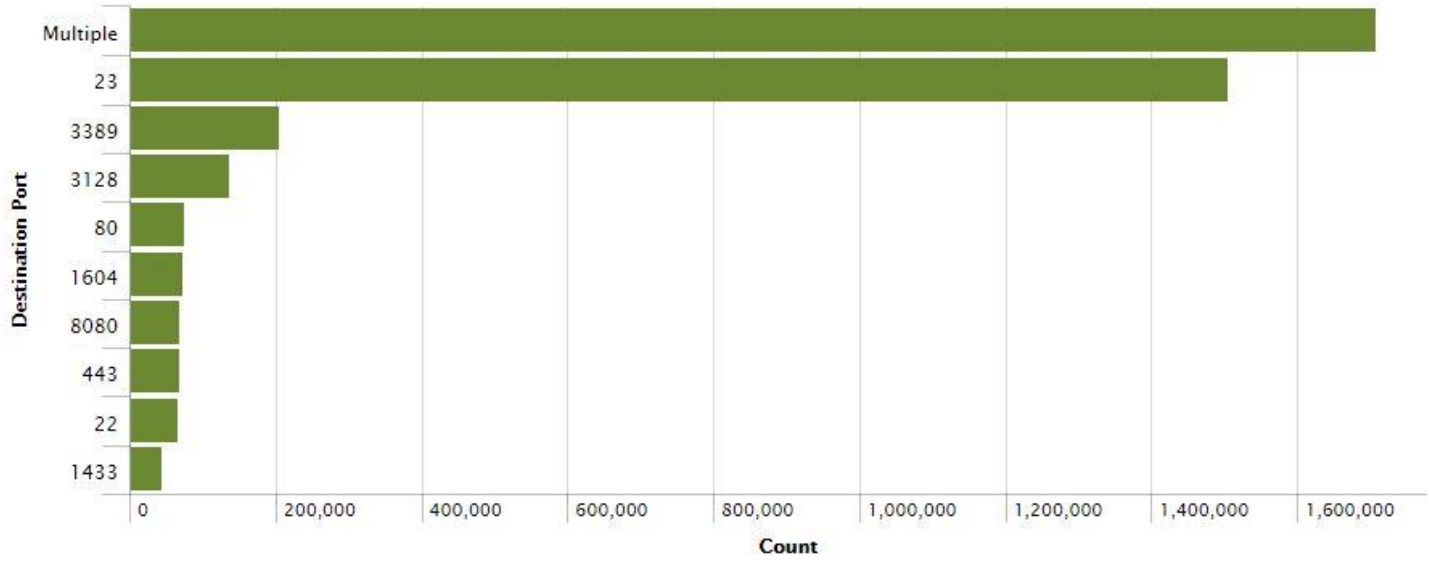
This port is commonly bruteforced for default administrative accounts which usually provide access to network and communications equipment.

**Port Information:** Port **5060** (sip)

The default gateway commonly associated with the SIP (Session Initiation Protocol) is the system port 5060. This communication portal supports the signaling protocol which is widely deployed for setting up (including tearing down) of sessions involving multimedia communication like video calls, voice calls and even VoIP (Voice over Internet Protocol). Threat actors commonly seek out these servers to comandeer the service in order to make free calls to countries of their choice or use them to carry out phone scams.

**Graph: Top Probed Applications Blocked**

This report shows historical view of the Top probed L4 ports.

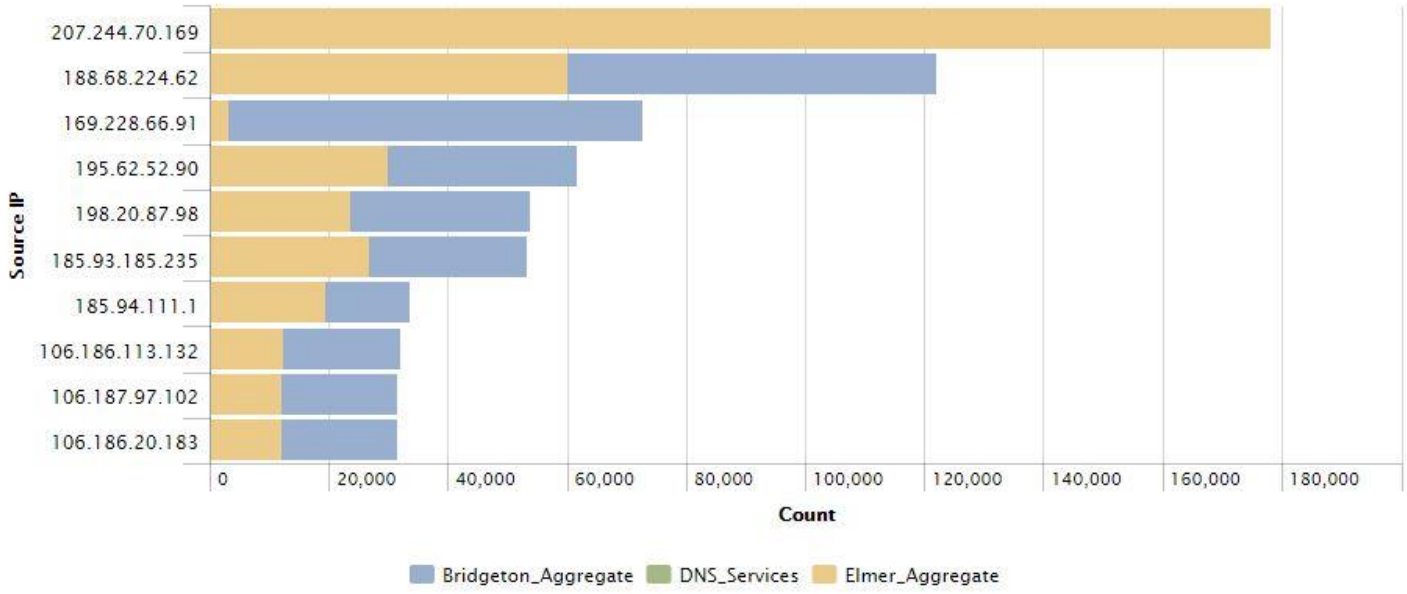


**Graph: Top Probed IP Addresses Blocked**

This report shows historical view of the Top probed IP addresses that were being scanned along with the network security rule.

**Graph: Top Scanners Blocked (Source IP Addressed)**

This report shows historical view of the Top source IP addresses that have scanned the network by network scanning activities along with the network security rule.




**NOTE:** See Appendix 2 – Top Scanners Blocked (Source IP Addressed)

## Vulnerability Management

It is important to establish a vulnerability management program as part of the information security strategy because soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their systems compromised.

The GLESEC AVDS Management System platform performs a security mapping of your organization network, runs tests on everything the speaks IP, and accurately evaluates the presence of vulnerabilities.

Many of the vulnerabilities will provide CVE data. CVE (Common
Vulnerabilities and Exposures) is a list of information security exposures and vulnerabilities sponsored by US-CERT and maintained by the MITRE Corporation. The CVE mission is to provide standard names for all publicly known security exposures as well as standard definitions for security terms. The CVE can be searched online at http://nvd.nist.gov/.

## Vulnerability Score

The score of a vulnerability is determined by its risk factor; High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of each vulnerability. In addition to numeric scores, the CVSS provides severity rankings of High, Medium, and Low but these qualitative rankings are simply mapped from the numeric CVSS scores.
Vulnerabilities are labelled as:

a) Low risk if they have a CVSS base score of 0.0 – 3.9
b) Medium risk if they have a CVSS base score of 4.0 – 6.9
c) High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerabilities in the report are classified into 3 risk categories: high, medium or low.

**High Risk**

Describes vulnerabilities that can allow an attacker to gain elevated privileges, remote command execution, full read/write access, or critical information disclosure (e.g. passwords, hashes) on a vulnerable machine and should be addressed as top priority.

**Medium Risk**

Describes vulnerabilities that either expose sensitive data, directory browsing and traversal, disclosure of security controls, facilitate unauthorized use of services or denial of service to an attacker.

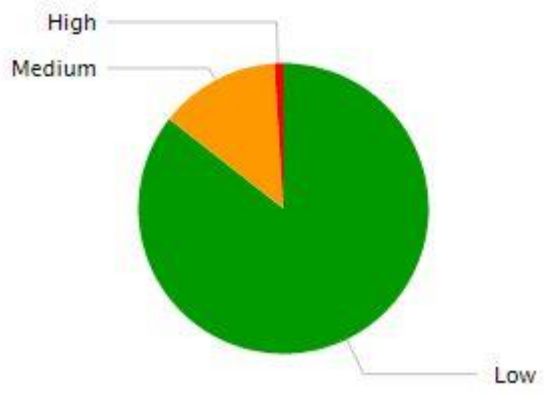
**Low Risk**

Describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social-engineering or similar attacks.

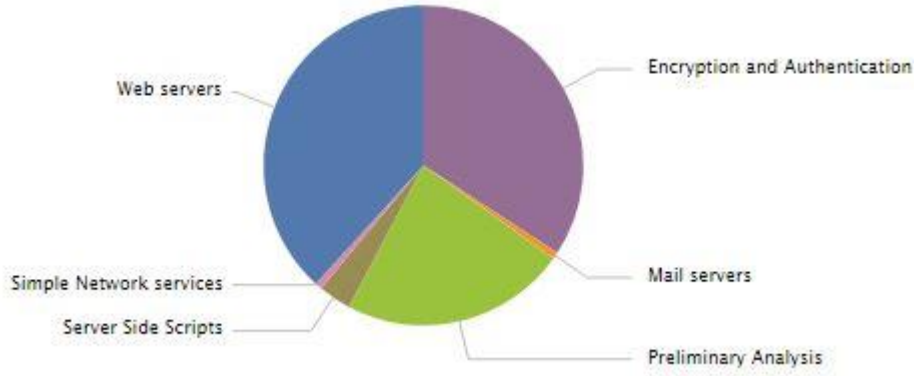
## Vulnerability Information

We can observe that Intrusions (known attack signatures), HTTP Flood and Web Scanning attempts are targeting Web Servers and are being dropped by the DefensePro. We cannot be 100% sure but there is a high probability that this type of attack is occurring and if the DefensePro was not in place, the attack might have been successfully carried out. The same is true for Mail servers which are frequently being scanned (Web Scanning).

**Graph: Risk Distribution**
This report depicts the risk distribution of vulnerabilities discovered this report period

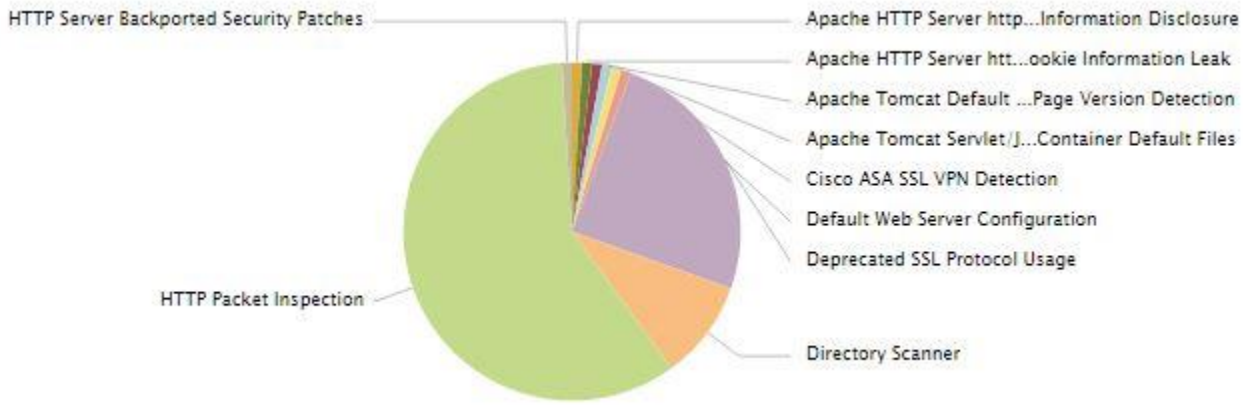



**Graph: Most Frequent Vulnerability Category**
This report depicts the most frequent vulnerabilities by category discovered this report period



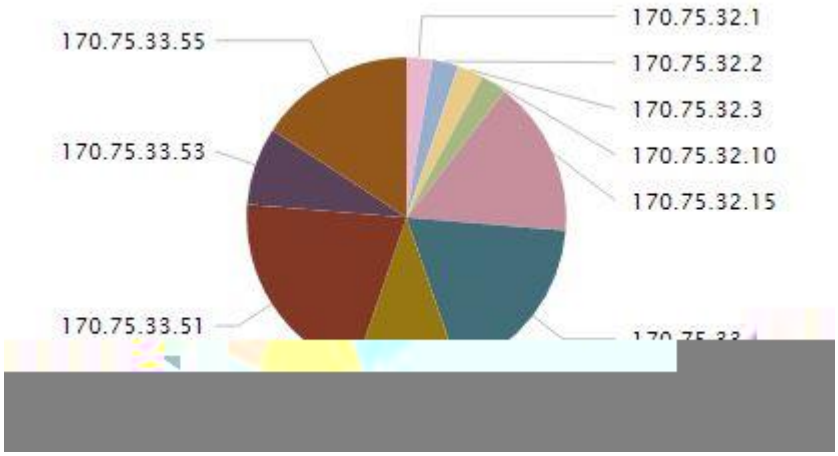
**Graph: Most Frequent Vulnerability Name**

This report depicts the most frequent vulnerabilities discovered this report period



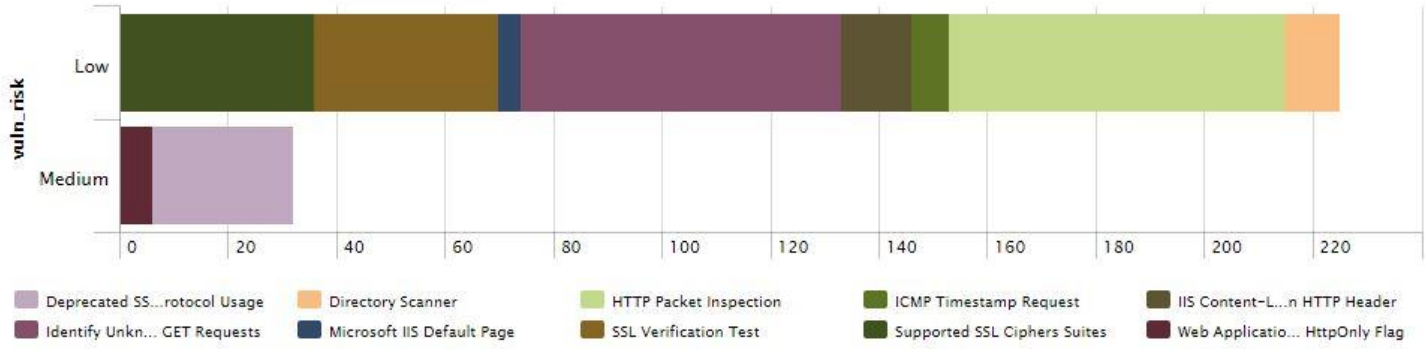

**Graph: Most Vulnerable Host**

This report depicts the most vulnerable hosts discovered this report period



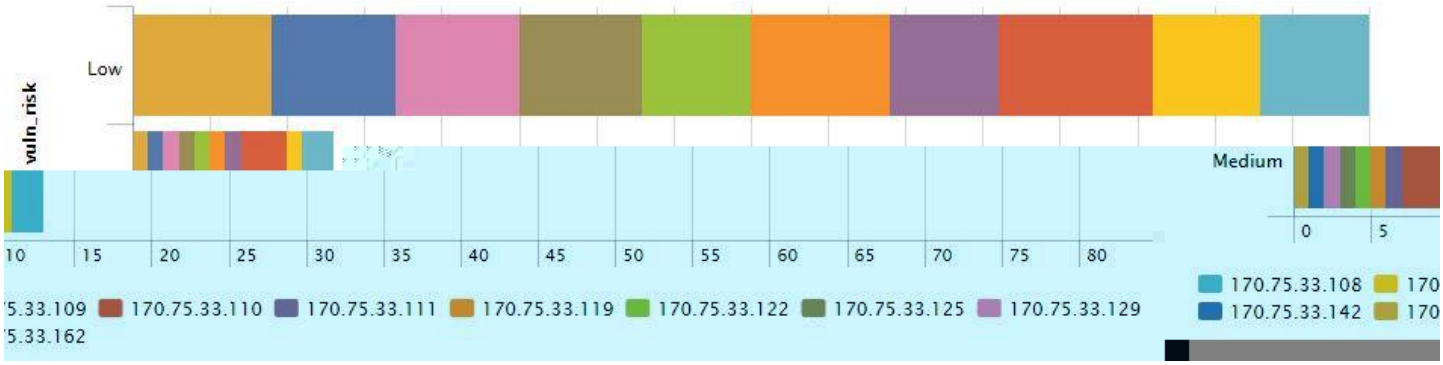

**Graph: Vulnerability Risk by Vulnerability Name**

This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



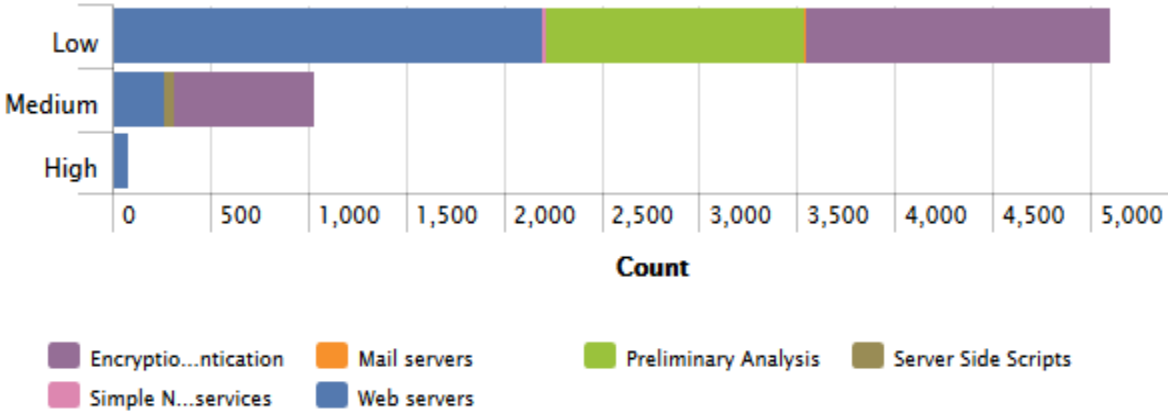
**Graph: Vulnerability Risk by Host**

This report illustrates the vulnerability risk and count by category discovered this report period



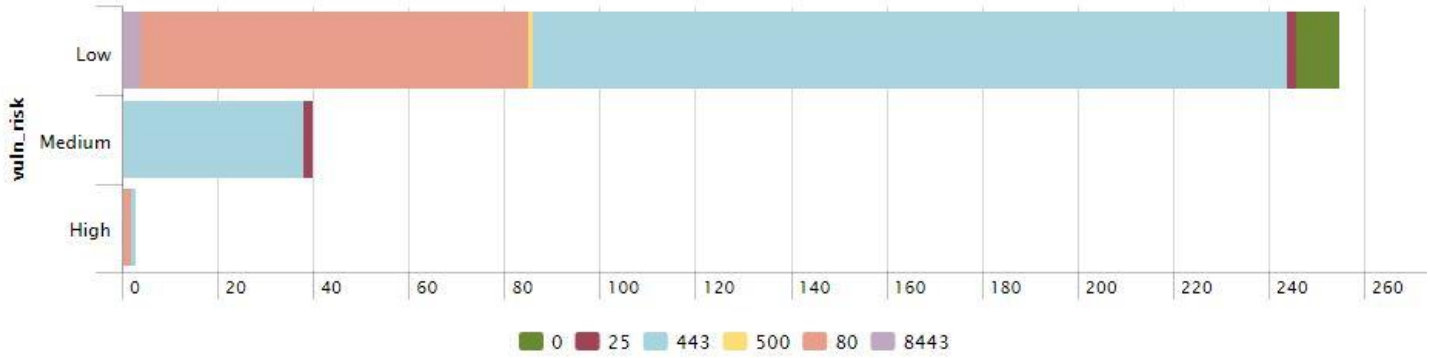

**Graph: Vulnerability Risk by Category**

This report illustrates the vulnerability risk and count by category discovered this report period



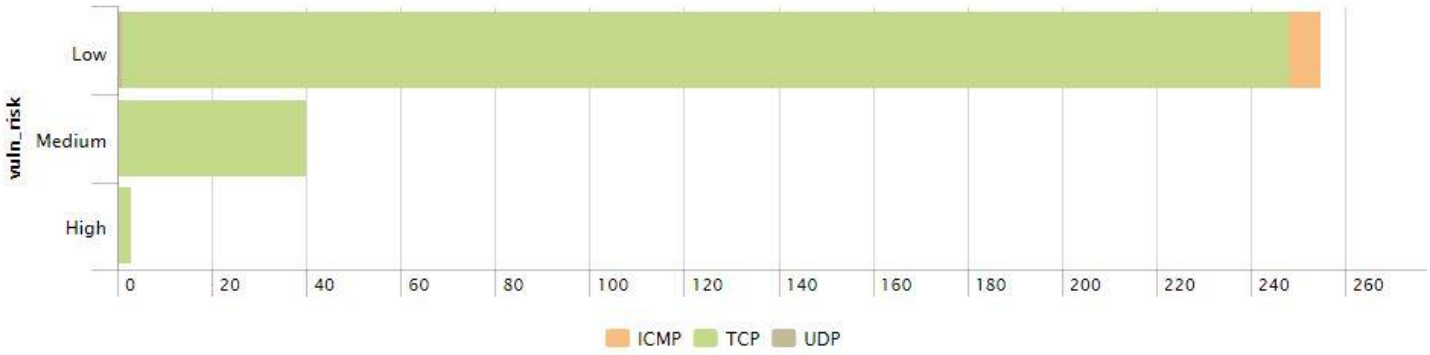

**Graph: Vulnerability Risk by Port**

This report illustrates the vulnerability risk and count by port discovered this report period



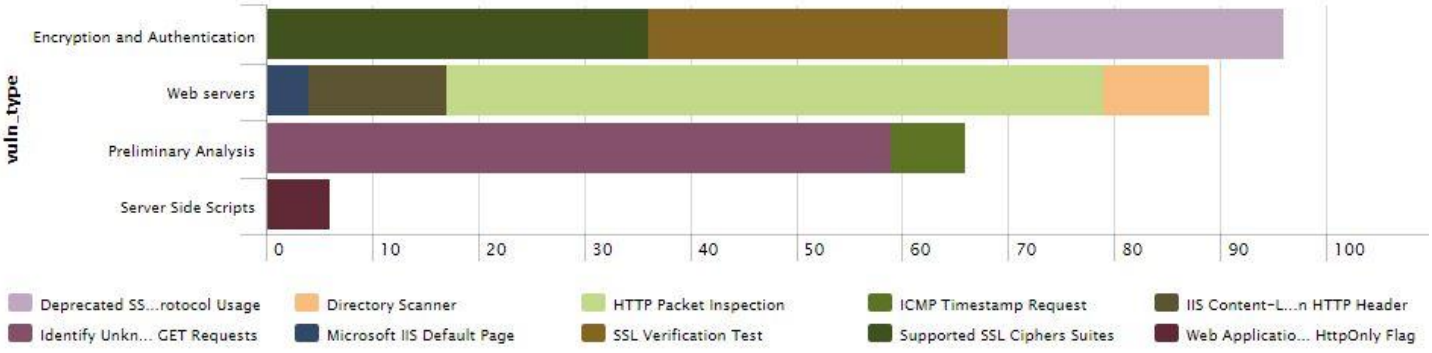

**Graph: Vulnerability Risk by Protocol**

This report illustrates the vulnerability risk and count by protocol discovered this report period



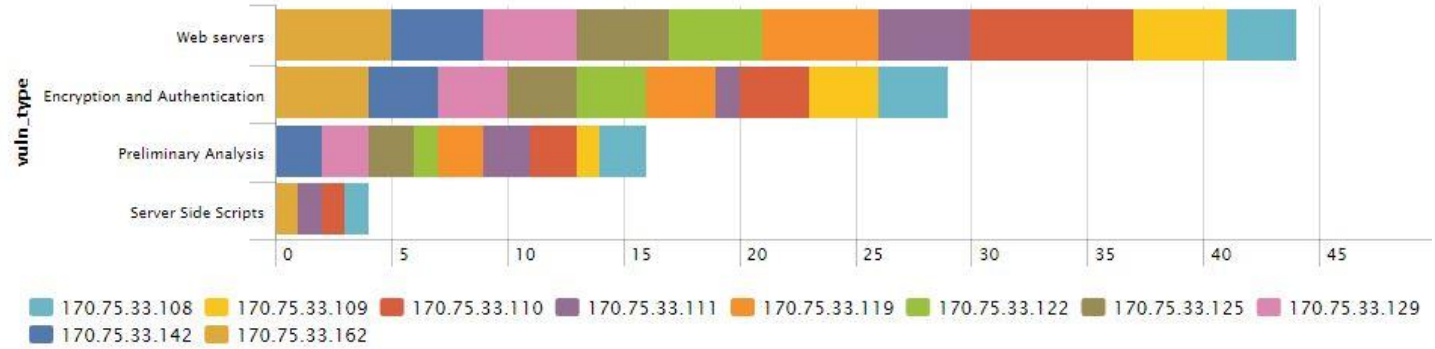

**Graph: Vulnerability Category by Vulnerability Name**

This report illustrates the vulnerability category and count by vulnerability name discovered this report period



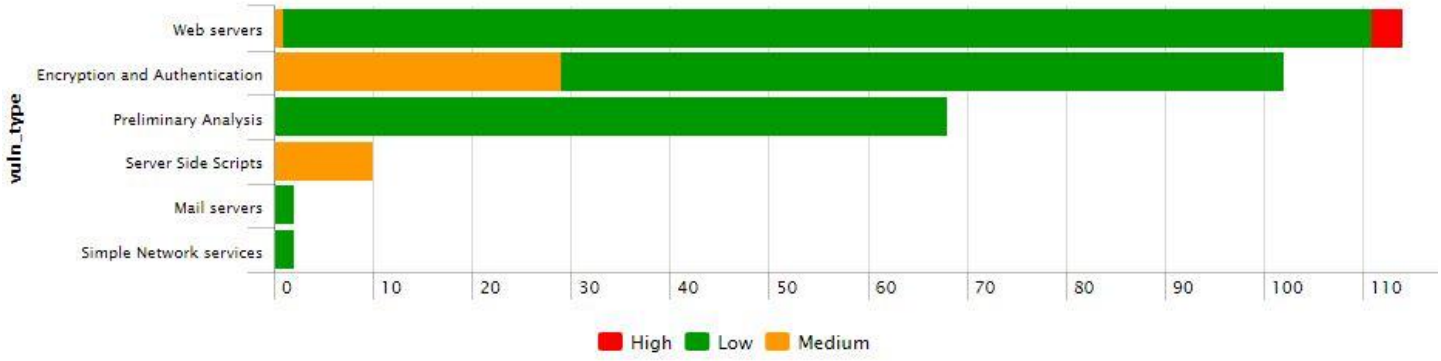
**Graph: Vulnerability Category by Host**

This report illustrates the vulnerability category and count by host discovered this report period



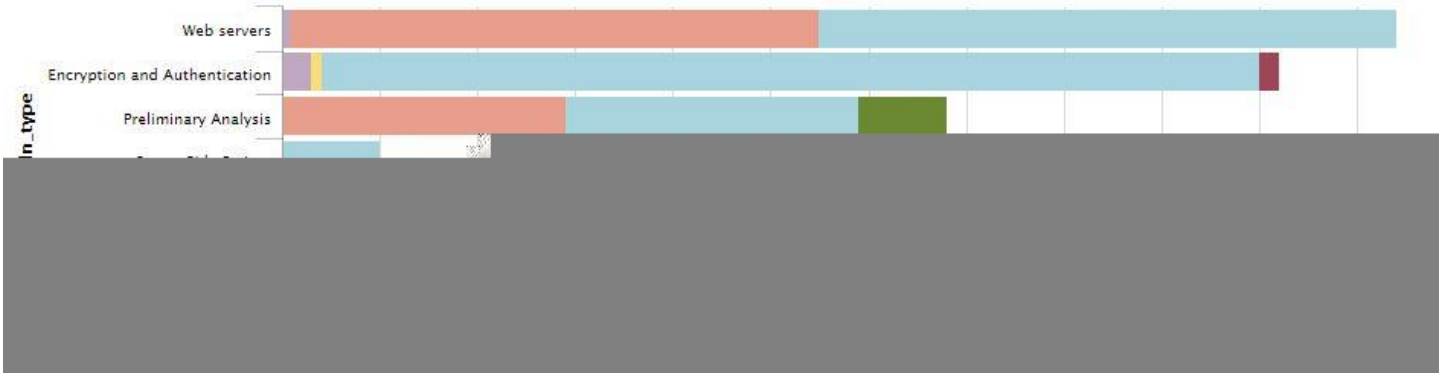

**Graph: Vulnerability Category by Risk**

This report illustrates the vulnerability category and count by risk discovered this report period



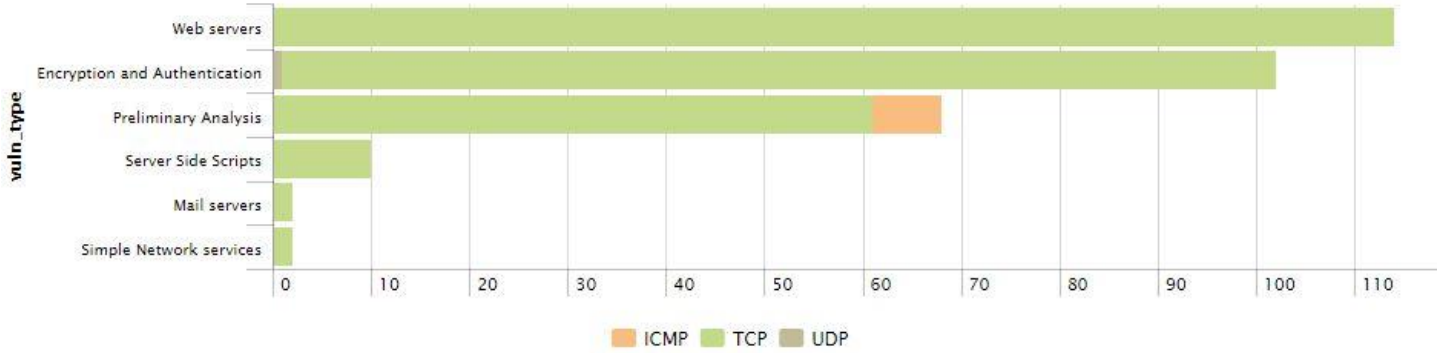

**Graph: Vulnerability Category by Port**

This report illustrates the vulnerability category and count by port discovered this report period



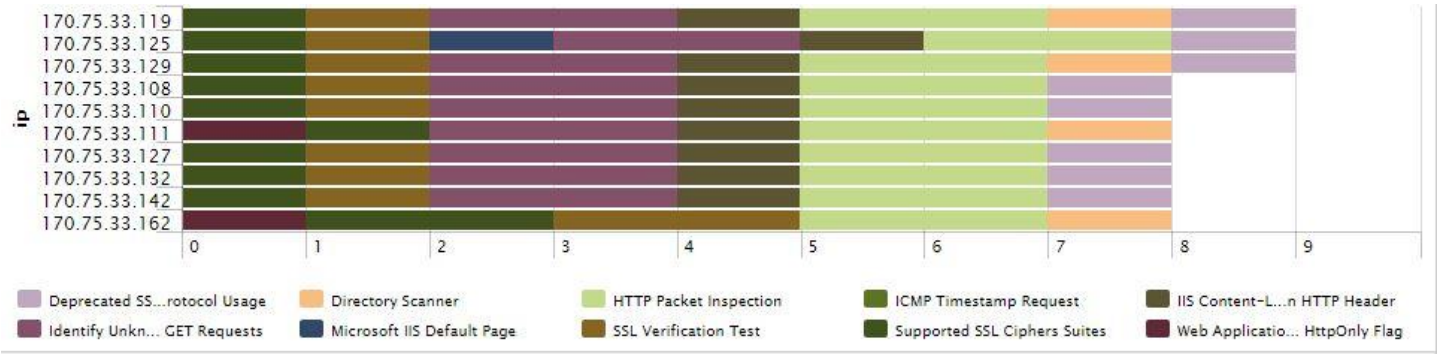
**Graph: Vulnerability Category by Protocol**

This report illustrates the vulnerability category and count by protocol discovered this report period



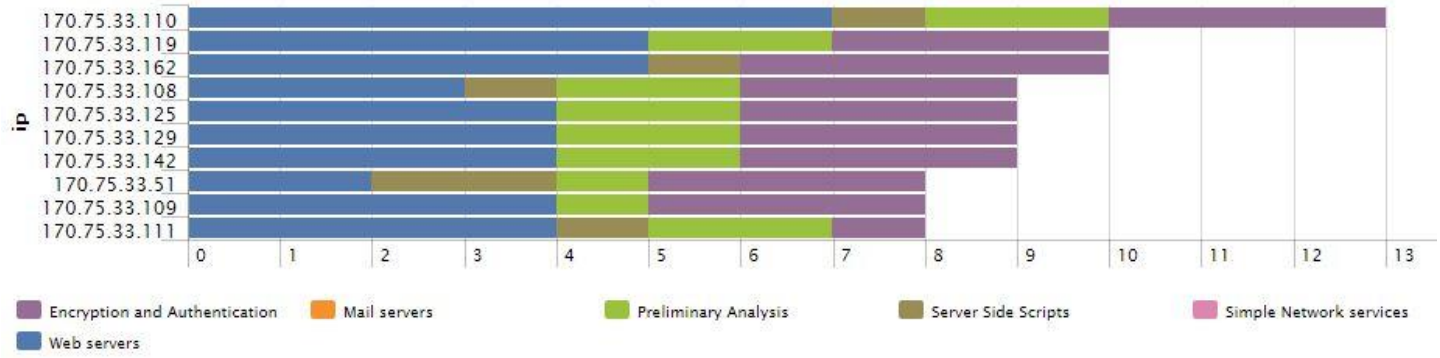

**Graph: Host by Vulnerability Name**

This report illustrates the vulnerability name and count by hosts discovered this report period



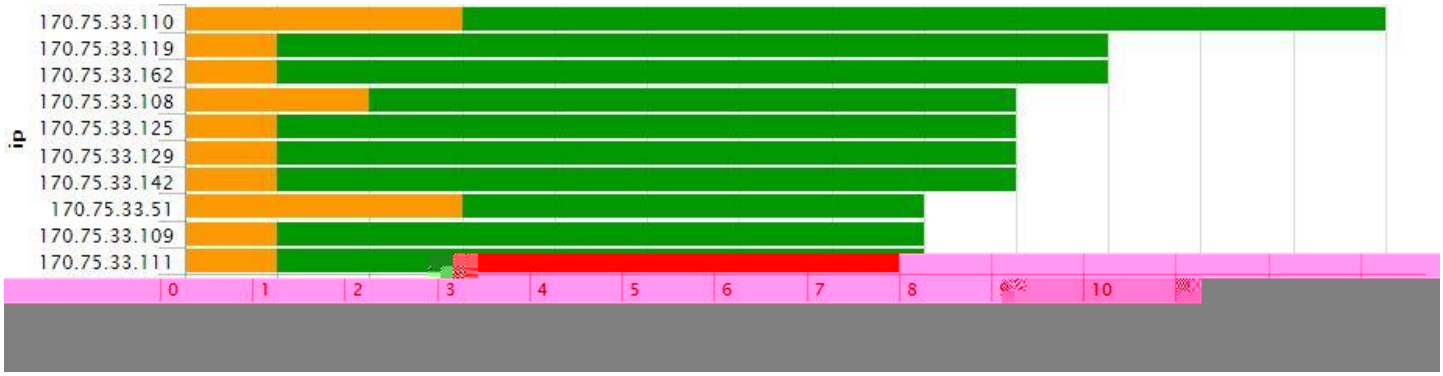

**Graph: Host by Vulnerability Category**

This report illustrates the vulnerability category and count by hosts discovered this report period



**Graph: Host by Vulnerability Risk**

This report illustrates the vulnerability risk and count by hosts discovered this report period

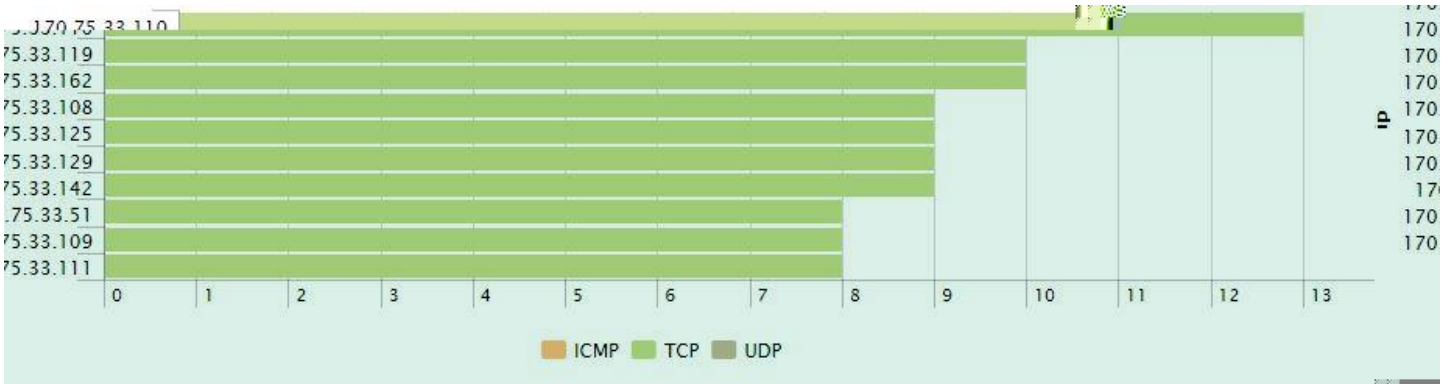



**Graph: Host by Port**

This report illustrates the port and count by hosts discovered this report period

**Graph: Host by Protocol**

This report illustrates the protocol and count by hosts discovered this report period



## *7. Security Operations*

The purpose of this section is to highlight the activities performed by GLESEC's Global Operations Center (GOC) including: monitoring availability and performance of equipment under contract, Change Management and Incident Response activities.

### a) Monitoring System Availability

**INSPIRA HEALTH NETWORK** DefensePro Availability:
The Bridgeton DefensePro 516 was considered up and available **100 %** during this report period.

**Host State Breakdowns:**

| State | Type / Reason | Time | % Total Time | % Known Time |
|---|---|---|---|---|
| UP | Unscheduled | 30d 0h 0m 0s | 100.000% | 100.000% |
| | Scheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Total | 30d 0h 0m 0s | 100.000% | 100.000% |
| DOWN | Unscheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Scheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Total | 0d 0h 0m 0s | 0.000% | 0.000% |
| UNREACHABLE | Unscheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Scheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Total | 0d 0h 0m 0s | 0.000% | 0.000% |
| Undetermined | Nagios Not Running | 0d 0h 0m 0s | 0.000% | |
| | Insufficient Data | 0d 0h 0m 0s | 0.000% | |
| | Total | 0d 0h 0m 0s | 0.000% | |
| All | Total | 30d 0h 0m 0s | 100.000% | 100.000% |

**State Breakdowns For Host Services:**

| Service | % Time OK | % Time Warning | % Time Unknown | % Time Critical | % Time Undetermined |
|---|---|---|---|---|---|
| PING | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| Average | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |

The Elmer DefensePro 516  was considered up and available **100 %** during this report period.

**Host State Breakdowns:**

| State | Type / Reason | Time | % Total Time | % Known Time |
|---|---|---|---|---|
| UP | Unscheduled | 30d 0h 0m 0s | 100.000% | 100.000% |
| | Scheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Total | 30d 0h 0m 0s | 100.000% | 100.000% |
| DOWN | Unscheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Scheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Total | 0d 0h 0m 0s | 0.000% | 0.000% |
| UNREACHABLE | Unscheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Scheduled | 0d 0h 0m 0s | 0.000% | 0.000% |
| | Total | 0d 0h 0m 0s | 0.000% | 0.000% |
| Undetermined | Nagios Not Running | 0d 0h 0m 0s | 0.000% | |
| | Insufficient Data | 0d 0h 0m 0s | 0.000% | |
| | Total | 0d 0h 0m 0s | 0.000% | |
| All | Total | 30d 0h 0m 0s | 100.000% | 100.000% |

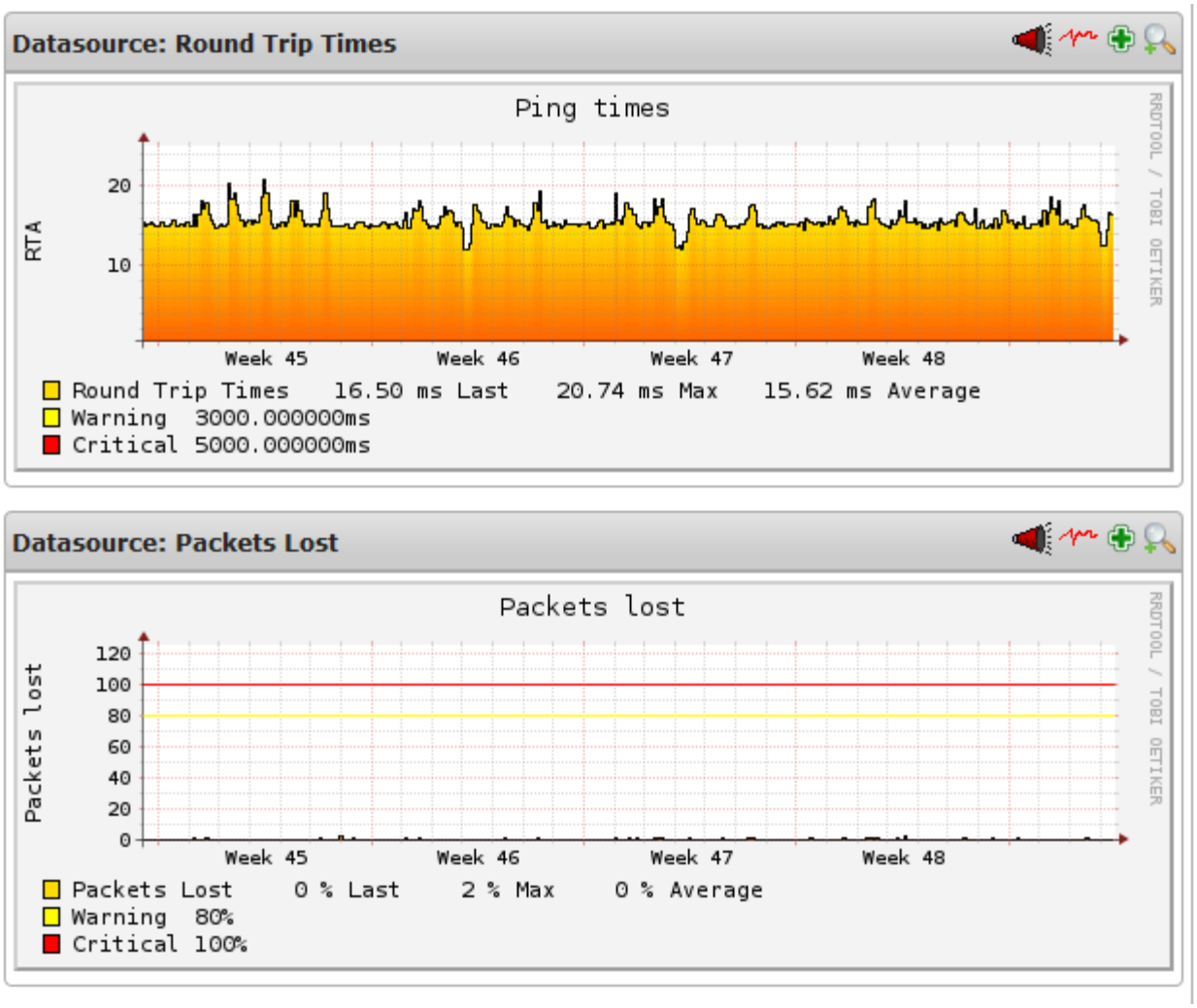
**State Breakdowns For Host Services:**

| Service | % Time OK | % Time Warning | % Time Unknown | % Time Critical | % Time Undetermined |
|---|---|---|---|---|---|
| PING | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |
| Average | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% |

## b) Monitoring system performance

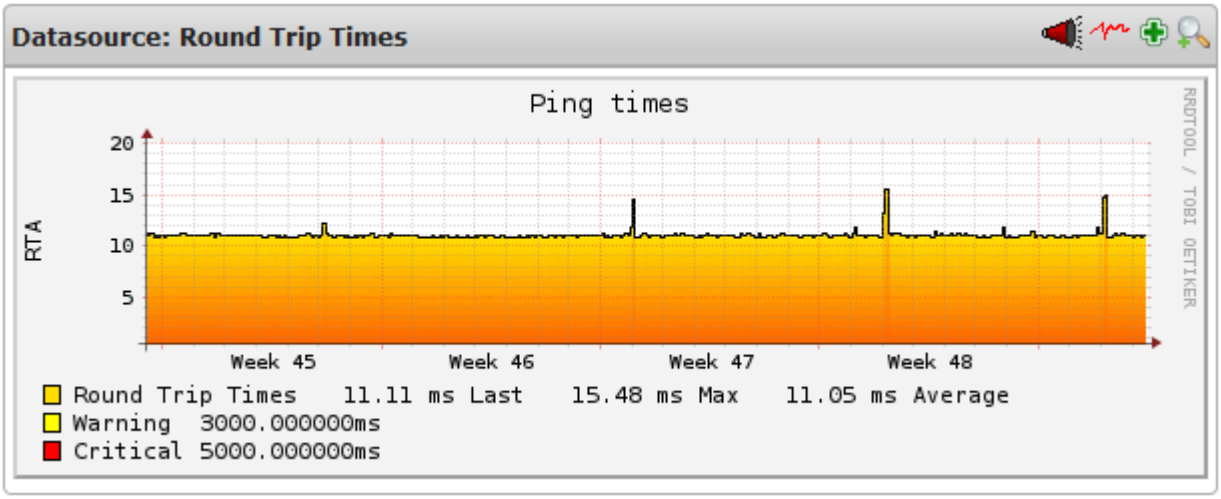
**INSPIRA HEALTH NETWORK** Bridgeton DefensePro 516 Host Performance

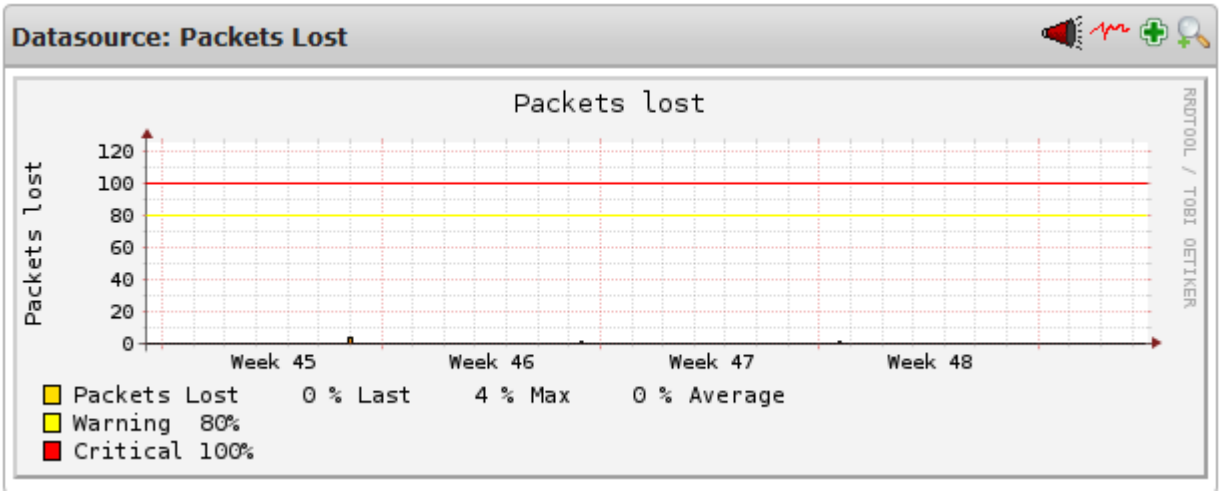
Round trip ping times averaged **15.62** ms from the GLESEC GOC to **INSPIRA HEALTH NETWORK** with **0 %** average packet loss.



**INSPIRA HEALTH NETWORK** Elmer DefensePro 516 Host Performance

Round trip ping times averaged **11.05**ms from the GLESEC GOC to **INSPIRA HEALTH NETWORK** with **0 %** average packet loss.



## c) Change Management

**No Change Management to report on June 2016**

## d) Incident Response

**No incident to report on June 2016**

## *8. Appendix 1 – Critical Attack Sources (WHOIS Information)*

This section provides additional WHOIS detail for the Graph: Critical Attacks

**inetnum:** **123.30.0.0 - 123.31.255.255**
netname: VDC-NET
country: vn
descr: VietNam Data Communication Company (VDC)
admin-c: VIG1-AP
tech-c: VIG1-AP
status: ALLOCATED NON-PORTABLE
changed: hm-changed@vnnic.net.vn 20090325
mnt-by: MAINT-VN-VNPT
source: APNIC

role: VDC IPADMIN GROUP
address: Internet Building, Block II, Thang Long Inter Village
address: Nguyen Phong Sac str, Cau Giay Dist, Ha Noi
country: VN
phone: +84-912-800008
fax-no: +84-4-9430427
e-mail: hathm@vdc.com.vn
remarks: send spam reports to abuse@vdc.com.vn
remarks: and abuse reports to abuse@vnn.vn
admin-c: THMH1-AP
tech-c: THMH1-AP
nic-hdl: VIG1-AP
notify: hm-changed@vnnic.net.vn
mnt-by: MAINT-VN-VNPT
changed: hm-changed@vnnic.net.vn 20090325
source: APNIC
changed: hm-changed@apnic.net 20111114

**inetnum:** **151.80.96.0 - 151.80.111.255**
netname: OVH
descr: OVH SAS
descr: Dedicated Servers Static IP

descr: http://www.ovh.com
country: FR
admin-c: OK217-RIPE
tech-c: OTC2-RIPE
status: LEGACY
mnt-by: OVH-MNT
changed: noc@ovh.net 20150401
created: 2015-04-01T14:14:23Z
last-modified: 2015-04-01T14:14:23Z
source: RIPE

role: OVH Technical Contact
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
e-mail: noc@ovh.net
admin-c: OK217-RIPE
tech-c: GM84-RIPE
tech-c: SL10162-RIPE
nic-hdl: OTC2-RIPE
notify: noc@ovh.net
abuse-mailbox: abuse@ovh.net
mnt-by: OVH-MNT
changed: noc@ovh.net 20101005
created: 2004-01-28T17:42:29Z
last-modified: 2014-09-05T10:47:15Z
source: RIPE

**NetRange: 104.192.0.0 - 104.192.3.255**
CIDR: 104.192.0.0/22
NetName: DATAWAGON
NetHandle: NET-104-192-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS27176
Organization: DataWagon LLC (DL-167)
RegDate: 2014-08-20

Updated: 2014-08-20
Comment: https://datawagon.net
Ref: http://whois.arin.net/rest/net/NET-104-192-0-0-1

OrgName: DataWagon LLC
OrgId: DL-167
Address: 3 Mead Pond Lane
City: Rye
StateProv: NY
PostalCode: 10580
Country: US
RegDate: 2014-03-04
Updated: 2014-08-21
Comment: https://datawagon.net
Ref: http://whois.arin.net/rest/org/DL-167

OrgAbuseHandle: ABUSE4637-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-914-715-3068
OrgAbuseEmail: abuse@datawagon.net
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE4637-ARIN

OrgNOCHandle: NOC31754-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-914-715-3068
OrgNOCEmail: noc@datawagon.net
OrgNOCRef: http://whois.arin.net/rest/poc/NOC31754-ARIN

OrgTechHandle: NOC31754-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-914-715-3068
OrgTechEmail: noc@datawagon.net
OrgTechRef: http://whois.arin.net/rest/poc/NOC31754-ARIN

**inetnum: 138.255.192/22**
aut-num: AS263971
abuse-c: LEVAL5
owner: FaleMais Comunicações LTDA

ownerid: 014.284.858/0001-30
responsible: Paulo Henrique Mem Pereira
country: BR
owner-c: LEVAL5
tech-c: LEVAL5
inetrev: 138.255.192/22
nserver: ns1.falemais.net.br
nsstat: 20151127 AA
nslastaa: 20151127
nserver: ns2.falemais.net.br
nsstat: 20151127 AA
nslastaa: 20151127
created: 20150831
changed: 20150831

nic-hdl-br: LEVAL5
person: Leonardo Valadares
e-mail: hostmaster@falemais.net.br
created: 20070102
changed: 20150520

**inetnum: 128.232.0.0 - 128.232.255.255**
netname: CL-CAM-AC-UK
descr: University of Cambridge Computer Laboratory
descr: 15 J J Thomson Avenue
descr: Cambridge CB3 0FD
country: GB
admin-c: PB22
admin-c: MAJ1
admin-c: PB3551-RIPE
tech-c: CLTC
org: ORG-UCAM1-RIPE
status: LEGACY
remarks: For information on "status:" attribute read
https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources
mnt-by: CL-CAM-AC-UK-MNT
mnt-lower: CL-CAM-AC-UK-MNT
mnt-routes: CL-CAM-AC-UK-MNT
mnt-domains: CL-CAM-AC-UK-MNT

mnt-by: CAM-AC-UK-MNT
mnt-by: JANET-HOSTMASTER
mnt-routes: JANET-HOSTMASTER
changed: tony@noc.ulcc.ac.uk 19911107
changed: hostmaster@ripe.net 20020807
changed: ipaddress@ukerna.ac.uk 20020923
changed: er-transfer@ripe.net 20040405
changed: ipaddress@ukerna.ac.uk 20050321
changed: hostmaster@cl.cam.ac.uk 20050322
changed: hostmaster@cl.cam.ac.uk 20050421
changed: hostmaster@cl.cam.ac.uk 20070313
changed: rcf34@cam.ac.uk 20150312
created: 2002-09-23T12:19:32Z
last-modified: 2015-05-05T02:00:51Z
source: RIPE

**NetRange: 107.180.0.0 - 107.180.127.255**
CIDR: 107.180.0.0/17
NetName: GO-DADDY-COM-LLC
NetHandle: NET-107-180-0-0-1
Parent: NET107 (NET-107-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS26496
Organization: GoDaddy.com, LLC (GODAD)
RegDate: 2014-02-11
Updated: 2014-02-25
Comment: Please send abuse complaints to abuse@godaddy.com
Ref: http://whois.arin.net/rest/net/NET-107-180-0-0-1

OrgName: GoDaddy.com, LLC
OrgId: GODAD
Address: 14455 N Hayden Road
Address: Suite 226
City: Scottsdale
StateProv: AZ
PostalCode: 85260
Country: US

RegDate: 2007-06-01
Updated: 2014-09-10
Comment: Please send abuse complaints to abuse@godaddy.com
Ref: http://whois.arin.net/rest/org/GODAD

OrgTechHandle: NOC124-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-480-505-8809
OrgTechEmail: noc@godaddy.com
OrgTechRef: http://whois.arin.net/rest/poc/NOC124-ARIN

OrgNOCHandle: NOC124-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-480-505-8809
OrgNOCEmail: noc@godaddy.com
OrgNOCRef: http://whois.arin.net/rest/poc/NOC124-ARIN

**NetRange: 104.192.0.0 - 104.192.3.255**
CIDR: 104.192.0.0/22
NetName: DATAWAGON
NetHandle: NET-104-192-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS27176
Organization: DataWagon LLC (DL-167)
RegDate: 2014-08-20
Updated: 2014-08-20
Comment: https://datawagon.net
Ref: http://whois.arin.net/rest/net/NET-104-192-0-0-1

OrgName: DataWagon LLC
OrgId: DL-167
Address: 3 Mead Pond Lane
City: Rye
StateProv: NY
PostalCode: 10580
Country: US
RegDate: 2014-03-04

Updated: 2014-08-21
Comment: https://datawagon.net
Ref: http://whois.arin.net/rest/org/DL-167

OrgNOCHandle: NOC31754-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-914-715-3068
OrgNOCEmail: noc@datawagon.net
OrgNOCRef: http://whois.arin.net/rest/poc/NOC31754-ARIN

OrgAbuseHandle: ABUSE4637-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-914-715-3068
OrgAbuseEmail: abuse@datawagon.net
OrgAbuseRef: http://whois.arin.net/rest/poc/ABUSE4637-ARIN

OrgTechHandle: NOC31754-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-914-715-3068
OrgTechEmail: noc@datawagon.net
OrgTechRef: http://whois.arin.net/rest/poc/NOC31754-ARIN

**inetnum: 183.182.84.0 - 183.182.87.255**
netname: RPNET-IN
descr: RAJESH PATEL NET SERVICES PVT LTD
country: IN
admin-c: AP343-AP
tech-c: AP343-AP
status: ALLOCATED PORTABLE
mnt-by: MAINT-IN-IRINN
mnt-lower: MAINT-IN-RPNET
mnt-routes: MAINT-IN-RPNET
mnt-irt: IRT-RPNET-IN
changed: hm-changed@apnic.net 20130919
source: APNIC

irt: IRT-RPNET-IN
address: 10/5 M.G. ROAD
address: INDORE M.P. 452001
address: INDIA

e-mail: rajesh@rpnspl.com
abuse-mailbox: akshar@rpnspl.com
admin-c: AP343-AP
tech-c: AP343-AP
auth: # Filtered
mnt-by: MAINT-IN-RPNET
changed: hm-changed@apnic.net 20130919
source: APNIC

person: AKSHAR PATEL
nic-hdl: AP343-AP
e-mail: akshar@rpnspl.com
address: 10/5 M.G. ROAD
address: INDORE M.P. 452001
address: INDIA
phone: +91-9826709002
country: IN
changed: rajeshkumargpatel@gmail.com 20091128
mnt-by: MAINT-NEW
source: APNIC

route: 183.182.85.0/24
descr: RAJESH PATEL NET SERVICES PVT LTD
origin: AS131276
mnt-by: MAINT-IN-RPNET
changed: rajeshkumargpatel@gmail.com 20091221
source: APNIC

route: 183.182.85.0/24
descr: RAJESH PATEL NET SERVICES PVT LTD
origin: AS55353
mnt-by: MAINT-IN-RPNET
changed: rajeshkumargpatel@gmail.com 20091221
source: APNIC
Tools

**NetRange: 141.212.121.0 - 141.212.121.255**
CIDR: 141.212.121.0/24
NetName: UMICH-21024
NetHandle: NET-141-212-121-0-1
Parent: UMICH-2 (NET-141-212-0-0-1)
NetType: Reassigned

status: ASSIGNED PA
mnt-by: MNT-PIN
mnt-by: MNT-PINSUPPORT
org: ORG-CL291-RIPE
mnt-routes: ROOT-MNT
changed: admin@pinspb.ru 20131026
created: 2013-10-26T11:25:36Z
last-modified: 2015-01-21T18:09:00Z
source: RIPE

organisation: ORG-CL291-RIPE
org-name: CubeHost Ltd.
org-type: OTHER
address: 51, 102 Vienna Street,
address: Ras Al Khaimah
address: United Arab Emirates
phone: +971-7-226-9235
abuse-c: CN3142-RIPE
e-mail: info@cubehost.biz
abuse-mailbox: info@cubehost.biz
mnt-ref: MNT-PINSUPPORT
mnt-by: CUBEHOST-MNT
changed: info@cubehost.biz 20150121
created: 2015-01-21T15:33:45Z
last-modified: 2015-01-21T18:08:43Z
source: RIPE

role: CubeHost NOC
address: 51, 102 Vienna Street,
address: Ras Al Khaimah
address: United Arab Emirates
abuse-mailbox: abuse@cubehost.biz
e-mail: info@cubehost.biz
nic-hdl: CN3142-RIPE
mnt-by: CUBEHOST-MNT
changed: info@cubehost.biz 20150121
created: 2015-01-21T15:36:58Z

last-modified: 2015-01-21T15:36:58Z
source: RIPE

## *9. Appendix 2 – Top Scanners Blocked (WHOIS Information)*

This section provides additional WHOIS detail for the Graph: Top Scanners Blocked (Source IP Addressed)

**inetnum: 188.138.9.0 - 188.138.9.255**
descr: BSB-SERVICE Dedicated Server Hosting
netname: BSB-SERVICE-1
country: DE
admin-c: NPA10-RIPE
tech-c: NPA10-RIPE
status: ASSIGNED PA
mnt-by: intergenia-mnt
mnt-lower: bsb-service-mnt
changed: ripe@intergenia.de 20141114
created: 2012-10-31T09:40:10Z
last-modified: 2014-11-14T08:56:19Z
source: RIPE

role: NMC PlusServer AG
address: PlusServer AG
address: Daimlerstr. 9-11
address: 50354 Huerth
phone: +49 1801 119991
fax-no: +49 2233 612-53500
e-mail: nmc@intergenia.de
abuse-mailbox: abuse@plusserver.de
remarks:
remarks: **********
remarks: * Auskunftsersuchen gemaess TKG werden nur unter
remarks: * Fax: +49 2233 612 5165
remarks: * Mail: legal at intergenia punkt de
remarks: * bearbeitet!

remarks: **********
remarks:
admin-c: JBPS-RIPE
tech-c: ADPS-RIPE
nic-hdl: NPA10-RIPE
mnt-by: INTERGENIA-MNT
created: 2007-12-10T16:02:37Z
last-modified: 2015-10-14T12:18:35Z
source: RIPE

**inetnum: 212.47.228.0 - 212.47.239.255**
netname: POPS-NAS
descr: Tiscali France
country: FR
admin-c: BG34
admin-c: LTAD1-RIPE
tech-c: TTFR1-RIPE
status: ASSIGNED PA
remarks: **********
remarks: All abuse requests MUST be sent to ' abuse@tiscali.fr '
remarks: and the logs must include the timezone and GMT offset.
remarks: ripe-mnt@net.tiscali.fr IS NOT the mail to use to report abuses
remarks: Toute requete abuse DOIT etre envoyee a ' abuse@tiscali.fr '
remarks: en les logs doivent inclure l'heure exacte et le decalage GMT.
remarks: ripe-mnt@net.tiscali.fr N'EST PAS le mail a utiliser pour signaler un abuse.
remarks: **********
notify: ripe-mnt@net.tiscali.fr
mnt-by: MNT-TISCALIFR
mnt-lower: MNT-TISCALIFR
changed: ripe-mnt@net.tiscali.fr 20030415
changed: ripe-mnt@net.tiscali.fr 20031217
remarks: Tag: Int
created: 2002-09-24T15:24:31Z
last-modified: 2003-12-17T20:06:40Z

source: RIPE

role: LIBERTYSURF TELECOM ABUSE DEPARTMENT
remarks: now known as Online S.A.S. / Iliad-Entreprises
address: 8, rue de la ville l'eveque
address: 75008 Paris
address: France
e-mail: abuse@iliad-entreprises.fr
admin-c: IENT-RIPE
tech-c: IENT-RIPE
nic-hdl: LTAD1-RIPE
mnt-by: MNT-TISCALIFR
changed: ripe-mnt@net.tiscali.fr 20030416
changed: nlimage+ripe@online.net 20121105
created: 2002-09-24T15:24:32Z
last-modified: 2012-11-05T16:06:32Z
source: RIPE

**inetnum: 46.228.192.0 - 46.228.207.255**
netname: DE-FASTIT-20110208
descr: myLoc managed IT AG
country: DE
org: ORG-fIG1-RIPE
admin-c: DTH
tech-c: DTH
status: ALLOCATED PA
notify: hostmaster@fastit.net
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: FASTIT-MNT
mnt-lower: FIBRE1-MNT
mnt-lower: MYLOC-MNT
mnt-routes: FASTIT-MNT
mnt-routes: FIBRE1-MNT
changed: hostmaster@ripe.net 20110208

created: 2011-02-08T14:10:41Z
last-modified: 2011-02-08T14:10:41Z
source: RIPE

organisation: ORG-fIG1-RIPE
org-name: myLoc managed IT AG
org-type: LIR
address: Am Gatherhof 44
address: 40472
address: Duesseldorf
address: GERMANY
phone: +4921161708110
fax-no: +4921161708111
e-mail: hostmaster@myloc.de
admin-c: DTH
admin-c: MST
mnt-ref: FASTIT-MNT
mnt-ref: RIPE-NCC-HM-MNT
mnt-ref: MYLOC-MNT
mnt-by: RIPE-NCC-HM-MNT
abuse-c: MOPS-RIPE
abuse-mailbox: abuse@myloc.de
created: 2004-04-17T11:07:16Z
last-modified: 2015-10-21T13:01:12Z
changed: bitbucket@ripe.net 20151021
source: RIPE

**inetnum: 193.105.134.0 - 193.105.134.255**
netname: SWEDENDEDICATED-NET
descr: Christian Maurice Sebastiaan Hein
remarks: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
remarks: !! All abuse to info@swedendedicated.com !!
remarks: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
country: SE

org: ORG-SD20-RIPE
admin-c: CH446-RIPE
tech-c: CH446-RIPE
status: ASSIGNED PI
notify: info@swedendedicated.com
mnt-by: RIPE-NCC-END-MNT
mnt-by: MNT-SWEDEDI
mnt-by: MNT-PORTLANE
mnt-routes: MNT-SWEDEDI
mnt-routes: MNT-PORTLANE
mnt-domains: MNT-SWEDEDI
changed: hostmaster@ripe.net 20100217
created: 2010-02-17T13:13:28Z
last-modified: 2015-05-05T02:08:08Z
source: RIPE
sponsoring-org: ORG-PS39-RIPE
changed: hostmaster@ripe.net 20141210
changed: hostmaster@ripe.net 20150409

organisation: ORG-SD20-RIPE
org-name: Christian Maurice Sebastiaan Hein
org-type: OTHER
address: Sweden Dedicated Land�v�gen 8 66060 Molkom
e-mail: info@swedendedicated.com
abuse-mailbox: abuse@swedendedicated.com
mnt-ref: MNT-SWEDEDI
mnt-by: MNT-SWEDEDI
created: 2010-02-08T09:52:29Z
last-modified: 2015-04-07T04:10:16Z
source: RIPE
changed: info@swedendedicated.com 20100214

**inetnum: 31.6.70.0 - 31.6.71.255**
netname: LIVENET

descr: Livenet sp. z o.o.
descr: Grodzka 1
descr: 42-600 Tarnowskie Gory Poland
descr: contact: bok@slaskdatacenter.pl +48 324508888
descr: Abuse contact: bok@slaskdatacenter.pl
country: PL
admin-c: MP22024-RIPE
tech-c: MP22024-RIPE
status: ASSIGNED PA
changed: tomek@sitel.net.pl 20121205
mnt-by: sitelnetpl-mnt
created: 2012-12-05T11:27:18Z
last-modified: 2012-12-05T11:27:18Z
source: RIPE

person: Michal Piech
address: ul. Grodzka1
address: 42-600 Tarnowskie Gory, Poland
phone: +48 324508888
phone: +48 535331463
e-mail: bok@slaskdatacenter.pl
nic-hdl: MP22024-RIPE
mnt-by: sitelnetpl-mnt
changed: tomek@sitel.net.pl 20110805
created: 2011-08-04T22:05:00Z
last-modified: 2011-08-04T22:10:59Z
source: RIPE

**inetnum: 202.75.32.0 - 202.75.63.254**
netname: TM-VADS-DC
descr: TM VADS DC Hosting
country: MY
admin-c: MSS13-AP
tech-c: SLMY1-AP

status: ALLOCATED NON-PORTABLE
notify: idc@vads.com
mnt-by: MAINT-MY-EASTGATE
mnt-lower: MAINT-MY-EASTGATE
mnt-routes: MAINT-MY-EASTGATE
mnt-irt: IRT-EASTGATE-MY
changed: msobri@tmnet.com.my 20110527
source: APNIC

irt: IRT-EASTGATE-MY
address: 3rd Floor, TM IT Complex
address: 3300 Lingkaran Usahawan 1 Timur
address: 63000 Cyber Jaya Selangor
e-mail: idc@vads.com
abuse-mailbox: abuse@netmyne.com
admin-c: MSS13-AP
tech-c: SLMY1-AP
auth: # Filtered
mnt-by: MAINT-MY-EASTGATE
changed: hm-changed@apnic.net 20101116
source: APNIC

**inetnum: 185.94.108.0 - 185.94.111.255**
netname: RU-QRATOR-20150331
descr: HLL LLC
country: RU
org: ORG-LA267-RIPE
admin-c: QL-RIPE
tech-c: QL-RIPE
status: ALLOCATED PA
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: MNT-QRATOR
mnt-routes: MNT-QRATOR
changed: hostmaster@ripe.net 20150331

changed: hm-changed@vnnic.net.vn 20090325
mnt-by: MAINT-VN-VNPT
source: APNIC

role: VDC IPADMIN GROUP
address: Internet Building, Block II, Thang Long Inter Village
address: Nguyen Phong Sac str, Cau Giay Dist, Ha Noi
country: VN
phone: +84-912-800008
fax-no: +84-4-9430427
e-mail: hathm@vdc.com.vn
remarks: send spam reports to abuse@vdc.com.vn
remarks: and abuse reports to abuse@vnn.vn
admin-c: THMH1-AP
tech-c: THMH1-AP
nic-hdl: VIG1-AP
notify: hm-changed@vnnic.net.vn
mnt-by: MAINT-VN-VNPT
changed: hm-changed@vnnic.net.vn 20090325
source: APNIC
changed: hm-changed@apnic.net 20111114

## *10. Appendix 3 Glossary of Terms*

**Amplification Attack**
An Amplification Attack is any attack where an attacker is able to use an amplification factor to multiply its power. Amplification attacks are “asymmetric”, meaning that a relatively small number or low level of resources is required by an attacker to cause a significantly greater number or higher level of target resources to malfunction or fail. Examples of amplification attacks include Smurf Attacks (ICMP amplification), Fraggle Attacks (UDP amplification), and DNS Amplification.
**Botnet**
A botnet is a collection of compromised computers often referred to as “zombies” infected with malware that allows an attacker to control them. Botnet owners or “herders” are able to control the machines in their botnet by means of a covert channel such as IRC (Internet Relay

Chat), issuing commands to perform malicious activities such as distributed denial-of-service (DDoS) attacks, the sending of spam mail, and information theft. As of 2006, the average size of any given botnet around the world was around 20,000 machines (as botnet owners attempted to scale down their networks to avoid detection), although some larger more advanced botnets such as BredoLab, Conficker, TDL-4, and Zeus have been estimated to contain millions of machines.

**Computer Emergency Readiness Team Computer Emergency Response Team Computer Security Incident Response Team**

Computer Emergency Response Team is a name given to expert groups that handle computer security incidents. Most groups append the abbreviation CERT or CSIRT to their designation where the latter stands for Computer Security Incident Response Team.

**DDoS (Distributed Denial-of-Service) Attack**

DDoS or Distributed Denial-of-Service attacks are a variant of Denial-of-Service DoS attacks where an attacker or a group of attackers employ multiple machines to carry out a DoS attack simultaneously, therefore increasing its effectiveness and strength. The "army" carrying out the attack is mostly often composed of innocent infected zombie computers manipulated as bots and being part of a botnet controlled by the attacker via a Command and Control Server. A botnet is powerful, well coordinated and could count millions of computers. It also insures the anonymity of the original attacker since the attack traffic originates from the bots' IPs rather than the attacker's. In some cases, mostly in ideological DDoS attacks, this "army" could also be composed of recruited hackers/hacktivits participating in large DDoS attack campaigns (Operation Blackout, Operation Payback etc.). DDoS attacks are hard to detect and block since the attack traffic is easily confused with legitimate traffic and difficult to trace.

There are many types of DDoS attacks targeting both the network and the application layers. They could be classified upon their impact on the targeted computing resources (saturating bandwidth, consuming server's resources, exhausting an application) or upon the targeted resources as well:

- Attacks targeting Network Resources: UDP Floods, ICMP Floods, IGMP Floods.
- Attacks targeting Server Resources: the TCP/IP weaknesses –TCP SYN Floods, TCP RST attacks, TCP PSH+ACK attacks – but also Low and Slow attacks as Sockstress for example and SSL-based attacks, which detection is particularly challenging.
- Attacks targeting the Application Resources: HTTP Floods, DNS Floods and other Low and Slow attacks as Slow HTTP GET requests (Slowloris) and Slow HTTP POST requests (R-U-Dead-Yet).

A DDoS attack usually comprises more than three attack vectors thus increasing the attacker's chances to hit its target and escape basic DoS mitigation solutions.

**DoS (Denial-of-Service) Attack**

A Denial-of-Service DOS attack is an attack targeting the availability of web applications. Unlike other kinds of attacks, DoS attacks' primary goal is not to steal information but to slow

or take down a web site. The attackers' motivations are diverse, ranging from simple fun, to financial gain and ideology (hacktivism). A DoS attack generates high or slow rate attack traffic exhausting computing resources of a target, therefore preventing legitimate users from accessing the website. DoS attacks affect enterprises from all sectors (e-gaming, Banking, Government etc.), all sizes (mid/big enterprises) and all locations. They target the network layer and up to the application layer, where attacks are more difficult to detect since they could easily get confused with legitimate traffic. There are several types of DoS attacks. A (non-distributed) DoS attack is when an attacker uses a single machine's resources to exhaust those of another machine, in order to prevent it from functioning normally. Large Web servers are usually robust enough to withstand a basic DoS attack from a single machine without suffering performance loss. A DoS attack famous variant is the DDoS or Distributed Denial of Service attack where the attack originates from multiple computers simultaneously, therefore causing the victim's resources exhaustion.

**DNS Amplification Attack**

DNS amplification attack is a sophisticated denial of service attack that takes advantage of DNS servers' behavior in order to amplify the attack. In order to launch a DNS amplification attack, the attacker performs two malicious tasks. First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address. This will cause all DNS replies from the DNS servers to be sent to the victim's servers. Second, the attacker finds an internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. This results in large replies from the DNS servers, usually so big that they need to be split over several packets. Using very few computers, the attacker sends a high rate of short DNS queries to the multiple DNS servers asking for the entire list of DNS records for the internet domain it chose earlier. The DNS servers look for the answer and provide it to the DNS resolver. However, because the attacker spoofed the IP address of the DNS resolver and set it to be the IP address of the victim, all the DNS replies from the servers are sent to the victim. The attacker achieves an amplification effect because for each short DNS query it sends, the DNS servers reply with a larger response, sometimes up to 100 times larger. Therefore, if the attacker generates 3 Mbps of DNS queries, it is actually amplified to 300Mbps of attack traffic on the victim. The victim is bombed with a high rate of large DNS replies where each reply is split over several packets. This requires the victim to reassemble the packet, which is a resource consuming task, and to attend to all of the attack traffic. Soon enough, the victim's servers become so busy handling the attack traffic that they cannot service any other request from legitimate users and the attacker achieves a denial-of-service.

**DNS Flood**

A DNS Flood is an application-specific variant of a UDP flood. Since DNS servers use UDP traffic for name resolution, sending a massive number of DNS requests to a DNS server can

consume its resources, resulting in a significantly slower response time for legitimate DNS requests.

**Exploit**

An exploit is an implementation of a vulnerability meant to allow one to actually compromise a target. Exploits can be difficult to develop, as most modern vulnerabilities are much more complex than older ones due to the existence of advanced security measures and complicated constructs in modern hardware and software. Exploits based on previously unknown vulnerabilities, known as “Zero-Day” exploits are highly sought after by hackers and developers and manufacturers alike. By using a zero-day exploit, a hacker can guarantee that his or her attempt to break into a particular computer or device that possesses such vulnerability that the exploit is based on will succeed. Zero-day exploits are traded on both the black market and through legitimate middlemen between legitimate parties from anywhere between $5,000 to $250,000 depending on the effects of the exploit and which system they target. Where a PDF exploit might only fetch a few thousand dollars, a severe exploit targeting the latest version of Apple’s mobile operating system, iOS, might fetch $100,000 or more.

**Flood**

“Flood” is the generic term for a denial-of-service (DoS) attack in which the attacker attempts to constantly send traffic (often high volume of traffic) to a target server in an attempt to prevent legitimate users from accessing it by consuming its resources. Types of floods include (but are not limited to): HTTP floods, ICMP floods, SYN floods, and UDP floods.

**Hacker**

The term “hacker” has been used to mean various things in the world of computing: one who is able to subvert computer security (regardless of intentions), one who is a member of the open-source software community and subculture, and one who attempts to push the limits of computer software and hardware through home modifications. In the world of computer security, the term “hacker” is often portrayed as negative by mass media, despite the prevalence of “white hat hacking”, or ethical hacking for the purpose of discovering potential security flaws and reporting them to the proper individuals or organizations so that the flaws may be patched. Black hat hacking, on the other hand, is the breaking into computer systems without any intention of reporting discovered vulnerabilities, often with malicious or financial incentives. The hackers who fall somewhere on the spectrum between “white hats” and “black hats” are referred to as “grey hats”. Grey hat hackers will often perform mischievous activities with (usually non-malicious although at times questionably ethical) motivations. Additionally, grey hat hackers often choose not to report security flaws to the proper channels; rather, they report such information to the hacking community and the general public, enjoy watching the fallout as those with the security flaws scramble to fix them before they can be abused by black hat hackers. Within the open-source software and computer hobbyist communities, however, “hacker” usually has a less negative connotation. Within

these cultures, hackers are often individuals regarded as intelligent and clever, and able to come up with creative solutions to existing problems that a software or hardware product developer may have not thought of or publicly released yet. These hackers often refer to “hackers” within the computer security world as “crackers” (as in safe-cracker) to emphasize their belief that calling such individuals “hackers” is incorrect. With the rise of hacker and “hacktivist" groups such as LulzSec (now LulzSec Reborn) and Anonymous, the mass media portrayal of the term “hacker” continues to lead the general public to believe “hacker” is synonymous with “cybercriminal”.

**Hacktivist**

“Hacktivist”, a portmanteau of “hack” and “activism”, was a term coined in 1996 by Omega, a member of the hacking coalition “Cult of the Dead Crow” (cDc). The term can be loosely defined as, “the ethically ambiguous use of computers and computer networks in order to affect the normal operation of other systems, motivated by a desire to protest or promote political ends.”Oftentimes these events take the form of web site defacements, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, typo squatting, and virtual sabotage. The term has become popular among media outlets in recent years due to the rise of various politically motivated cyber attacks by groups such as Anonymous and LulzSec (now LulzSec Reborn) on governments and corporations across the world.

**Honeypot**

In computer security, a honeypot is a program or a server voluntarily made vulnerable in order to attract and lure hackers. The attackers who think they are targeting a real resource behave “normally”, using their attack techniques and tools against this lure site, which allow the defenders to observe and monitor their activities, analyze their attacking methods, learn and prepare the adequate defenses for the real resources. There are several kinds of honeypots, some used for research purposes only while others are actively acting as defenses for the real sites.

**HTTP Flood**

An HTTP flood is an attack method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a target web server. These requests are specifically designed to consume a significant amount of the server’s resources, and therefore can result in a denial-of-service condition (without necessarily requiring a high rate of network traffic). Such requests are often sent en masse by means of a botnet, increasing the attack’s overall power. HTTP flood attacks may be one of the most advanced non-vulnerability threats facing web servers today. It is very hard for network security devices to distinguish between legitimate HTTP traffic and malicious HTTP traffic, and if not handled correctly, it could cause a high number of false-positive detections. Rate-based detection engines are also not successful at detecting HTTP flood attacks, as the traffic volume of HTTP floods may be under detection thresholds. Because of this, it is necessary to use several parameters detection including rate-based and rate-invariant.

**I2P**

I2P is an anonymous overlay network - a network within a network. It is intended to protect communication from dragnet surveillance and monitoring by third parties such as ISPs.

**ICMP Flood**

Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood - the sending of an abnormally large number of ICMP packets of any type (especially network latency testing “ping” packets) - can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

**Internet pipe saturation**

These attacks are volumetric floods and often involve flooding the target with an overwhelming bandwidth. Common attacks utilize UDP as it is easily spoofed and difficult to mitigate downstream. Out of state, SYN floods and malformed packets are also often seen. While many attacks aim at saturating inbound bandwidth, it’s not uncommon for attackers to identify and pull large files from websites, ftp shares, etc. in order to saturate outbound bandwidth as well.

**IP Address**

An IP address is an identifier for a device connected to a network using TCP/IP - a protocol that routes network traffic based on the IP address of its destination. IP addresses can either be 32-bit IPv4 addresses consisting of four base-10 numbers separated by periods representing eight digit binary (base-2) numbers called “octets” (i.e. 0.0.0.0 to 255.255.255.255), or 128-bit IPv6 addresses consisting of eight hexadecimal (base-16) numbers separated by colons representing sixteen digit binary (base-2) numbers (i.e. 0000:0000:0000:0000:0000:0000:0000:0000 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF where consecutive groups of four zeroes are replaced by a double colon). When the Internet first became popular, IPv4, with its 32-bit addresses, offered 232, or roughly 4.3 x 109 unique addresses. As the number of Internet-connected devices began to grow significantly, people worried that the IPv4 protocol would not contain enough addresses to meet the growing demand for new unique addresses this is why IPv4 will eventually be replaced by IPv6 on a large scale (IPv6 already officially launched in August 2012), which contains 2128 or roughly 3.4 x 1038 unique addresses. The Dynamic Host Configuration Protocol (DHCP), which runs on special devices (usually routers) allows for the assigning of IP addresses within a local area network (LAN). DHCP assigns IP addresses on a temporary “lease” basis; once a device’s IP address lease expires, a DHCP server will assign it a new (potentially different) one. IP addresses automatically assigned by a DHCP server are therefore referred to as “dynamic IP addresses”, as a device with a DHCP-assigned IP address may eventually receive an IP different from its original one.

DHCP servers will not assign devices just any IP address in the maximum range of IPv4 addresses (0.0.0.0 to 255.255.255.255), as certain IP addresses are reserved for special purposes. Such addresses include:

- 0.0.0.0 – Represents the "default" network, i.e. any connection
  255.255.255.255 – Represents the broadcast address, or place to route messages to be sent to every device within a network
- 127.0.0.1 – Represents "localhost" or the "loopback address", allowing a device to refer to itself, regardless of what network it is connected to
- 169.254.X.X – Represents a "self-assigned IP address", which a device will assign itself if it is unable to receive an IP address from a DHCP server

Users' DHCP-assigned IP addresses on a LAN are not the same as their "external" or Internet IP address. This address will be the same for all users connected to a DHCP server, which itself receives an IP address from the Internet Service Provider (ISP) it is connected to. As IP addresses can be used as unique identifiers for users' machines (and subsequently the users themselves), knowledge of a malicious user's external Internet IP address can allow law enforcement officials to block, locate, and eventually arrest him or her. As a result, the more advanced attack tools and hackers will employ anonymization techniques - such as the use of proxy servers, VPNs, or a routing network like Tor or I2P - that can make it seem like they are using a different IP address other than their own, located somewhere else in the world. An attack tool called Low Orbit Ion Cannon (LOIC) became infamous for not hiding its users' IP addresses; this resulted in the arrest of various LOIC users around the world for their participation in distributed denial-of-service (DDoS) attacks.

**IP Spoofing**

IP Spoofing is the act of creating an IP packet with a forged source IP address for the purpose of hiding the true source IP address, usually for the purpose of launching special types of distributed denial-of-service (DDoS attacks). By forging the source IP address of a packet; the individual sending it can direct the target IP address' machine to send its reply packet somewhere other than the real IP address of the source machine. Those wishing to launch DDoS attacks without large botnets can therefore send packets with random spoofed source IP addresses in order to both conceal their own identity and make the attack harder to block (as it looks like it is originating from many sources).

**IRC (Internet Relay Chat)**

IRC (Internet Relay Chat) is a protocol for real-time text messaging between internet-connected computers created in 1988. It is mainly used for group discussion in chat rooms called "channels" although it supports private messages between two users, data transfer, and various server-side and client-side commands. As of April 2011, the top 100 IRC networks served over 500,000 users at a time on hundreds of thousands of channels. IRC is a popular method used by botnet owners to send commands to the individual computers in their botnet. This is done either on a specific channel, on a public IRC network, or on a separate IRC

server. The IRC server containing the channel(s) that are used to control bots is referred to as a “command and control” or C2 server.

**ISP (Internet Service Provider)**

An Internet Service Provider (ISP) is a company that provides internet access for its customers. ISPs are required by law in many countries to provide a certain level of monitoring capabilities to aid government law enforcement and intelligence agencies, and are often asked by such officials to intervene during cyber attacks by cutting off internet service to the offending machines.

**itsoknoproblembro**

The 'itsoknoproblembro' tool was designed and implemented as a general purpose PHP script injected into a victim’s machine allowing the attacker to upload and execute arbitrary Perl scripts on the target’s machine. The 'itsoknoproblembro' script injects an encrypted payload, in order to bypass IPS and Malware gateways into the website main file index.php, allowing the attacker to upload new Perl scripts at any time. Initial server infection is usually done by using the well known Remote File Inclusion (RFI) technique. By uploading Perl scripts that run different DOS flood vectors, the server might act as a Bot in a DDOS Botnet army. Although originally designed for general purpose, some variants of this tool found in the wild were customized to act as a proprietary DDOS tool, implementing the flood vector logics inside without the need to upload additional scripts.

**Malware**

“Malware”, short for “malicious software”, is any program designed to help a hacker negatively affect the normal operation of a computer. Most forms of malware - including viruses, worms, Trojan horses, spyware, adware, and rootkits - are intended to allow hackers to gain unauthorized access to a machine, without the knowledge of its owner, in order to perform criminal tasks including information theft and amassing botnets to perform distributed denial-of-service (DDoS) attacks. Computer users are often tricked into installing malware through social engineering techniques, or are unaware that a seemingly non-malware infected program they have installed was infected, containing additional code designed to stealthily perform malicious tasks.

**MSSP**

An MSSP (Managed Security Service Provider) is an organization which provides "Security as a Service" (Sec-aaS) and may include elaborate operations such as SOCs and NOCs, or something as simple as a cloud-based key management service. Generally speaking, an MSSP is considered an outsourced operation of what was an internal security device or process management function.

**Network scan**

Scanning is typically an automated process that is used to discover devices such as pc, server and peripherals that exist on a network. Results can include details of the discovered devices, including IP addresses, device names, operating systems, running applications/services, open

shares, usernames and groups. Scanning is often related to pre -attack or reconnaissance activities. There are two types of scanning: Horizontal Scan in which the scanner scans for the same port on multiple IPs, and Vertical Scan in which the scanner scans multiple ports on one IP.

**Packet**

A packet is a formatted unit of data used to transmit information piece by piece across a packet switched network. Packets usually contain three sections: a header, the payload, and a trailer (also called "footer"). A packet header contains information such as the length of the packet (if the network does not use a predetermined fixed packet size), synchronization bits to help the packet match up with the network, a packet number to differentiate each packet from the others, the protocol (i.e. type of information contained within the packet), and the source and destination IP addresses. The "payload" of a packet contains the actual information being transmitted. The trailer or "footer" usually contains a series of bits signaling to the receiving device that it has reached the end of the packet, as well as some type of error-checking information to ensure that the packet was not modified in transit.

**Port Scan**

A port scanner is a technical leverage to identify available technical services (ports) on a server or application and may include logic to evaluate whether or not those services are vulnerable to common exploits or configuration issues. This is done by sending predetermined traffic to the target and based on a response or lack of a response, the port scanner in use makes its own conclusions with regards to the functionality of the port being scanned.

**Reflector/Reflective DoS attacks**

Reflection Denial of Service attacks makes use of a potentially legitimate third party component to send the attack traffic to a victim, ultimately hiding the attackers' own identity. The attackers send packets to the reflector servers with a source IP address set to their victim's IP therefore indirectly overwhelming the victim with the response packets.

The reflector servers used for this purpose could be ordinary servers not obviously compromised, which makes this kind of attack particularly difficult to mitigate. A common example for this type of attack is Reflective DNS Response attack.

**SIP Brute Force**

SIP brute force is an adaptation of normal brute force attacks which attack SIP servers and attempt access to servers to make unauthorized outbound calls at another's expense.

**SIP Client Call Flood**

This is a flood technique focused on SIP application protocol which involves illegitimate call requests. The idea here is to flood the Session Boarder Control (SBC) and / or SIP / VOIP PBX with too many requests to handle and thus making the service unavailable.

**SIP Malformed Attack**

Application layer attack on the Session Initiation Protocol- SIP in use in VoIP services, targeted at causing denial of service to SIP servers. A SIP malformed attack consists of sending any kind of non-standard messages (malformed SIP Invite for ex) with an intentionally invalid input, therefore making the system unstable.

**SIP Register flood**

Application layer attack on the Session Initiation Protocol- SIP in use in VoIP services, targeted at causing denial of service to SIP servers. A SIP Register flood consists of sending a high volume of SIP REGISTER or INVITE packets to SIP servers (indifferently accepting endpoint requests as first step of an authentication process), therefore exhausting their bandwidth and resource

**SIP Server Flood**

Application layer attack on the Session Initiation Protocol- SIP (in use in VoIP services), targeted denial of service to SIP servers. Common attack vectors include SIP invite and register floods.

**Scrubbing Center**

A centralized data cleansing station where traffic is analyzed and malicious traffic (ddos, known vulnerabilities and exploits) is removed. Scrubbing centers are often used in large enterprises, such as ISP and Cloud providers, as they often prefer to off-ramp traffic to an out of path centralized data cleansing station. When under attack, the traffic is redirected (typically using DNS or BGP) to the scrubbing center where an attack mitigation system mitigates the attack traffic and passes clean traffic back to the network for delivery. The scrubbing center should be equipped to sustain high volumetric floods at the network and application layers, low and slow attacks, RFC Compliance checks, known vulnerabilities and zero day anomalies.

**Social Engineering**

Social Engineering (within the context of computer security) is the act of using psychological manipulation in order to gain access to sensitive information, computers, or computer networks. Many famous computer hackers (both white hat and black hat) have used social engineering in combination with computer-related methods in order to gain information; reformed cyber criminal Kevin Mitnick admitted that it's much easier to trick a person into giving up sensitive passwords or information than it is to obtain the same material solely through the use of computers. One example of a social engineering technique is "pretexting", or engaging the target subject in a specific manner with some form of background information that makes it more likely that he or she will divulge sensitive information. Pretexting often involves extensive research, as the social engineer will need to prepare answers to identifying questions that he or she may be asked during the process of obtaining information. This newly obtained information can often be used in further pretexting

attempts, especially in scenarios where the social engineer wishes to gain even greater access to his or her target.

**SQL Injection**

SQL injection is an attack targeting web applications taking advantage of poor application coding where the inputs are not sanitized therefore exposing application vulnerabilities. SQL injection is the most famous type of injection attacks which also count LDAP or XML injections. The idea behind a sql injection is to modify an application SQL (database language) query in order to access or modify unauthorized data or run malicious programs. Most web applications indeed rely on databases where the application data is stored and being accessed by SQL queries and modifications of these queries could mean taking control of the application. An attacker would for example be able to access the application database with administrator access, run remote commands on the server, drop or create objects in the database and more.

For instance, the sql query below, aiming at authenticating users, is common in web applications:

- myQuery= ”SELECT * FROM userstable WHERE username = 'userinput1' and password ='userinput2';”
- Replacing userinput1 by: ‘OR 1=1’); -- would result in granting the attacker access to the database without knowing the real username and password as the assertion “1=1” is always true and the rest of the query is being ignored by the comment character (- - in our case).
- Replacing the userinput1 by ' OR 1=1"); drop table users;-- would additionally drop the application users table.

**SYN Flood**

A SYN flood is a denial-of-service (DoS) attack that relies on abusing the standard way that a TCP connection is established. Typically, a client sends a SYN packet to an open port on a server asking for a TCP connection. The server then acknowledges the connection by sending SYN-ACK packet back to the client and populating the client’s information in its Transmission Control Block (TCB) table. The client then responds to the server with an ACK packet establishing the connection. This process is commonly known as a “three-way handshake”. A SYN flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target machine to attempt to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. A server under a SYN flood attack will continue to wait for a SYN-ACK packet for each connection request, as the delay could be normal and related to network congestion. However, because a SYN-ACK packet never arrives for any of the connection requests; the massive number of half-open connections quickly fills up the server’s TCB table before it can time any connections out. This process continues for as long as the flood attack continues. Attackers will sometimes add legitimate information to their requests as well, such as

sequence number or source port 0, as this increases a target server's CPU usage on top of causing network congestion, and could more effectively cause a denial-of-service condition.

**TCP Flood**

TCP SYN floods are one of the oldest yet still very popular Denial of Service (DoS) attacks. The most common attack involves sending numerous SYN packets to the victim. The attack in many cases will spoof the SRC IP meaning that the reply (SYN+ACK packet) will not come back to it. The intention of this attack is overwhelm the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP; this is perhaps the biggest strength of the attack.

**Tor**

Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

**UDP Flood**

A UDP flood is a network flood and still one of the most common floods today. The attacker sends UDP packets, typically large ones, to single destination or to random ports. In most cases the attackers spoof the SRC IP which is easy to do since the UDP protocol is "connectionless" and does not have any type of handshake mechanism or session. The main intention of a UDP flood is to saturate the Internet pipe. Another impact of this attack is on the network and security elements on the way to the target server, and most typically the firewalls. Firewalls open a state for each UDP packet and will be overwhelmed by the UDP flood connections very fast.

**Vulnerability**

A vulnerability (in computer security) is any weakness in a computer system, network, software, or any device that allows one to circumvent security measures and perform actions not intended by its developers or manufacturers. Vulnerabilities range from minor to major, with the most significant allowing for privilege escalation (unauthorized administrator or root privileges) or code execution (the running of unsigned 3rd party software). New vulnerabilities can often be discovered by the process of "fuzzing", or purposely trying to break something by attempting to give it unreasonable input values. Once some kind of crash occurs and can be analyzed, one can discover the existence of a vulnerability that may have not been previously documented. Previously unknown vulnerabilities, known as "Zero-Day"

vulnerabilities are highly sought after by hackers and developers and manufacturers alike. By using an exploit based on zero-day vulnerability, a hacker can guarantee that his or her attempt to break into a particular computer or device that possesses such vulnerability will succeed. Zero-day exploits are traded on both the black market and through legitimate middlemen between parties for anywhere from $5,000 to $250,000 depending on the effects of the exploit and which system they target. Where a PDF exploit might only fetch a few thousand dollars, a severe exploit targeting the latest version of Apple's mobile operating system, iOS, might fetch $100,000 or more.

**Vulnerability Scanner**

A vulnerability scanner is a type of computer program used to gather information on computers and systems on a network in order to find their weaknesses. By using a vulnerability scanner tool such as nmap or unicornscan, one can determine the number of clients attached to a particular network as well as various information regarding their addresses, ports, applications and services and potential exploits that can be used against them. Some scanners offer the ability to deploy payloads for the purpose of using a found exploit, and others simply display information on network topology. Types of vulnerability scanners include: port scanners, network enumerators, network vulnerability scanners, web application security scanners, database security scanners, ERP security scanners, and computer worms (which require scanning capabilities to spread within a network).

**Wireshark**

Wireshark is a free cross-platform open-source network traffic capture and analysis utility. It began as a project called "Ethereal" in the late 1990s, but its name was changed to "Wireshark" in 2006 due to trademark issues. The initial code was written by Gerald Combs, a computer science graduate of the University of Missouri-Kansas City, today the Wireshark website now lists over 600 contributors. The program is GUI-based and uses pcap to capture packets, although there is also a command-line version of Wireshark called TShark with the same functionality. Wireshark essentially "understands" the formats of various types of network packets, and is able to display the header and content information of captured packets in an easy-to-read format with various filtering options. Packets can be either captured directly with Wireshark, or captured with a separate utility and later viewed within Wireshark. As a powerful (and free) network analysis tool, Wireshark has become an industry standard utility for network traffic analysis.

**Zeus**

Zeus is a well-known Trojan Horse that steals financial information from a user's browser using man-in-the-browser key logging and form grabbing. Additionally, Zeus installs a backdoor on the machines it infects, so these machines can become part of a botnet used for distributed denial-of-service (DDoS) attacks and other malicious activities. Zeus was first detected in 2007 when it was used to attack the United States Department of Transportation, however, it did not become significantly widespread until March 2009. Attacks involving the

use of Zeus occurred throughout 2010, including an October 2010 attack by a large organized crime ring attempting to steal over $70M from individuals in the US with Zeus-infected computers. The FBI made over 90 arrests of suspected members in the US, and various others were arrested in the UK and Ukraine in connection with the attack. In May 2011 the source code of the version used then of Zeus (v2) was leaked, leading to various customized Zeus-based bots being created. Some of the more advanced custom bots based on the leaked code (such as Ice IX) attempted to fix many of the existing issues with Zeus rendering it even harder to detect. However, many security researchers have discovered that even the most well-known custom versions are extremely similar to the original leaked Zeus source code, and are therefore not significantly more innovative or dangerous.

**Zero-Day/Zero-Minute Attack**

A Zero-Day (or Zero-Minute) Attack is a type of attack that uses a previously unknown vulnerability. Because the attack is occurring before "Day 1" of the vulnerability being publicly known, it is said that the attack occurred on "Day 0" - hence the name. Zero-Day exploits are highly sought after - often bought and sold by private firms anywhere from $5,000 to $250,000, depending on what applications and operating systems they target - as they almost guarantee that an attacker is able to stealthily circumvent the security measures of his or her target. Private security firms aside, software vendors will also usually offer a monetary reward among other incentives to report zero-day vulnerabilities in their own software directly to them.

**Zombie**

A "zombie" or "bot" is a compromised computer under the control of an attacker who often controls many other compromised machines that together make up a botnet. The term "zombie" was coined to describe such an infected computer because the computer's owner is often not aware that his or her computer is being used for malicious activities.

## References

http://security.radware.com/knowledge-center/DDoSPedia/

*Your Global e-Security Partner*

*www.glesec.com*
*info@glesec.com*

**United States**

Worldwide Corporate HQ
Address. 66 Witherspoon Street
Princeton, NJ 08542
Tel. 609.651.4246

**Panama**

Central America HQ
Address. Edificio Century Tower
El Dorado, 1th Floor D-12
Panama City, Panama
Tel. +507.836.5355

**Argentina**

South America HQ
+54.11.5917.6120

**Brazil**

+55.11.3711.5699

**Chile**

+56.2938.1496

**Peru**

+51.1708.7197

**Mexico**

+52.55.5018.1164