Operations and Intelligence

Inspira Health Network

December 2017

BEST IN CLASS – INFORMATION SECURITY

INTELLIGENCE AND OPERATIONS

Table of Contents

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	Service Expiration
MSS-APS	Radware	DefensePro 516 ODS2-S1 Bridgeton	1/1/18
MSS-APS	Radware	DefensePro 516 ODS2-S1 Elmer	1/1/18
MSS-VME			1/1/18

4. Executive Summary

This report corresponds to the period from 1 December to 31 December 2017.

This month we see a decrease of **161**% in attack activity from prior month and an increase of **91**% in critical attacks over the prior month with several attacks of more than one hour of duration. This may be in part due to the fact that for a week we did not have visibility of attacks thru Bridgeton which is the most active of the two sites. This occurred due to the process of upgrade and reversing the upgrade of the Radware DefensePro system. Most attacks are targeting multiple ports followed by port **1433** (ms-sql) and port **23** (telnet), attacks.

The geographical distribution of the attacks this month is: **Russian Federation, United States, Chile, China, Netherlands Germany, United Kingdom, France, Ukraine, and Brazil.**
The biggest attacks on your site are from Russian Federation, originating approx. **31.65**% of total attacks for this month.

The bulk of the attacks, **75.69 %** are packet anomalies which are specifically crafted to target firewalls and other network infrastructure. These are usually a more active reconnaissance stage in which after foot printing to gain an idea of the network structure is now actively crafting attacks against identified targets. The DefensePro is able to recognize and block this type of attack effectively.

There are **6** vulnerable hosts out of **59** hosts. The vulnerabilities in December are **17** medium vulnerabilities and **7** low to a total of **22** total.

The list below indicate your vulnerability most frequent:
General vulnerabilities are the most prevalent vulnerability category with 15 detected vulnerabilities followed by Misc with 3, Service Detection with 2, and Windows with 1 for the

report period.

The DefensePro Elmer system has operated properly with 100% up time and good performance.

External Network Vulnerabilities

External 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%, 75%, 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 these values (100, 75, 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	
59			6	
Risk Distribution				
Critical	High	Medium	Low	Total
0	0	15	7	22

According to the metrics:
RV= 0.037904468

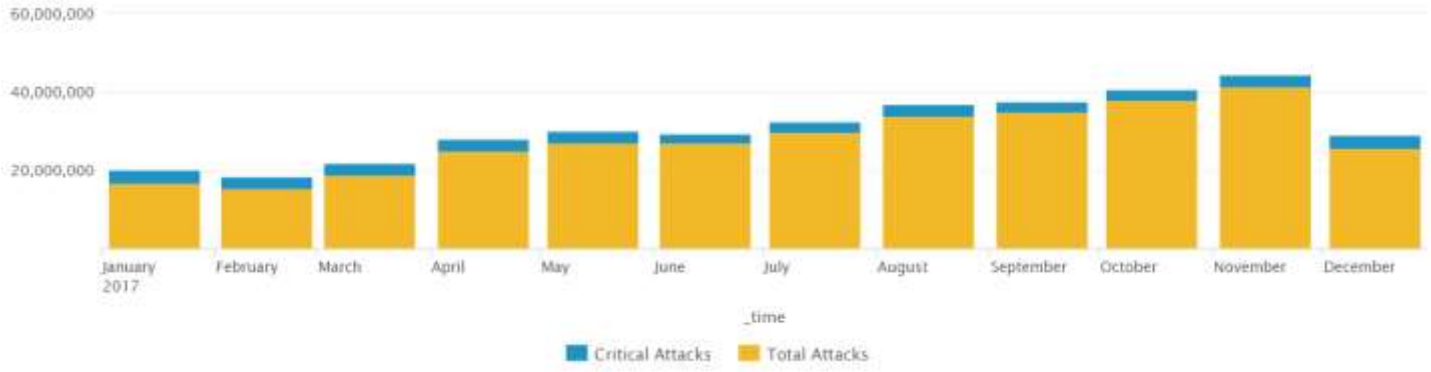
The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

Attack Summary

Based on the information gathered from the DefensePro during this period **25,753,535** attacks on Inspira Health Network **3,332,512** of which were considered critical were all stopped by the radware devices.

Inspira Health Network annual average is **25,837,550** total attacks and **2,720,088** critical attacks on a monthly basis this equates to an average of **915,227** total daily attacks and **96,352** critical daily attacks. As the graph illustrates total attack levels in relation to the previous report period totaled **41,575,804** total attacks and critical attacks in compared with a last period's total of **3,031,566.**

This statistical graph provides the count of critical and total attacks blocked per month calculated on a rolling 12 month period (Last 12 months). Note that this month there is an anomaly since the Bridgeton DefensePro was not available 100% of the time due to maintenance activities.

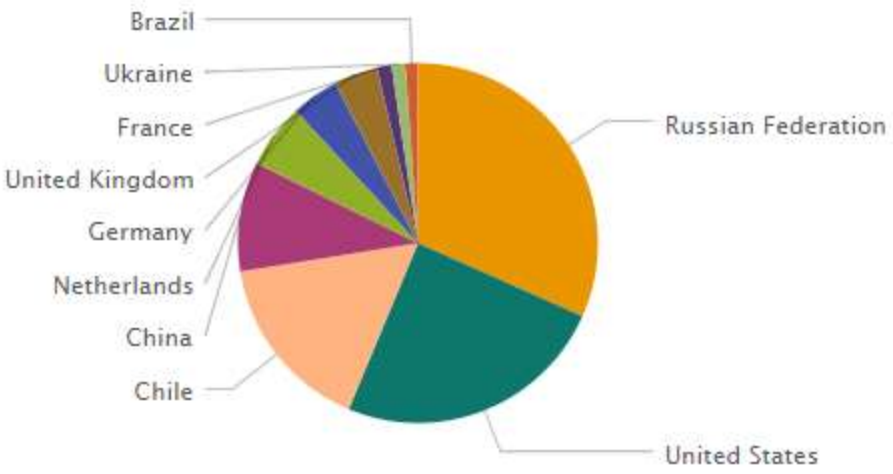


Comparison of previous month with month actual.

Description	November	December
Total Attack	41,575,804	25,753,535
Critical Attacks	3,031,566	3,332,512
Monthly attack average	25,151,515	25,837,550
Daily Attack Average	890,926	915,227
Monthly Critical attack average	2,750,180	2,720,088
Daily Critical Attack Average	97,418	96,352

Geography

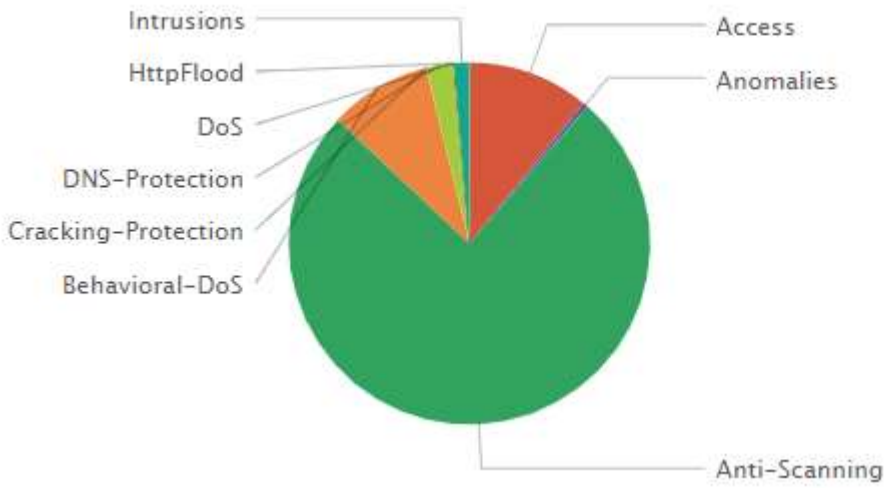
The vast majority of attacks on **Inspira Health Network** originated geographically from the following Top 10 countries**: Russian Federation, United States, Chile, China, Netherlands Germany, United Kingdom, France, Ukraine, and Brazil**. Listed in order of frequency. The attacks that we observed are 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 75.69 % 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 1.36 % 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 0.43 % 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 10.87 % of attacks during this report period

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

Denial of Service accounted for 0.053 % of attacks during this report period

Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server with requests and data. Depending on the nature of your enterprise, this can effectively disable your organization.

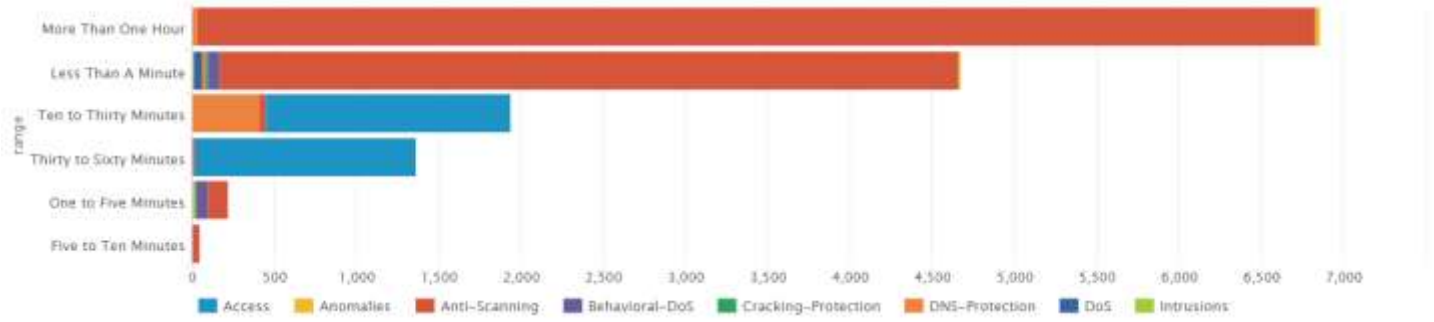
Behavioral-DoS accounted for 9.14 % of attacks during this report period

The B-DoS system protects against Network Flood Attacks, which cause a great deal of irrelevant traffic to fill available network bandwidth, denying the use of network resources to legitimate users.

Network Flood protection types include: SYN Flood, TCP Flood, UDP Flood, ICMP Flood, IGMP Flood

Duration

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



Bandwidth

Behavioral-DoS dropped 123.10 Gbps, Access protection dropped 138.24 Gbps, Intrusion protection dropped 15.52 Gbps of total traffic, 1.32 Gbps dropped by Packet Anomaly protection rules, Anti-Scanning protection dropped 54.82 Gbps, and a total of 491.71 Gbps of malicious traffic was discarded this period.

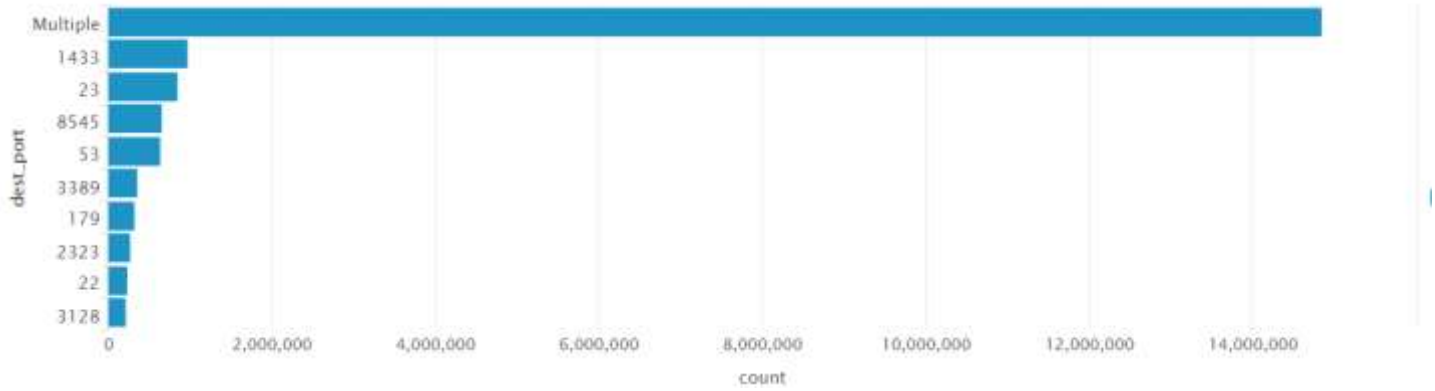
Category	Gbps	Mbps
DNS-Protection	158.51	162318.71
Access	138.24	141559.87
Behavioral-DoS	123.10	126055.46
Anti-Scanning	54.82	56138.22
Intrusions	15.52	15891.32
Anomalies	1.32	1350.84
DoS	0.18	189.12
Cracking-Protection	0.02	17.55
Total Bandwidth in Gbps/Mbps	491.71	503521.09

*Please view the , **Graph: Bandwidth by Blocked Threat Category by Hour of Day** and **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: multiple, 1433 (ms-sql), 23 (telnet), 8545(Rpc), 53(Dns) ,3389(Rdp),179(Bgp),2323(3d-nfsd),3128(tcp), in order of frequency for this report period.



Port number information utilized is based on and additional outside sources are used to illustrate the relationship to commonly exploited attacks vectors.

*Please view the **Port Information**, and available in the Security Intelligence section of the report.

External Vulnerabilities

The following network ranges for Inspira Health Network was scanned for vulnerabilities.
170.75.48.0/20 and 170.75.32.0/20

A total of **59** hosts were scanned **6** of which were found to be vulnerable.

Vulnerabilities were detected for the following host IPs:

Host	Critical	High	Medium	Low	Total
170.75.33.136			4	2	6
170.75.33.139			4	2	6
170.75.32.15			3	2	5
170.75.33.4			2	0	2
170.75.49.35			1	1	2
170.75.33.118			1	0	1

Vulnerability –Current Month and Previous Month
A comparison of persistent vulnerabilities of the current month and previous month.

host-ip	Previous Month	Current Month
170.75.32.15	5	5
170.75.33.118		1
170.75.33.134	7	
170.75.33.136	7	6
170.75.33.137	7	
170.75.33.139	7	6
170.75.33.140	2	
170.75.33.158	3	
170.75.33.4	2	2
170.75.49.35	7	2

Please view **Recommendations** for more details.

External Risk Distribution

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

Based on the information gathered from the GLESEC MSS-VME a total of **22** Vulnerabilities were found which consisted of **0** High Risk Vulnerabilities during this period, **15** Medium Risk Vulnerabilities and **7** Low Risk Vulnerabilities.

Name	Critical	High	Medium	Low	Total
Inspira Health Network			15	7	22

High risk vulnerabilities accounted for 0 % 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 68.18 % 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 31.81% 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:

General vulnerabilities are the most prevalent vulnerability category with 15 detected vulnerabilities followed by Misc with 3**,** Service Detection with 2, and Windows with 1 for the report period.

Name	Critical	High	Medium	Low	Total
General			12	3	15
Misc			0	3	3
Service detection			2	0	2
Web Servers			0	1	1
Windows			1	0	1

General vulnerabilities accounted for 68.18% of the discoveries during this report period

A set of checks that gather information about the remote system such as operating system and service identification, network connectivity, and more.

Service Detection vulnerabilities accounted for 9.09 % of the discoveries during this report period

Security checks that allow Nessus to detect a wide variety of services on a remote host.

Misc. vulnerabilities accounted for 13.63 % of the discoveries during this report period

Plugins that test for a wide variety of software including client-side and server issues.

Windows vulnerabilities accounted for 4.54 % of the discoveries during this report period

Checks for software installed on Microsoft Windows systems including Adobe Reader, Adobe Flash, Antivirus software, web browsers, iTunes, and much more

5. Recommendations for External Vulnerabilities

GLESEC recommends for Inspira Health Network to address the following vulnerabilities assigned a **Medium** Risk by the MSS-VME.

Description

SSL Certificate Cannot Be Trusted

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Systems Affected

Port	Host
4443 / tcp / www	170.75.33.136, 170.75.33.139
25 / tcp / smtp	170.75.33.4

Solution

Purchase or generate a proper certificate for this service.

Description

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.)

Systems Affected

Port	Host
443 / tcp / www	170.75.32.15
4443 / tcp / www	170.75.33.136, 170.75.33.139

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Description

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Systems Affected

Port	Host
4443 / tcp / www	170.75.33.136, 170.75.33.139
443 / tcp / www	170.75.32.15

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

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:

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)

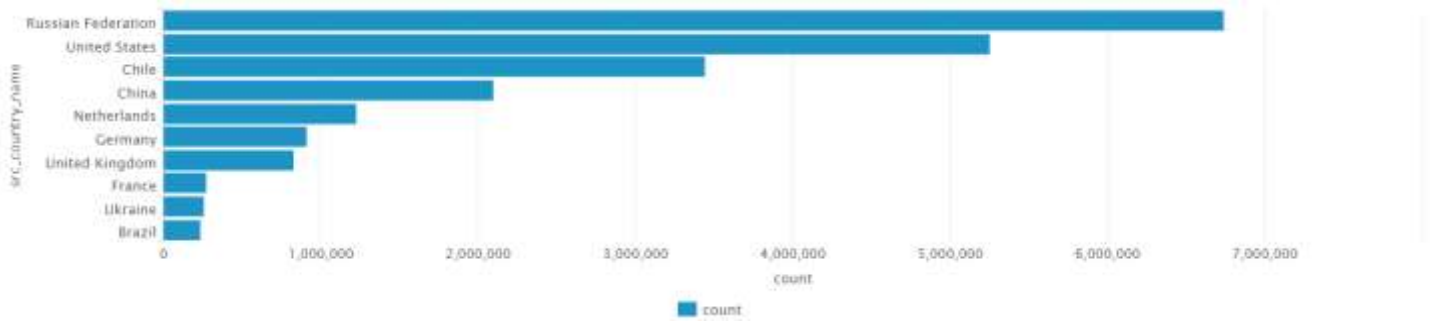
6. Security Intelligence

The purpose of this section is to highlight intelligence gathered from the services 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 **Russian Federation, United States, Chile, China, Netherlands Germany, United Kingdom, France, Ukraine, and Brazil**. Listed in order of frequency.

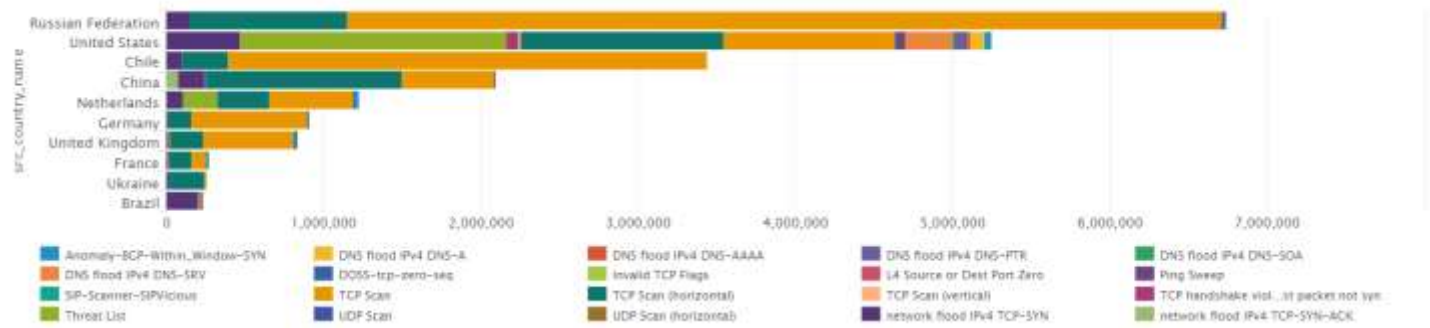
The attacks that we observed are happening to companies all around the world. Some results do not include location information that allows map plotting.

Graph: Top 10 Attacking Countries Blocked
This report provides the count of total attacks blocked by country



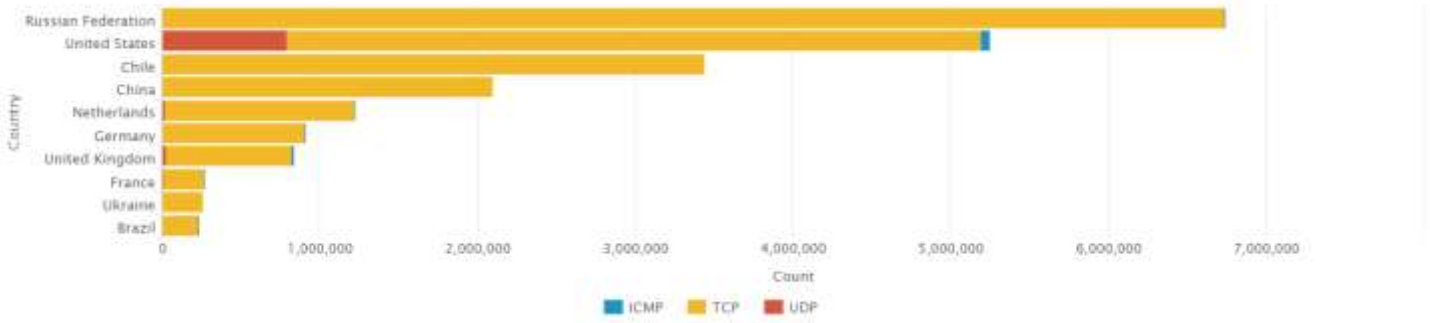
Graph: Top 10 Attacking Countries Blocked by Attack Type

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



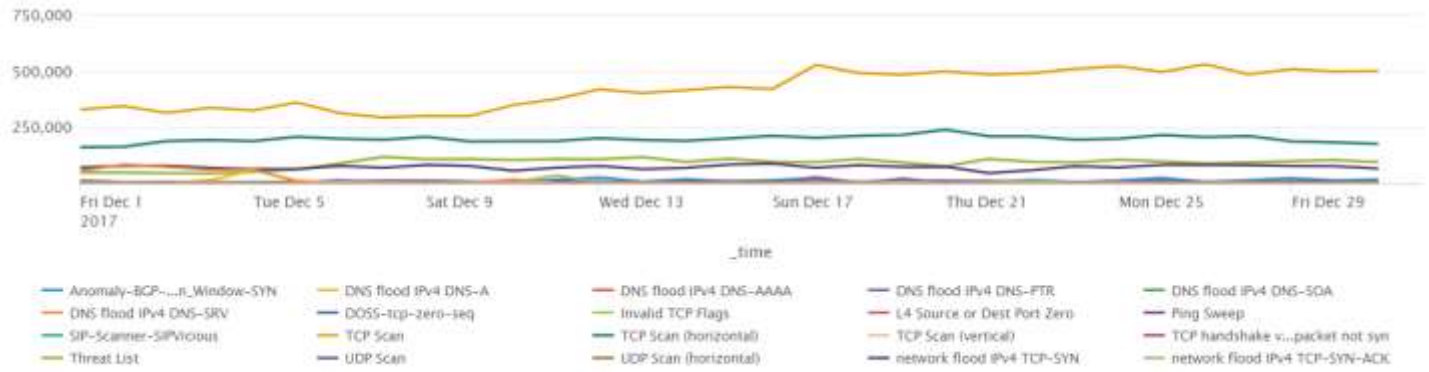
Graph: Top 10 Attacking Countries Blocked by Protocol

This report provides the count of attack protocols blocked by country



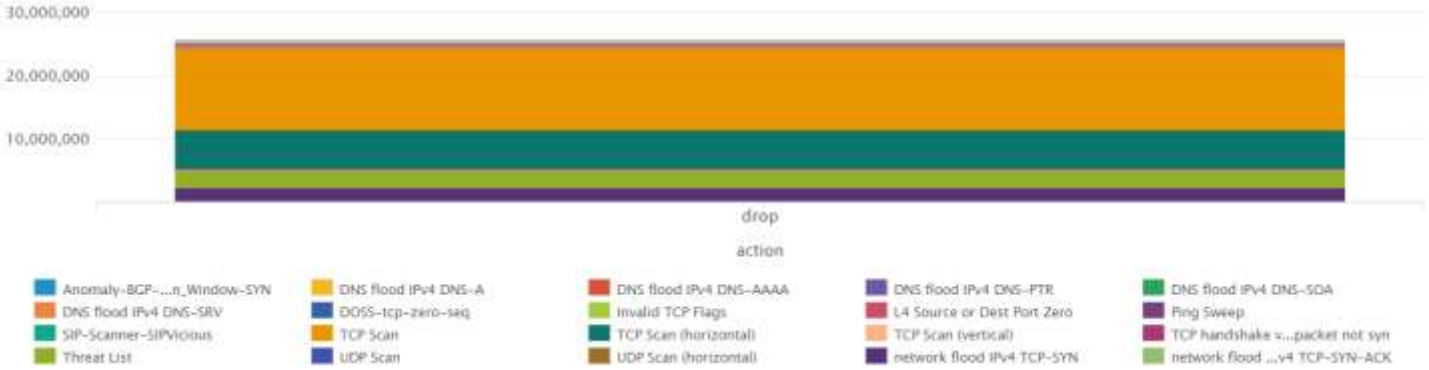
Graph: Attacks Types Blocked by Week

This report provides the count of attacks blocked by week



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.

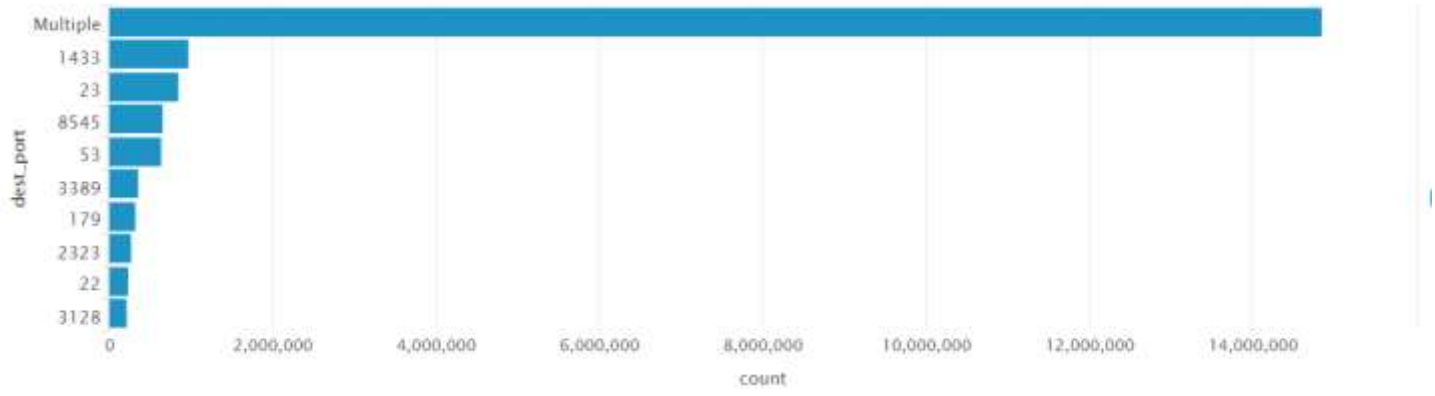
Web based forms must allow some access to your database to allow entry of data and a response, so this kind of attack bypasses firewalls and endpoint defenses. Any web form, even a simple logon form or search box, might provide access to your data by means of SQL injection if coded incorrectly.

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

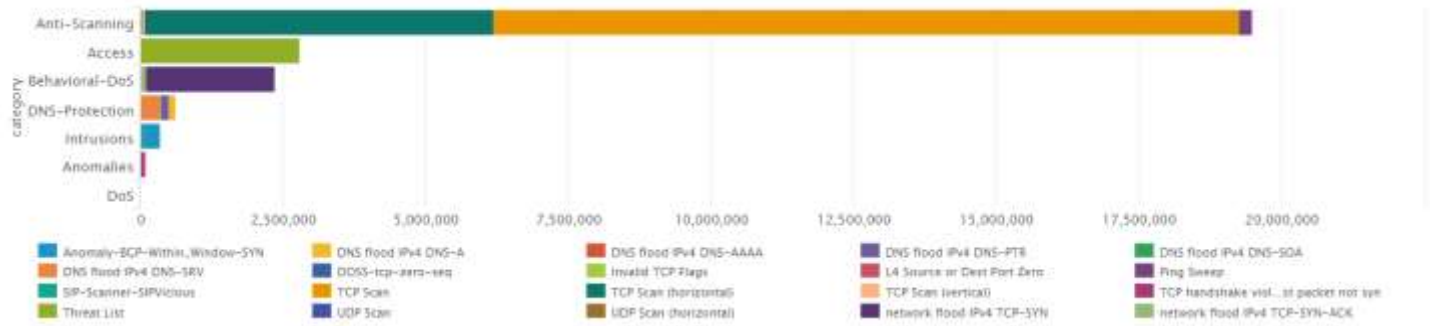
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

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.

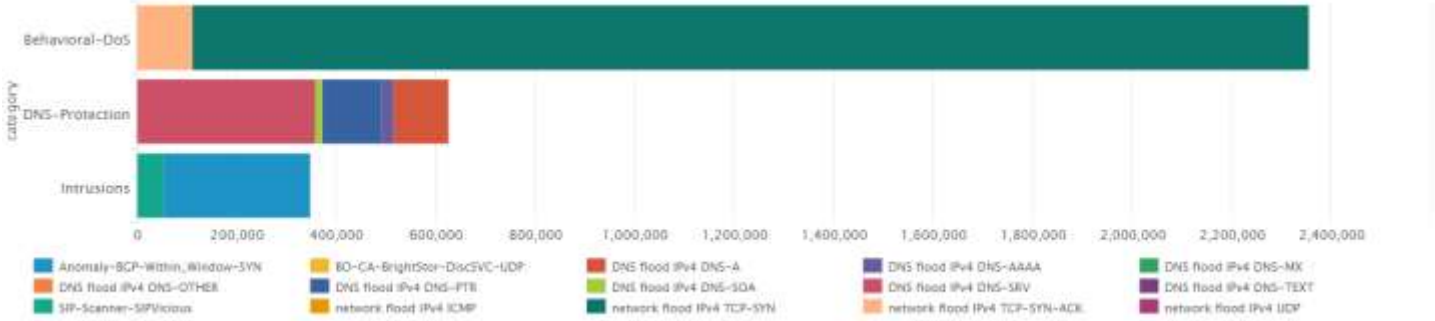


Graph: Attacks Blocked By Threat Category
This report lists the attacks blocked per Attack Category, listing the attack name.



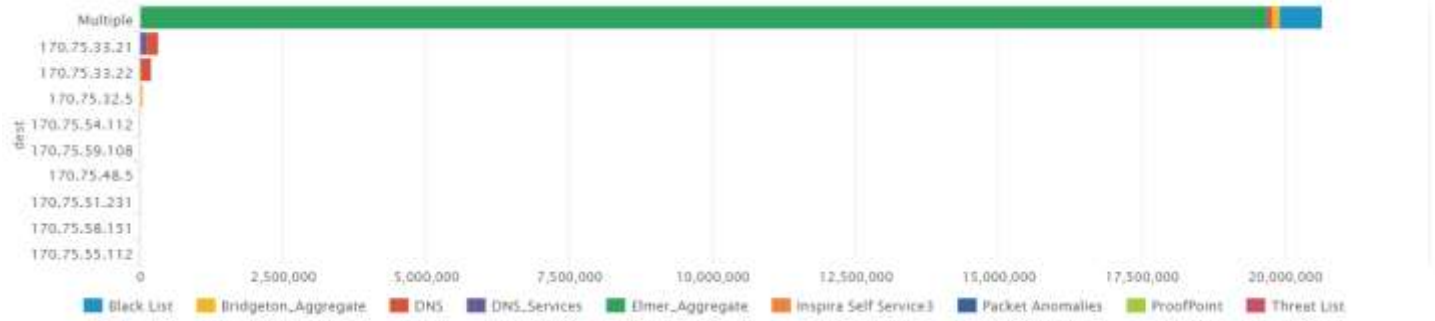
Graph: Critical Attacks Blocked

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



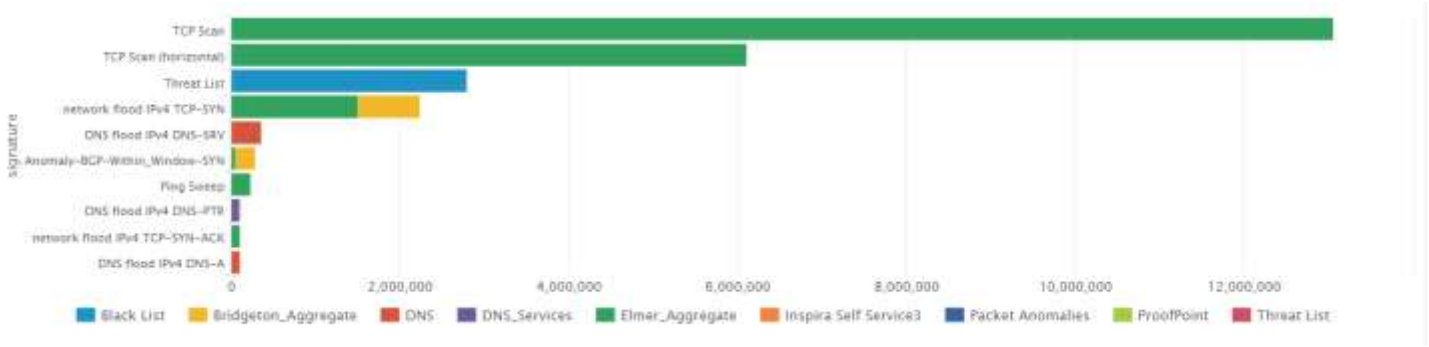
Graph: Top Attacked Destinations Blocked

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.



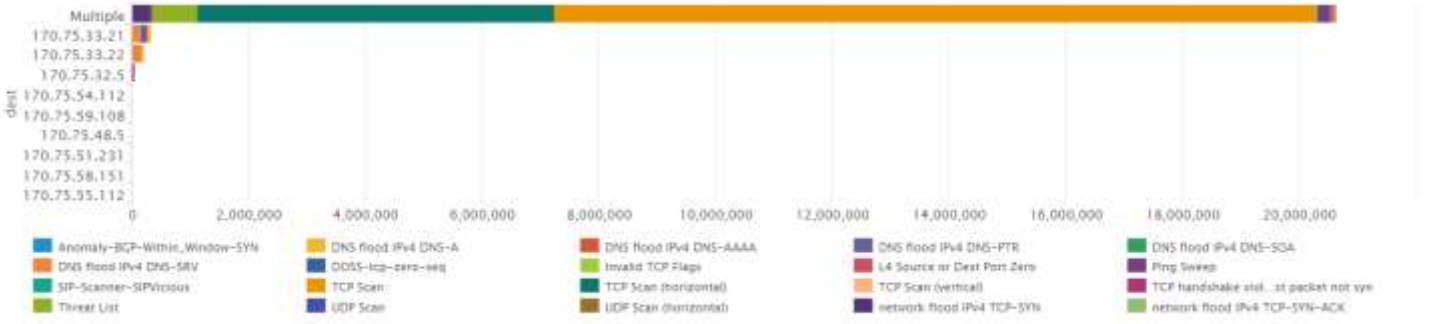
Graph: Top Attacks Blocked

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.



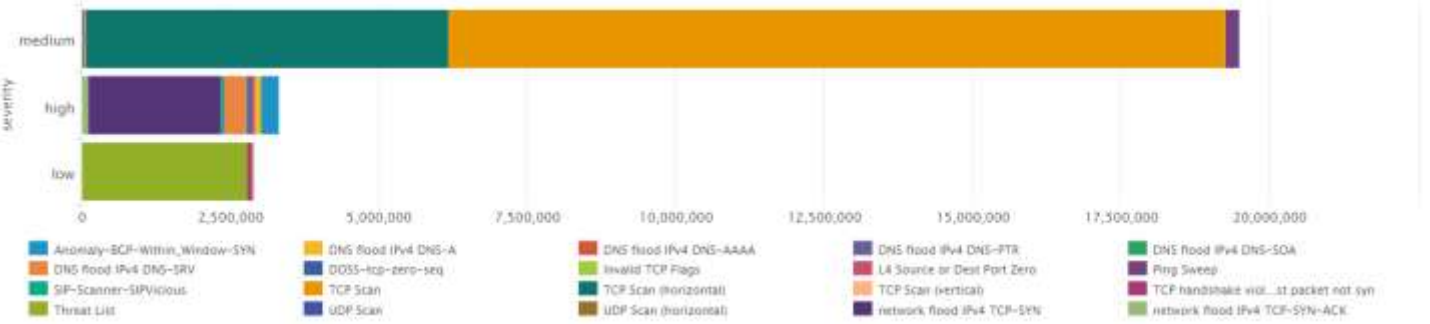
Graph: Top Attacks Blocked by Destination

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.



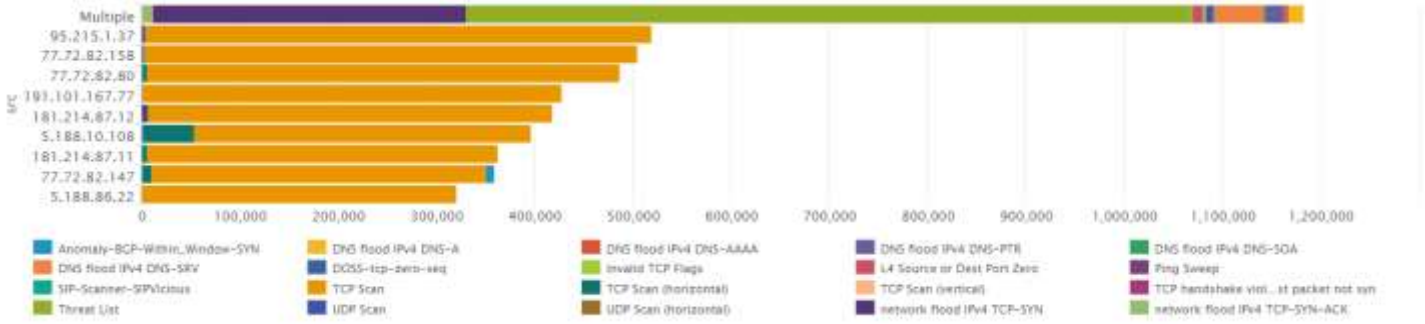
Graph: Top Attacks Blocked By Risk

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

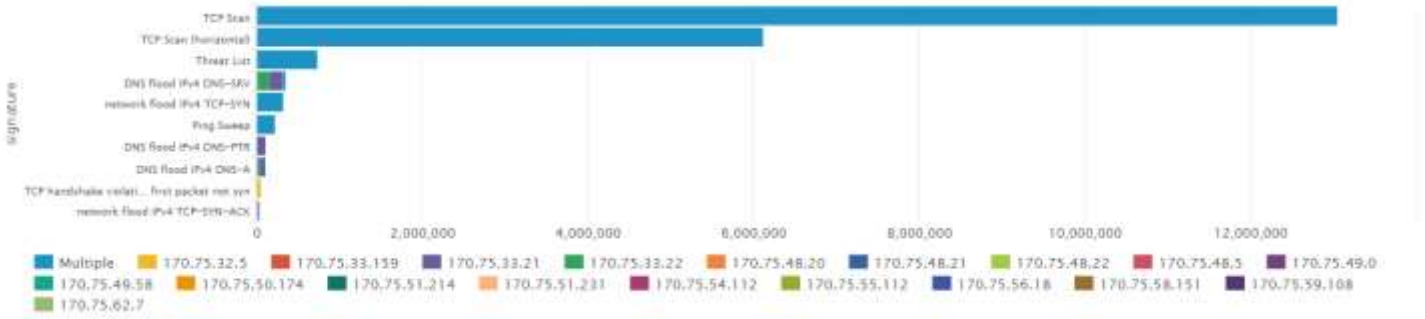
This report provides information on the top attacks blocked, categorized by attacks for each source that was the source of attacks along with the attack name and the number of attacks that triggered with this combination.



See Appendix 1 – Critical Attack Sources (WHOIS Information)

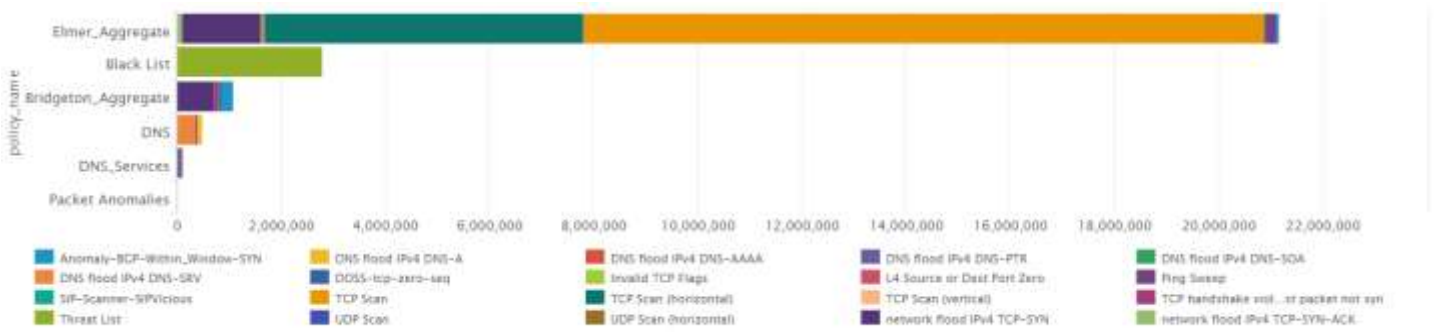
Graph: Top Destinations by Attacks Blocked

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



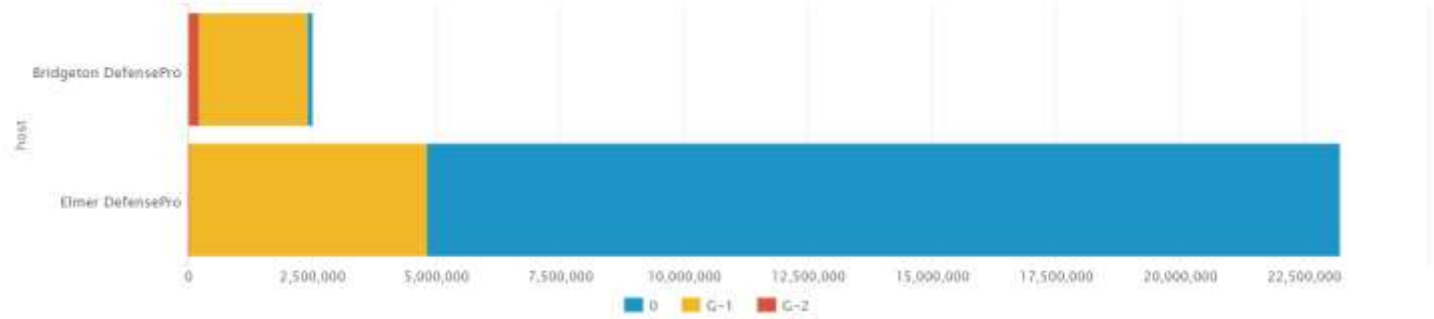
Graph: Attacks Blocked by Network Security Rule

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.



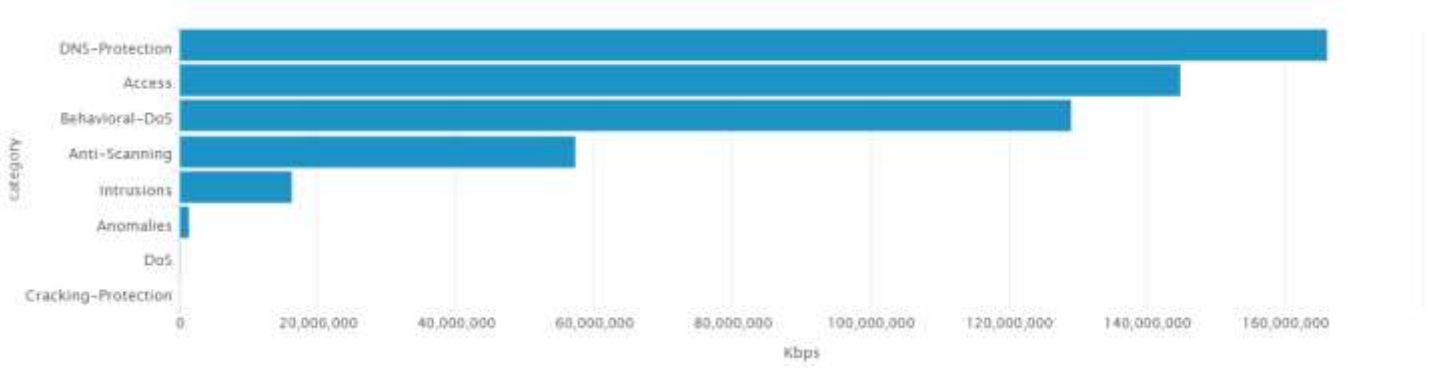
Bandwidth

Behavioral-DoS dropped 123.10 Gbps, Access protection dropped 138.24 Gbps, Intrusion protection dropped 15.52 Gbps of total traffic, 1.32 Gbps dropped by Packet Anomaly protection rules, Anti-Scanning protection dropped 54.82 Gbps, and a total of 491.71 Gbps of malicious traffic was discarded this period.

Category	Gbps	Mbps
DNS-Protection	158.51	162318.71
Access	138.24	141559.87
Behavioral-DoS	123.10	126055.46
Anti-Scanning	54.82	56138.22
Intrusions	15.52	15891.32
Anomalies	1.32	1350.84
DoS	0.18	189.12
Cracking-Protection	0.02	17.55
Total Bandwidth in Gbps/Mbps	491.71	503521.09

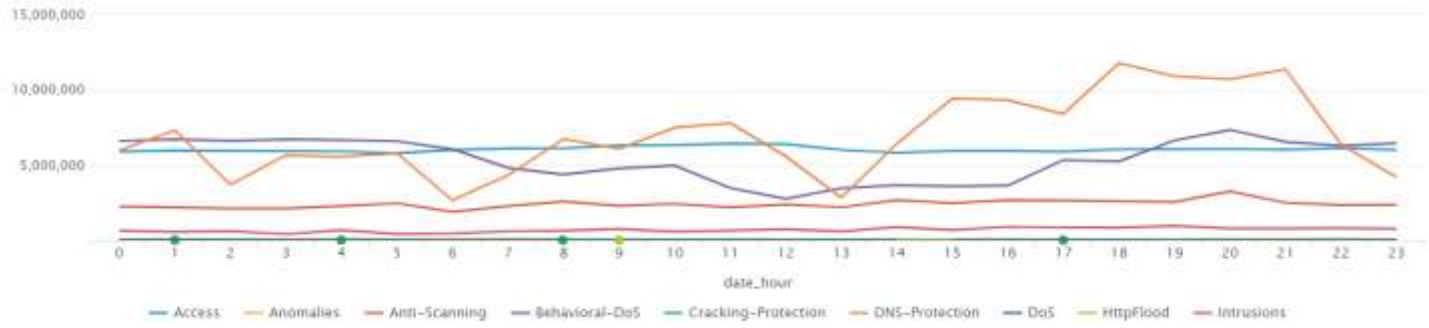
Graph: Attack Categories Blocked by Bandwidth

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



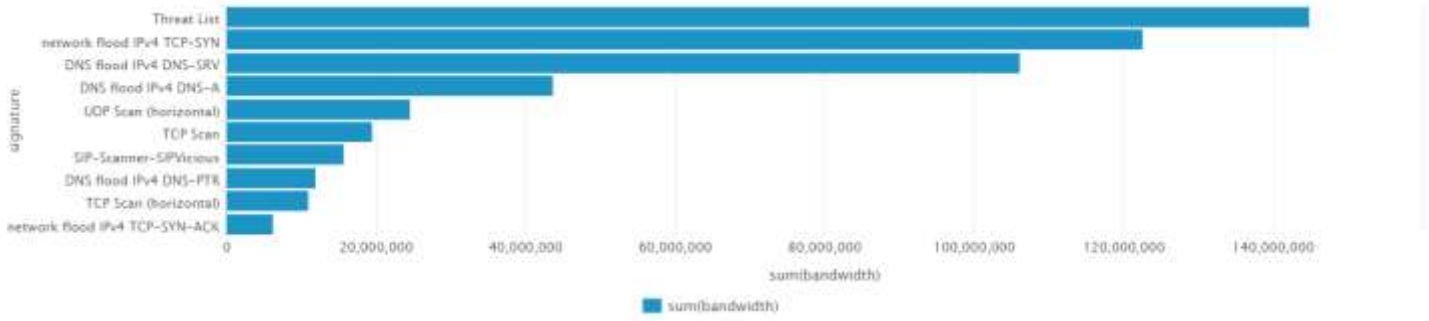
Graph: Bandwidth by Blocked Threat Category by Hour of Day

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.



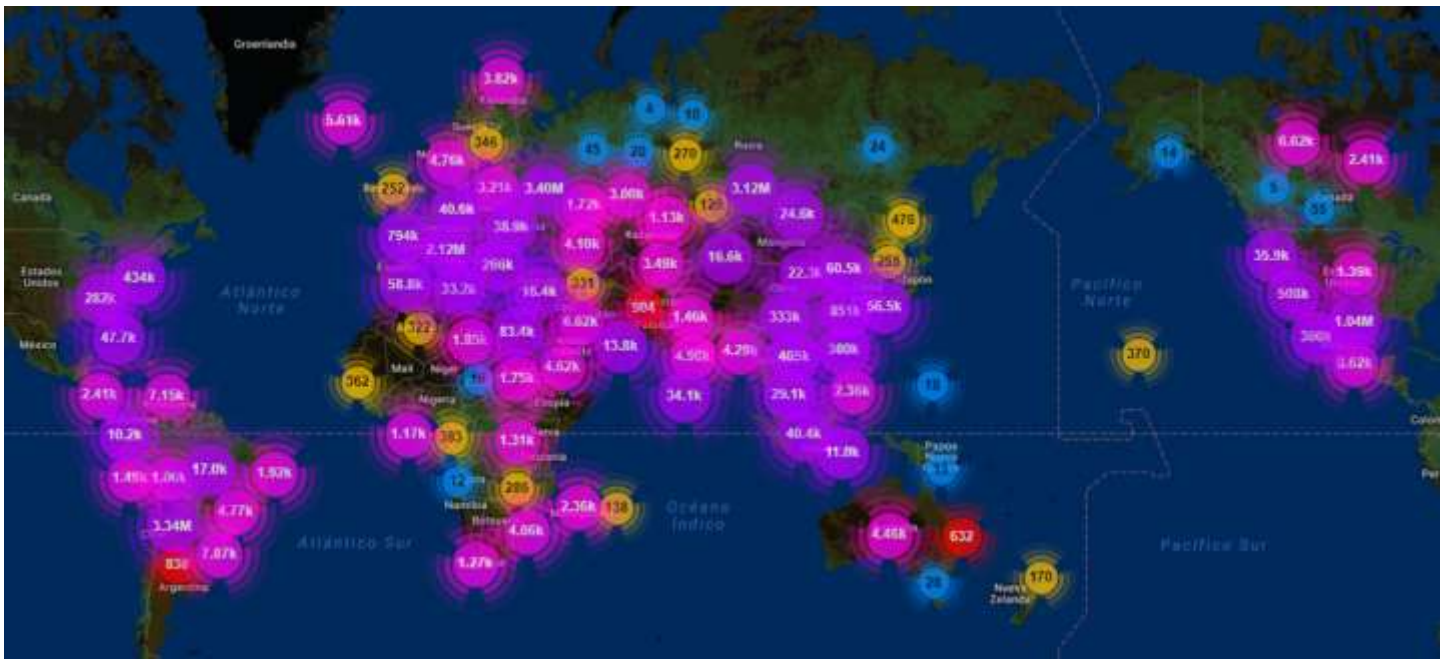
Graph: Top Attacks Blocked by Bandwidth

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



Scanning Information

Map of geographic distribution of **19,553,793** 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.

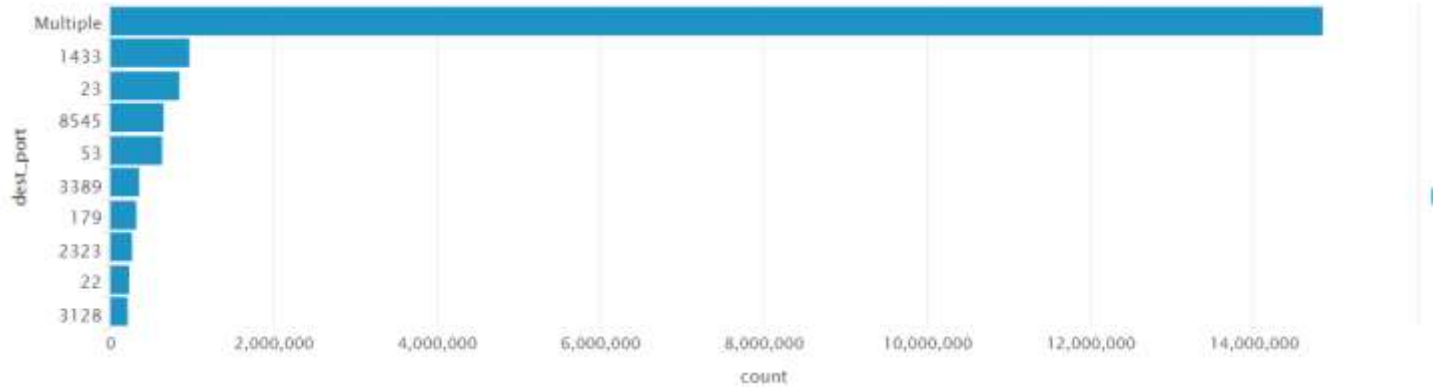
A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (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.

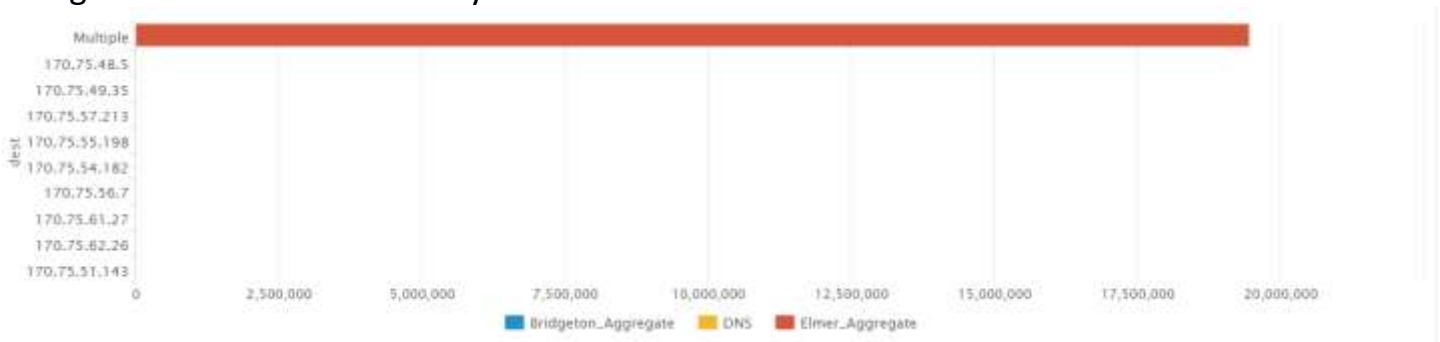
Graph: Top Probed Applications Blocked

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



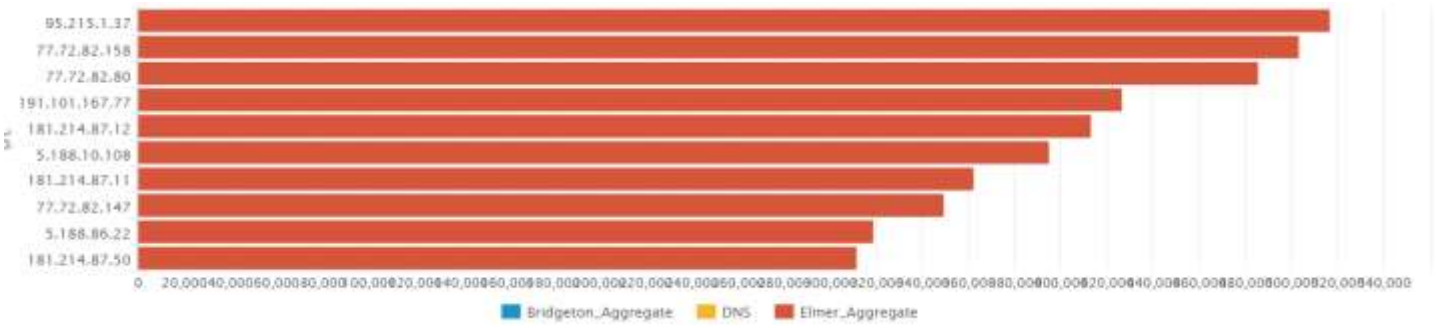
Graph: Top Probed IP Addresses Blocked

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.



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 MSS'VME 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

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

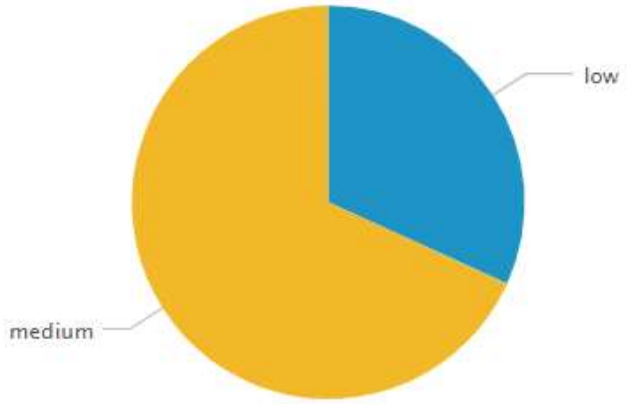
Describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social-engineering or similar attacks.

Vulnerability Information

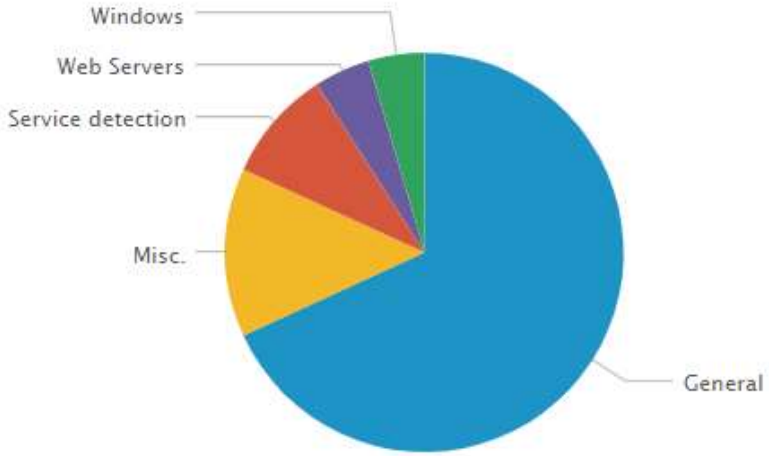
We can observe that Intrusions (known attack signatures), HTTP Flood and Web Scanning attempts are targeting Web Servers and are being dropped by the DefensePro. We cannot be 100% sure but there is a high probability that this type of attack is occurring and if the DefensePro was not in place, the attack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

7. MSS-VME

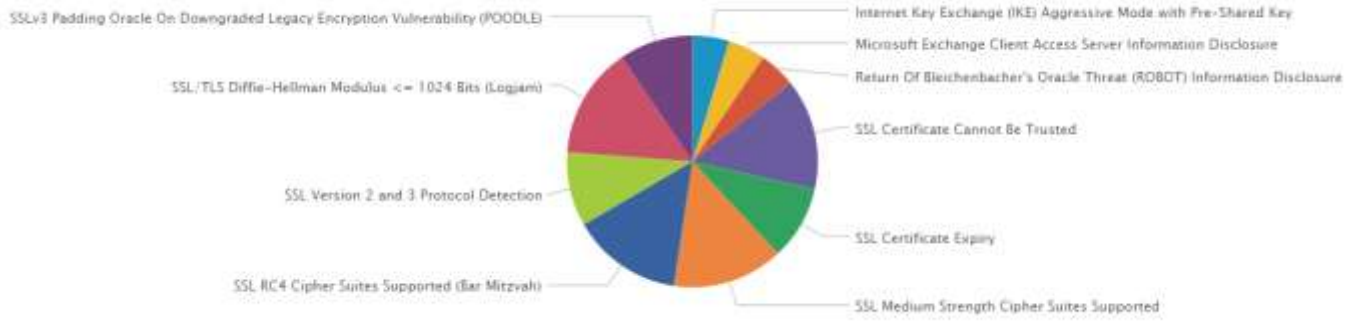
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



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

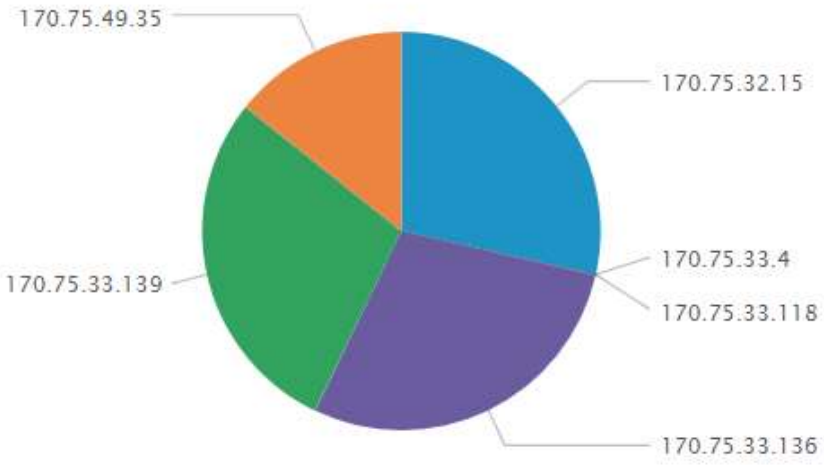


Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



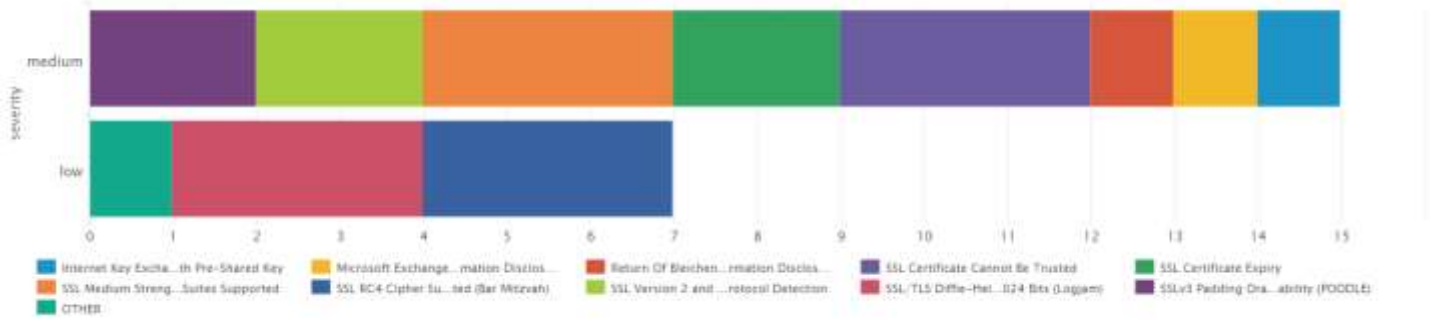
Graph: Most Vulnerable Host

This report depicts the most vulnerable hosts discovered this report period



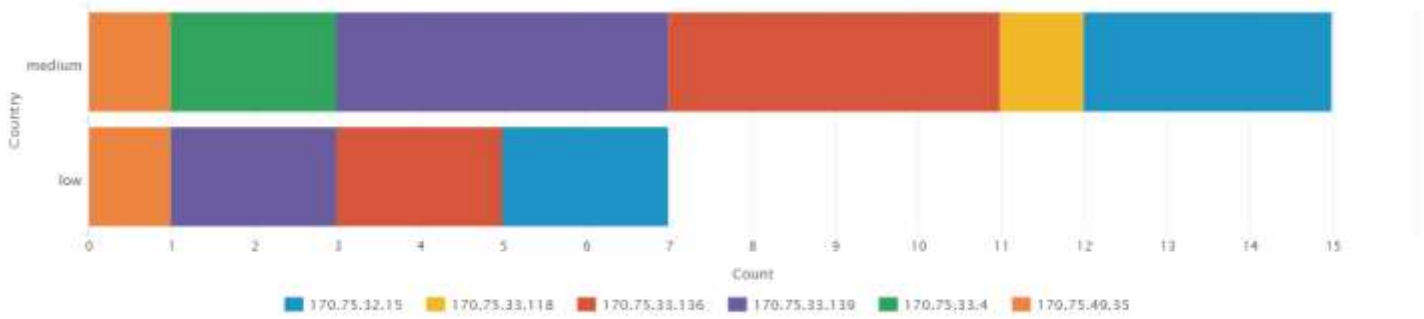
Graph: Vulnerability Risk by Vulnerability Name

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



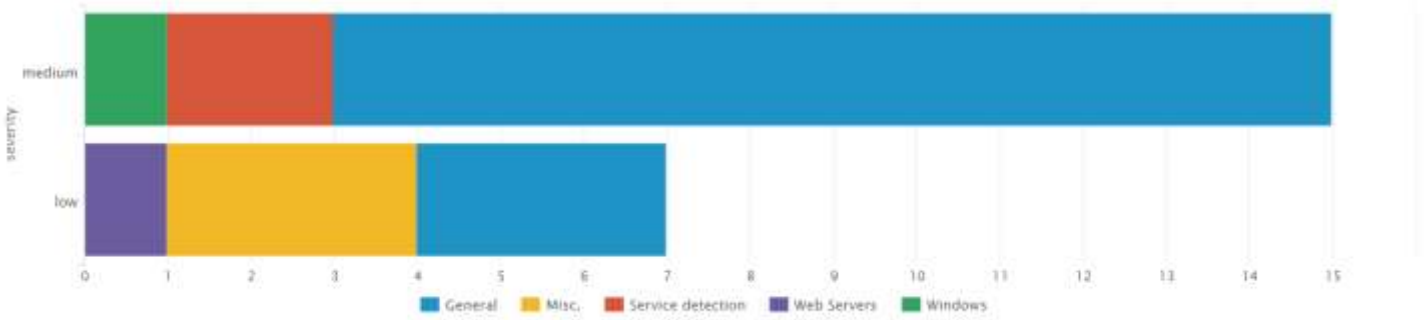
Graph: Vulnerability Risk by Host

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



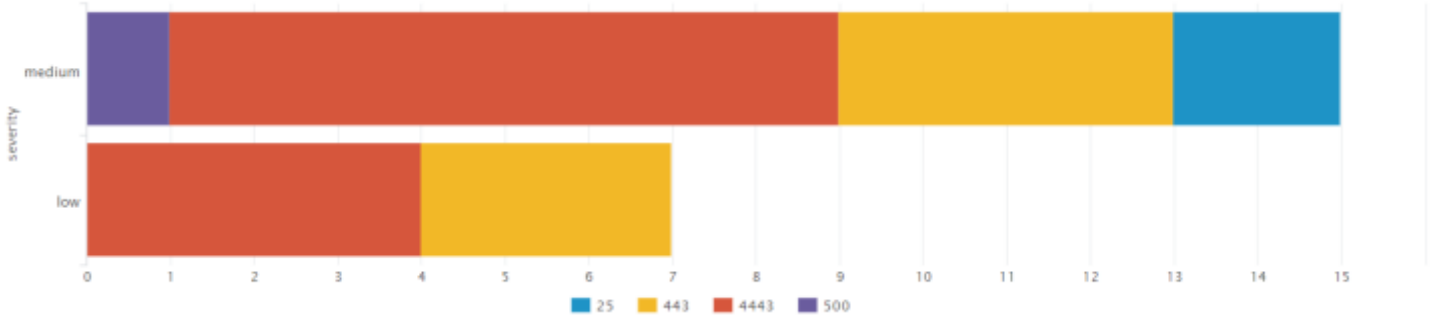
Graph: Vulnerability Risk by Category

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



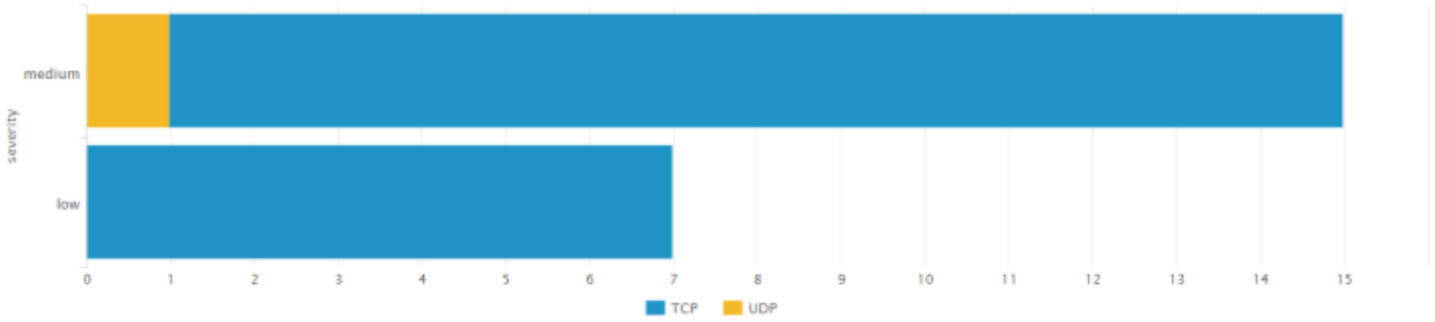
Graph: Vulnerability Risk by Port

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



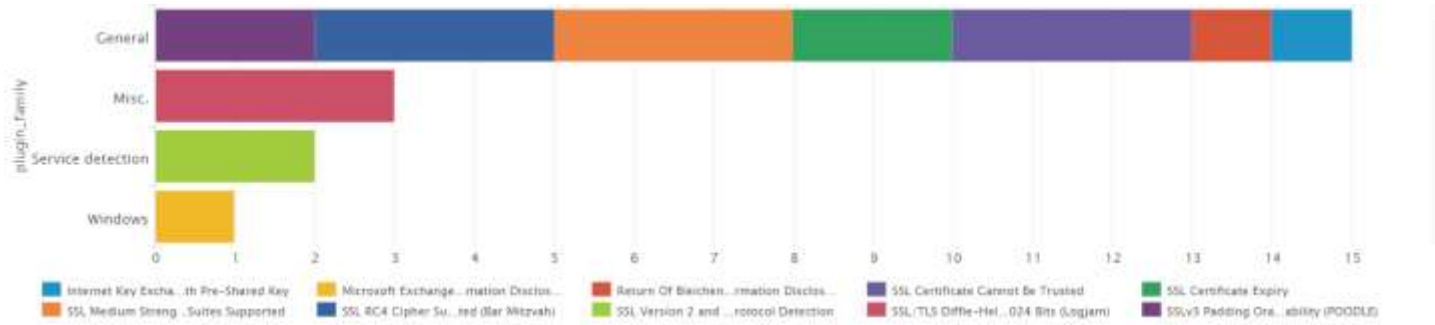
Graph: Vulnerability Risk by Protocol

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



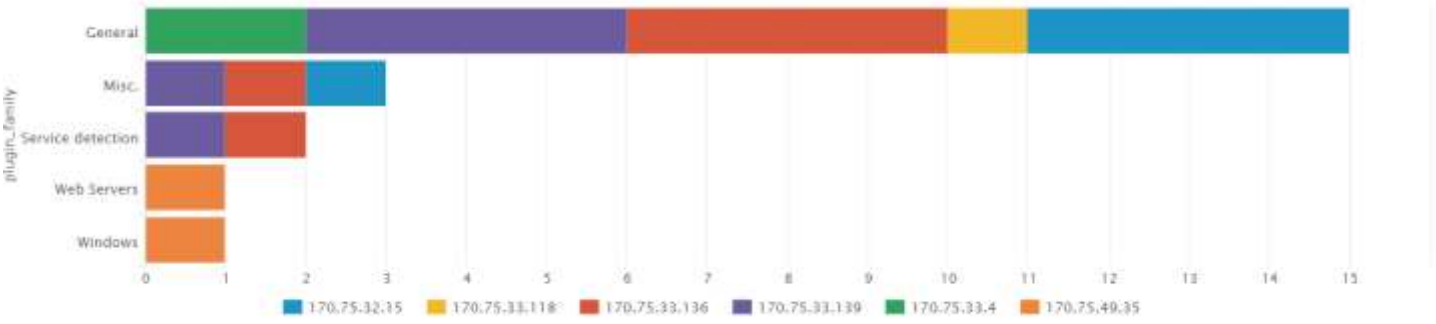
Graph: Vulnerability Category by Vulnerability Name

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



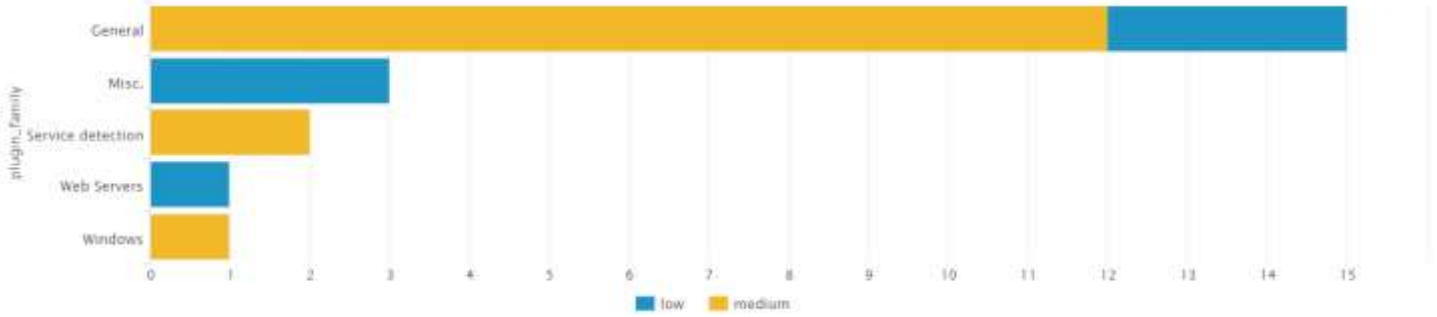
Graph: Vulnerability Category by Host

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



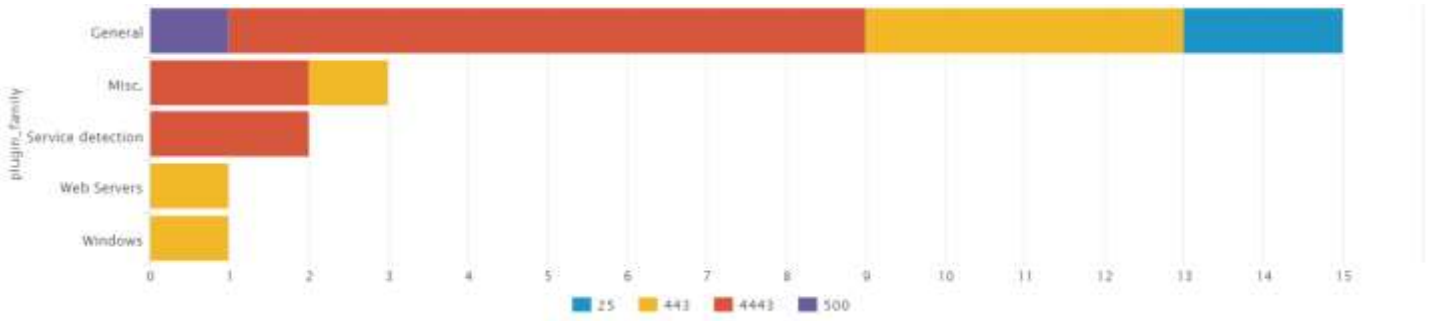
Graph: Vulnerability Category by Risk

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



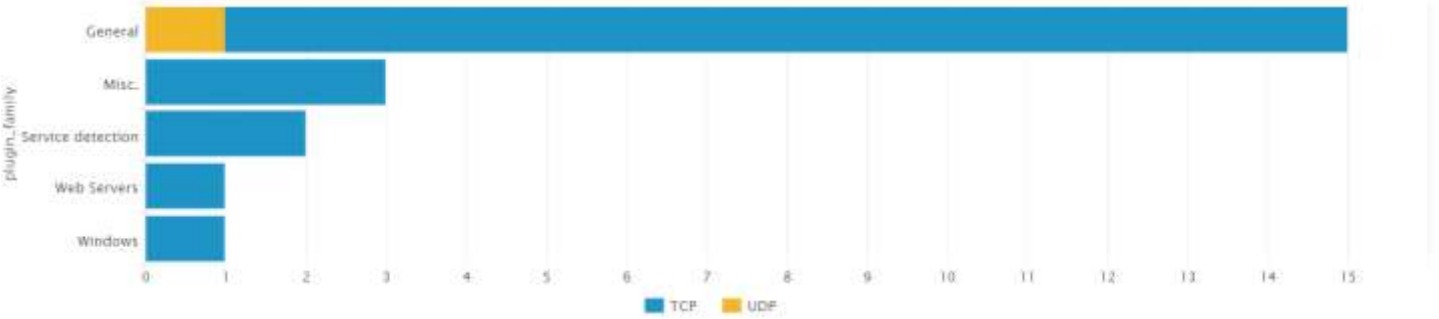
Graph: Vulnerability Category by Port

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



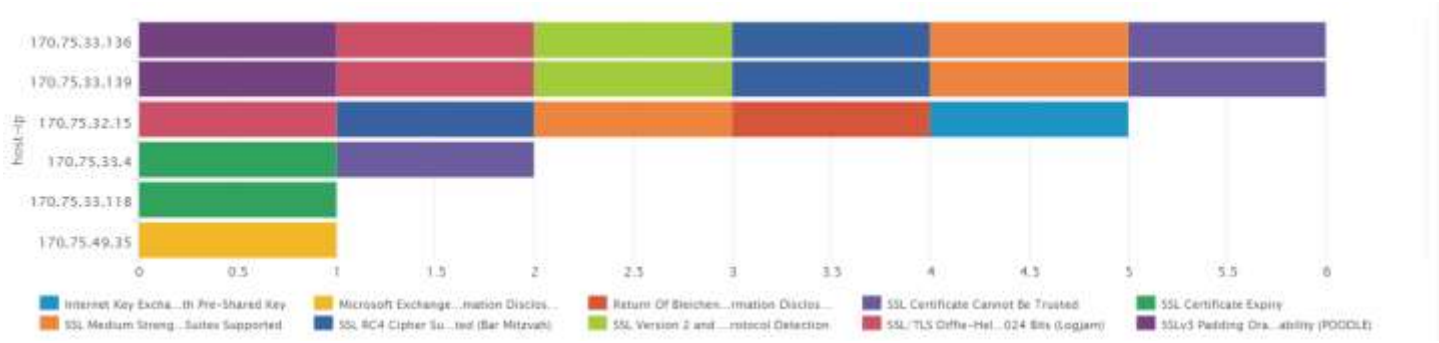
Graph: Vulnerability Category by Protocol

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



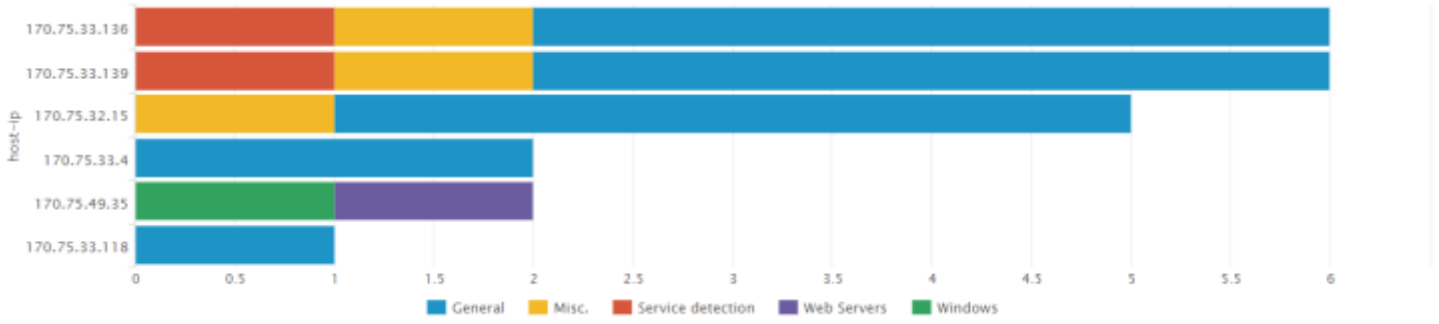
Graph: Host by Vulnerability Name

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



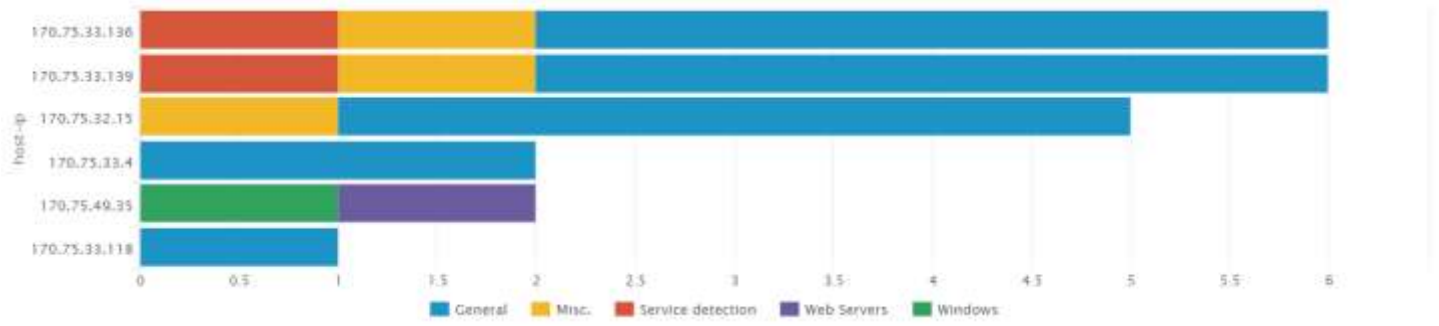
Graph: Host by Vulnerability Category

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



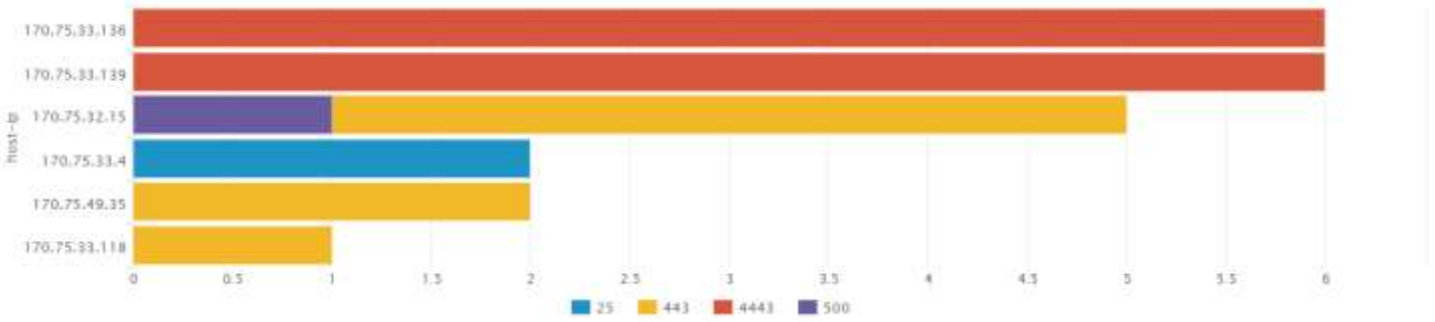
Graph: Host by Vulnerability Risk

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

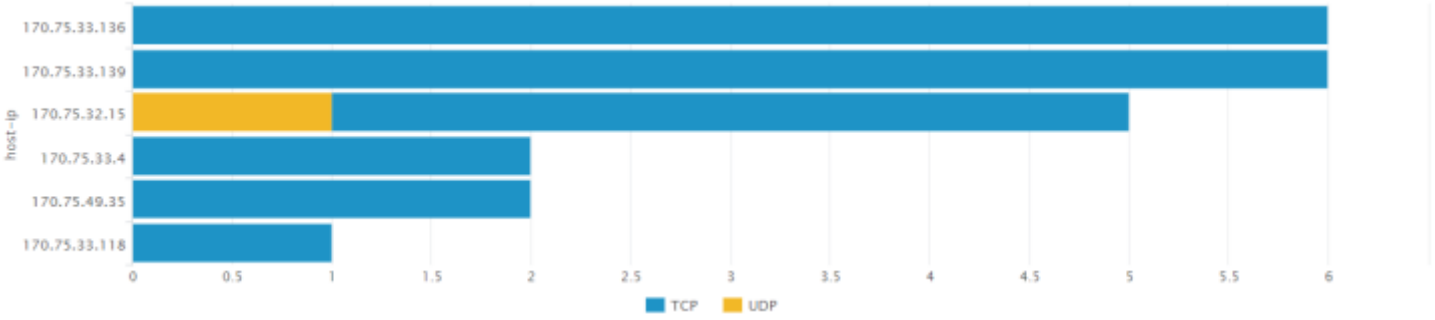


Graph: Host by Port

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



8. 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 Elmer Availability:

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

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	32d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	32d 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	32d 0h 0m 0s	100.000%	100.000%

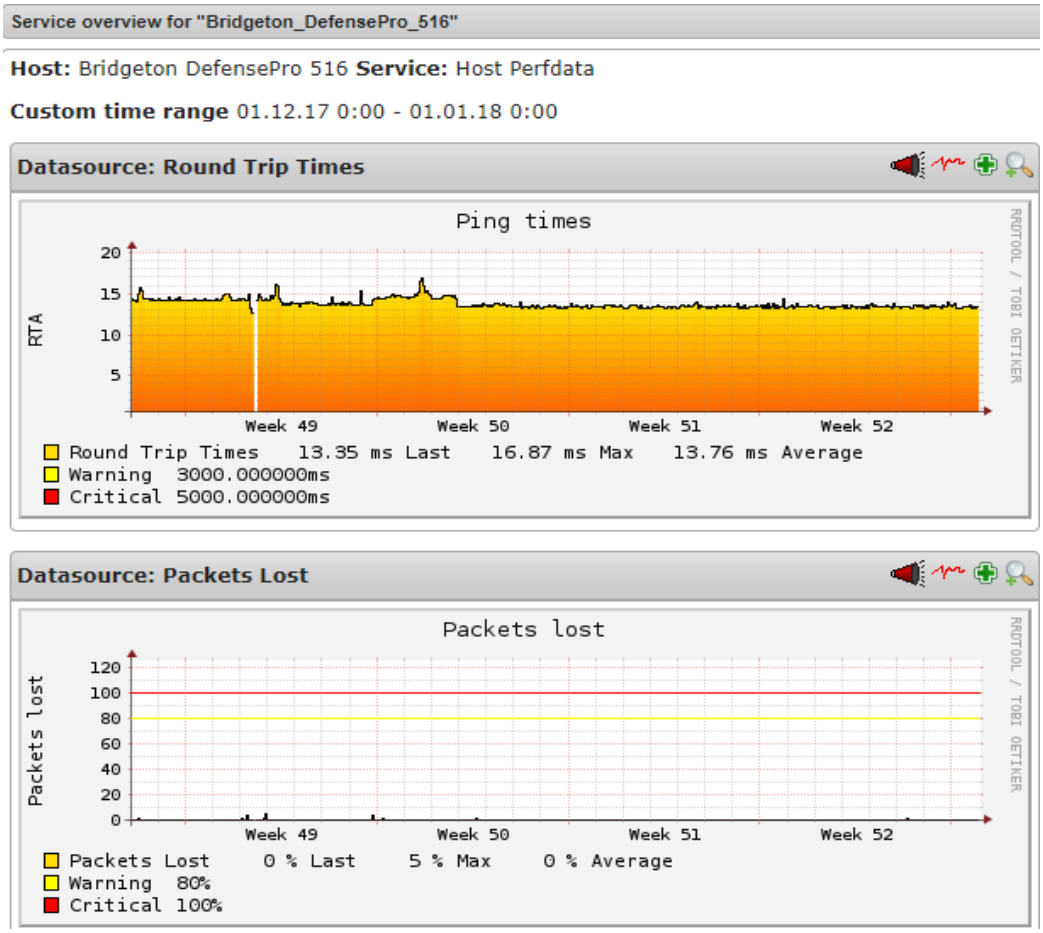
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.990% (99.990%)	0.000% (0.000%)	0.000% (0.000%)	0.010% (0.010%)	0.000%
Average	99.990% (99.990%)	0.000% (0.000%)	0.000% (0.000%)	0.010% (0.010%)	0.000%

b) Monitoring system performance

Inspira Health Network DefensePro Bridgeton Host Performance

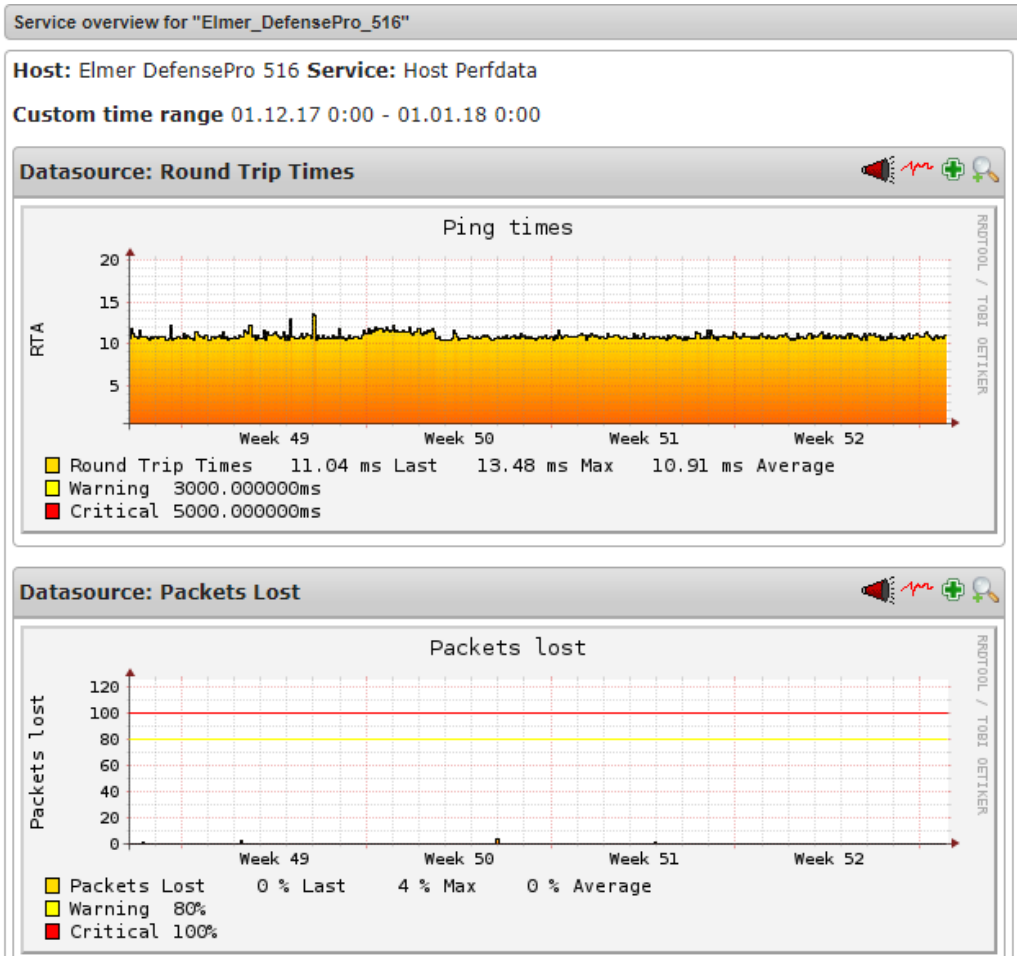
Round trip ping times averaged 16.87ms from the GLESEC GOC to Inspira Health Network DefensePro Bridgeton with 0 % average packet loss.



Inspira Health Network DefensePro Elmer Host Performance

Round trip ping times averaged 13.48ms from the GLESEC GOC to Inspira Health Network

DefensePro Elmer with 0 % average packet loss.



c) Change Management Activities.

As part of the **validation** process for the MSS-APS services provided to Inspira Health Network which involve the review of software and firmware versions and configurations for the security countermeasures for the service, in this case the Radware DefensePro it was determined that an update was necessary for both sites, the Bridgeton and the Elmer locations.

The initial activities were conducted such as creating a copy of the configuration and support files for the DefensePro Bridgeton and verification that the ports being used were configured in fail-open mode, in case of any unforeseen events. We followed standard procedures of Change Management, completed internal forms, requested a window of maintenance with the member-client.

Incident

While following our normal validation and upgrade procedure in the maintenance window that was programmed for this purpose, and updating to current version of the DefensePro in Bridgeton started to drop all traffic causing an Internet outage.

Troubleshooting

An extensive troubleshooting process was performed to address this outage. An assigned team consisting of Inspira, GLESEC and Radware personnel worked on the problem and escalation and documentation procedures were followed. There were complications in the process due to the fact that the changes were done initially on prime-time in a production environment and with the expectations that traffic can be re-directed in full on a secondary path (via Elmer). We learned that a number of the assumptions were not valid in the process. The process took more time than desired due to two factors, one that the DefensePro was put off-line and therefore we could not see its behavior and the second that returning the system to the initial software version required a USB stick of certain characteristics which were not available on-site and we had to get one shipped over.

Problems discovered during the incident

1. The network topology does not have a real built in redundancy, causing that: the traffic has to be manually diverted via Elmer, when Bridgeton is down. We assumed this is the same case with Bridgeton if Elmer is down.
2. Not all the traffic deviated from Bridgeton was being passed through the DefensePro-EL (this was stated by Francois in the conference of Dec 6)
3. Elmer and Bridgeton are not setup with symmetric routing; this means that not all of the sub-nets are advertised by both BGP routers at the same time. This has implications to some of the protection capabilities of the service.
4. The syslog of the DefensePro did not provide indications of the problem, this was later found in other event logs.

Resolution

The problem occurred when the DefensePro was restarted and a rule that was not active became active, forcing the drop of all traffic. This rule (which does not exist in the DefensePro at Elmer) existed but was disabled in Bridgeton.

As a side note, it is important to know that the policies for: TCP scanning and DNS flood are disabled because these are not supported on asymmetric environments. Therefore we should consider the possibility to make changes in the network to improve the flow and the security countermeasures.

Recommendations

1. Validation
    a. The process of software update and verification of active policies with validation to needed policies still has to be conducted.
    b. We should have a more comprehensive conference to discuss this for all stakeholders and also more strict change management activities (see below).
2. Network documentation
    a. We need up-to-date documentation for the network. Topology maps, critical devices assets…
3. Network optimization analysis
    a. We recommend reviewing the network for better traffic flow in case of an incident and symmetric paths.
4. Implement stronger Change Management

We are reviewing our process to apply stronger conditions, for example we should insist on implementing these changes after hours, among other considerations. We will provide Inspira with visibility of our Change Management Forms and review the plan together beforehand

d) Incident Response Activities

No incidents reported this month

9. Appendix 1 – Top Scanners Blocked (WHOIS Information)

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

NetRange: 65.5.139.96 - 65.5.139.127
CIDR: 65.5.139.96/27
OriginAS:
NetName: BLS-65-5-139-96-27-1007264407
NetHandle: NET-65-5-139-96-1
Parent: NET-65-0-0-0-1
NetType: Reassigned
RegDate: 2010-07-26
Updated: 2010-07-26
Ref: http://whois.arin.net/rest/net/NET-65-5-139-96-1

CustName: Datapro
Address: 770 Ponce De Leon
City: Coral Gables
StateProv: FL
PostalCode: 33131
Country: US
RegDate: 2010-07-26
Updated: 2011-03-19
Ref:
OrgAbuseHandle: ABUSE81-ARIN
OrgAbuseName: Abuse Group
OrgAbusePhone: +1-919-319-8265
OrgAbuseEmail:
OrgAbuseRef:
OrgTechHandle: IPOPE3-ARIN
OrgTechName: IP Operations
OrgTechPhone: +1-888-510-5545
OrgTechEmail:
OrgTechRef:
RAbuseHandle: ABUSE81-ARIN
RAbuseName: Abuse Group

RAbusePhone: +1-919-319-8265
RAbuseEmail:
RAbuseRef:

RTechHandle: IPOPE3-ARIN
RTechName: IP Operations
RTechPhone: +1-888-510-5545
RTechEmail:
RTechRef:

inetnum: 200.46.160/20
status: allocated
aut-num: N/A
owner: Cable Onda
ownerid: PA-CAON1-LACNIC
responsible: Climaco Manuel Paz
address: Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address: 55-0593 - Panama - PA
country: PA
phone: +507 390 3485 []
owner-c: CAO
tech-c: CAO
abuse-c: CAO
inetrev: 200.46.174/23
nserver: NS.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 19981221
changed: 20140826

nic-hdl: CAO
person: Cable Onda Panama
e-mail:
address: Edificio Cable Onda, Pueblo Nuevo, 0, 0
address: 0831-0059 - Panama - PA

country: PA
phone: +507 3907616 []
created: 20021009
changed: 20071107

inetnum: 200.46.160/20
status: allocated
aut-num: N/A
owner: Cable Onda
ownerid: PA-CAON1-LACNIC
responsible: Climaco Manuel Paz
address: Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address: 55-0593 - Panama - PA
country: PA
phone: +507 390 3485 []
owner-c: CAO
tech-c: CAO
abuse-c: CAO
inetrev: 200.46.174/23
nserver: NS.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 19981221
changed: 20140826

nic-hdl: CAO
person: Cable Onda Panama
e-mail:
address: Edificio Cable Onda, Pueblo Nuevo, 0, 0
address: 0831-0059 - Panama - PA
country: PA
phone: +507 3907616 []
created: 20021009
changed: 20071107

NetRange: 23.24.0.0 - 23.25.255.255
CIDR: 23.24.0.0/15
NetName: CBC-ALLOC-4
NetHandle: NET-23-24-0-0-1
Parent: NET23 (NET-23-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Comcast Business Communications, LLC (CBCI)
RegDate: 2012-01-13
Updated: 2012-02-23
Ref: http://whois.arin.net/rest/net/NET-23-24-0-0-1

OrgName: Comcast Business Communications, LLC
OrgId: CBCI
Address: 1800 Bishops Gate Blvd.
City: Mount Laurel
StateProv: NJ
PostalCode: 08054-4628
Country: US
RegDate: 2001-12-21
Updated: 2011-01-06
Ref: http://whois.arin.net/rest/org/CBCI

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName: Network Abuse and Policy Observance
OrgAbusePhone: +1-888-565-4329
OrgAbuseEmail:
OrgAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

OrgTechHandle: IC161-ARIN
OrgTechName: Comcast Cable Communications Inc
OrgTechPhone: +1-856-317-7200
OrgTechEmail:
OrgTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

RTechHandle: IC161-ARIN
RTechName: Comcast Cable Communications Inc
RTechPhone: +1-856-317-7200

RTechEmail:
RTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

RAbuseHandle: NAPO-ARIN
RAbuseName: Network Abuse and Policy Observance
RAbusePhone: +1-888-565-4329
RAbuseEmail:
RAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

NetRange: 23.24.160.0 - 23.24.191.255
CIDR: 23.24.160.0/19
NetName: CBC-MIAMI-25
NetHandle: NET-23-24-160-0-1
Parent: CBC-ALLOC-4 (NET-23-24-0-0-1)
NetType: Reallocated
OriginAS:
Organization: Comcast Business Communications, LLC (CBCI)
RegDate: 2012-02-24
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-23-24-160-0-1

OrgName: Comcast Business Communications, LLC
OrgId: CBCI
Address: 1800 Bishops Gate Blvd.
City: Mount Laurel
StateProv: NJ
PostalCode: 08054-4628
Country: US
RegDate: 2001-12-21
Updated: 2011-01-06
Ref: http://whois.arin.net/rest/org/CBCI

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName: Network Abuse and Policy Observance
OrgAbusePhone: +1-888-565-4329
OrgAbuseEmail:
OrgAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

OrgTechHandle: IC161-ARIN
OrgTechName: Comcast Cable Communications Inc
OrgTechPhone: +1-856-317-7200
OrgTechEmail:
OrgTechRef:

inetnum: 190.34/15
status: allocated
aut-num: N/A
owner: Cable & Wireless Panama
ownerid: PA-CWPA-LACNIC
responsible: Cable and Wireless Panama
address: 0834-00659, Panama, 9A,
address: 083400659 - Panama - -
country: PA
phone: +507 2696181 []
owner-c: CAP3
tech-c: CAP3
abuse-c: CAP3
inetrev: 190.34/15
nserver: NS.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 20061122
changed: 20061122

nic-hdl: CAP3
person: Russell Bean
e-mail:
address: Apartado 659, PA,
address: 9A - Panama -
country: PA
phone: +507 882 2200 [22]
created: 20030416
changed: 20130509

inetnum: 190.33/16
status: allocated
aut-num: N/A
owner: Cable & Wireless Panama
ownerid: PA-CWPA-LACNIC
responsible: Cable and Wireless Panama
address: 0834-00659, Panama, 9A,
address: 083400659 - Panama - -
country: PA
phone: +507 2696181 []
owner-c: CAP3
tech-c: CAP3
abuse-c: CAP3
inetrev: 190.33/16
nserver: NS.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 20060815
changed: 20060815

nic-hdl: CAP3
person: Russell Bean
e-mail:
address: Apartado 659, PA,
address: 9A - Panama -
country: PA
phone: +507 882 2200 [22]
created: 20030416
changed: 20130509

inetnum: 200.46.226.208/28
status: reallocated
owner: STARUN, S.A.
ownerid: PA-STSA1-LACNIC
responsible: NET2NET IP Admin

address: Colon, 1, 1
address: 11111 - Colon -
country: PA
phone: +507 3008888 []
owner-c: NEA3
tech-c: NEA3
abuse-c: NEA3
created: 20050504
changed: 20050504
inetnum-up: 200.46.224/19

nic-hdl: NEA3
person: Net2Net Admin
e-mail:
address: Plaza Bal Harbour Paitilla, 1,
address: 55-0779 - Panama - PA
country: PA
phone: +507 206-3000 [ATM]
created: 20030414
changed: 20091028

NetRange: 22.0.0.0 - 22.255.255.255
CIDR: 22.0.0.0/8
NetName: DNIC-SNET-022
NetHandle: NET-22-0-0-0-1
Parent: ()
NetType: Direct Allocation
OriginAS:
Organization: DoD Network Information Center (DNIC)
RegDate: 1989-06-26
Updated: 2009-04-15
Ref: http://whois.arin.net/rest/net/NET-22-0-0-0-1

OrgName: DoD Network Information Center
OrgId: DNIC
Address: 3990 E. Broad Street
City: Columbus
StateProv: OH

PostalCode: 43218
Country: US
RegDate:
Updated: 2011-08-17
Ref: http://whois.arin.net/rest/org/DNIC

OrgTechHandle: REGIS10-ARIN
OrgTechName: Registration
OrgTechPhone: +1-800-365-3642
OrgTechEmail: disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef: http://whois.arin.net/rest/poc/REGIS10-ARIN

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName: Network DoD
OrgTechPhone: +1-614-692-6337
OrgTechEmail: disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef: http://whois.arin.net/rest/poc/MIL-HSTMST-ARIN

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName: Registration
OrgAbusePhone: +1-800-365-3642
OrgAbuseEmail: disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgAbuseRef:
inetnum: 203.178.0.0 - 203.183.255.255
netname: JPNIC-NET-JP
descr: Japan Network Information Center
country: JP
admin-c: JNIC1-AP
tech-c: JNIC1-AP
remarks: JPNIC Allocation Block
remarks: Authoritative information regarding assignments and
remarks: allocations made from within this block can also be
remarks: queried at whois.nic.ad.jp. To obtain an English
remarks: output query whois -h whois.nic.ad.jp x.x.x.x/e
mnt-by: MAINT-JPNIC
changed: 19991208
status: ALLOCATED PORTABLE
source: APNIC

role: Japan Network Information Center
address: Urbannet-Kanda Bldg 4F
address: 3-6-2 Uchi-Kanda
address: Chiyoda-ku, Tokyo 101-0047,Japan
country: JP
phone: +81-3-5297-2311
fax-no: +81-3-5297-2312
e-mail:
admin-c: JI13-AP
tech-c: JE53-AP
nic-hdl: JNIC1-AP
mnt-by: MAINT-JPNIC
changed: 20041222
changed: 20050324
changed: 20051027
changed: 20120828
source: APNIC

inetnum: 190.62/16
status: allocated
aut-num: AS22833
abuse-c: RAC3
owner: CTE S.A. de C.V.
ownerid: SV-CSCV-LACNIC
responsible: CLARO INTERNET
address: Colonia Roma, Calle El Progreso, Complejo Telecom, A,
address: 4175 - San Salvador - SS
country: SV
phone: +503 22503836 []
owner-c: EAB4
tech-c: EAB4
abuse-c: EAB4
created: 20110121
changed: 20120523

nic-hdl: EAB4
person: Alexander Peña

e-mail:
address: xxxx, ,
address: 0000 - San Salvador -
country: SV
phone: +503 503 22505555 []
created: 20101103
changed: 20130809

nic-hdl: RAC3
person: Alberto Lemus
e-mail:
address: Colonia Roma Calle El Progreso Complejo Telecom, 4175,
address: 4175 - San Salvador - SS
country: SV
phone: +503 250 3836 []
created: 20040510
changed: 20060713

10. Appendix 2 – 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/

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

Panamá
Central America HQ
Prime Time
Address. La Rotonda Costa del Este
Panamá City, Panamá
Tel. +507.836.5355

Argentina
South América HQ
+54.11.5917.6120

Brasil
+55.11.3711.5699

Chile
+56.2938.1496

Perú
+51.1708.7197

México
+52.55.5018.14