OPERATIONS & INTELLIGENCE EXECUTIVE CYBER SECURITY REPORT

BANVIVIENDA

JULY, 2018

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

Table of Contents

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

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 services under contract. The information generated by these services is then aggregated, correlated and analyzed. The more complete the set of services under contract the more accurate and complete the results will be.

The report is organized in three parts; the first is the Executive Summary with recommendations (as necessary or applicable), the second is the Intelligence Section with more detail information and analysis dashboards and the last is Operational Section with status of the services and counter-measures under contract, tickets for change management and incidents reported and consulting activity for the month.

We at GLESEC believe that information security is a holistic and dynamic process that requires on-going research and follow up and should be handled with the right tools, systems, processes, skill personnel and focus attention. The process is dynamic due to 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 activism are the very cause of information security exposure and are most commonly driven by financial gain. GLESEC's outsourcing services, based on its proprietary TIPTM platform portfolio provide the ideal response to the above.

Confidentiality

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

- Client name and contact information
- System architecture, configuration, access methods and access control
- Security content

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

Scope of this Report

GLESEC Contracted Services Table

Type	Service	Contracted?	Service Expiration
Threat Mitigation	MSS-APS		
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	July 1, 2019
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM	YES	July 1, 2019
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EIR	YES	July 1, 2019
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS		

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Executive Summary

This report corresponds to the period from July, 2018.

The following table describes the major categories that GLESEC has identified to report on the state-of-security of its member-clients. The categories in the table below are based on risk-management methodology. This is a principal foundational aspect of GLESEC.

RISK

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. The NIST Cyber-Security Framework.

One of GLESEC's foundational columns is basing all its activities to support RISK determination and mitigation. What any organization should want to know if what is their level of RISK, and in this case in particular to cyber-security. Cyber-Security RISK has a direct impact to the business and as such is of paramount importance to the Board and Management of the company.

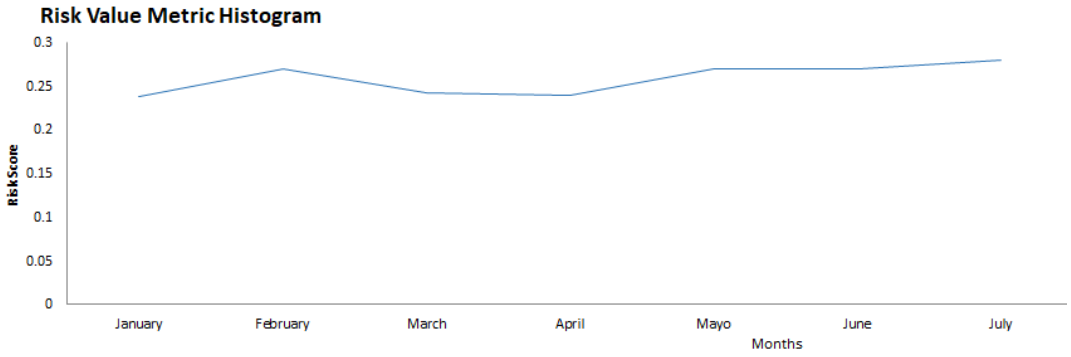
We at GLESEC measure RISK through a number of perspectives and using several of the TIP™ platform portfolio of services. The MSS-VM or Managed Vulnerability Service provides us with one view, how weak are the systems of the organization.

The MSS-BAS provides us a view of how weak are the defenses of the organization to the latest threats. The MSS-APS, MSS-SIEM, MSS-UTM, MSS-EIR, MSS-EPS provides us with attack information both internal and external, DDOS, Malware, Ransomware and other attack vector information as well as provide protection level services. The MSS-EPS also provides us RISK level information for non-compliance with internal or external requirements and/or regulations. All in all, a variety of services provide us with different views and together we have the most complete view of our client's security posture.

We determine that the risk condition for the BANVIVIENDA for the month of July is high. This can be seen in the security indicator as indicated below.

Risk Indicator	Service	Condition	Comments
Risk Value Metric	MSS-VME	HIGH	4 high vulnerabilities are reported. Any one of these can cause an impact to the BANVIVIENDA.

The RISK VALUE METRIC histogram below represents the changes in the Vulnerability based Risk Value Metric over the past six months.



During this period of the month, 15of its systems were accessed, of which 10 are vulnerable.

Compared to the previous month, this month high level vulnerabilities were detected, these vulnerabilities are related to the TLS protocol, we recommend to BANVIVIENDA apply the detailed recommendations in our monthly technical report.

VULNERABILITIES

GLESEC's MSS-VM(E/I) service is used to conduct two weekly testing to external

and/or internal systems (depending on the options of the contracted service). Of the two tests performed weekly, one is to test for discovery of assets on the network and the other to test for vulnerabilities. The external testing is performed from GLESEC' cloud platform and the internal is conducted with the GLESEC Multi-Security Appliance (GMSA).

Vulnerabilities are weaknesses that if exploited can compromise the organization and as such are a component of RISK for the organization. If there are vulnerabilities and also threats, there is RISK that the organization can be impacted. The vulnerabilities reported by GLESEC should be considered all important and addressed according to the priority (Critical, High, Medium and Low). An effective process is to work with the GLESEC provided information and GLESEC consulting team to address the recommendations provided in a systematic and continuous way. Progress can be determined by the weekly testing.

15 hosts were discovered, of which 10 are vulnerable, BANVIVIENDA has 38 vulnerabilities in total this month, the vast majority have been medium risk vulnerabilities 25 (66%), high 4 (10%) and low risks 9 (23 %) and No vulnerabilities of critical severity have been found during the month.

There was an increase in the number of high vulnerabilities compared to the previous period in which there were 0, but there was a decrease of 16% in the vulnerabilities of average severity.

The number of medium and low vulnerabilities has remained the same throughout the month. The category of Vulnerabilities presented is: General (81), Service Detection (11%), Misc (5%) and Windows (3%).

The 6 most vulnerable hosts of your organization during this period and which have medium severity vulnerabilities.

- 200.90.137.87
- 200.90.137.89
- 200.90.137.83
- 200.46.227.230
- 200.46.19.100
- 200.90.137.91

The vulnerabilities of average consideration found for this period are the following:

- SSL Medium Strength Cipher Suites Supported
- SSL Certificate Cannot Be Trusted
- SSL Certificate Signed Using Weak Hashing Algorithm
- SSL Self-Signed Certificate
- SSL Weak Cipher Suites Supported
- SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE).

Risk Value Metric

GLESEC utilizes a metric to provide a way to quantify the vulnerabilities-based risk of an organization. This metric is to measure the relative value of vulnerabilities and also the record of change over time.

It is important to mention that this metric considers a median value for the vulnerabilities classified as "critical", "high", "medium" and "low", giving them a weight of 100%, 75%, 50% and 10% respectively.

This takes into consideration all of the vulnerabilities but is important to point out that this values (100%, 75%, 50% and 10%) are arbitrarily chosen by us, so this measure can in time change as we understand more of the risks involved. We can use this metric to evaluate the progress in time and to compare one over the other using a common amount set.

The following external network ranges 200.46.227.224/28, 200.90.137.80/28, 200.46.80.104/29, 200.46.19.96/29 for BANVIVIENDA were scanned for vulnerabilities.

The following table indicates the external vulnerability metric.

Total IP's Scanned	IP's Vulnerable
15	10

Risk Distribution				
Critical	High	Medium	Low	Total
0	4	25	9	38

According to the metrics:

RV= 0.287719298

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

External listing of vulnerabilities by condition:

Host	High	Low	Medium	Total
200.90.137.87	1	2	5	8
200.90.137.89	1	2	5	8
200.90.137.83	1	1	3	5
200.46.227.230	0	1	3	4
200.46.19.100	1	1	1	3
200.90.137.91	0	0	3	3
200.90.137.94	0	1	2	3
200.90.137.84	0	1	1	2
200.46.19.98	0	0	1	1
200.46.227.227	0	0	1	1

The following table provides a comparison of persistent external vulnerabilities of the current month and previous month.

host-ip	Previous Month	Current Month
200.46.19.100	3	3
200.46.19.98	1	1
200.46.227.227	1	1
200.46.227.230	4	4
200.90.137.83	5	5
200.90.137.84	2	2
200.90.137.87	8	8
200.90.137.89	8	8
200.90.137.91	3	3
200.90.137.94	3	3

Please view Recommendations for more details. This can be seen on the GLESEC MEMBER PORTAL (GMP).

Vulnerability Categories

The following table indicates the categories that we use for vulnerabilities as a way to provide context to them and facilitate the prioritization of how to handle remediation.

Preliminary Analysis	Firewalls	Network Devices
SMB/NetBIOS	SSH Servers	Malformed Packets
Simple Network Services	Mail Servers	Proxy Servers
Policy Checks	SQL Servers	Wireless AP
Web Servers	FTP Servers	Webmail Servers
RPC Services	Server Side Scripts	NFS Services
Backdoors	SNMP Services	Printers
Encryption and Authentication	DNS Servers	

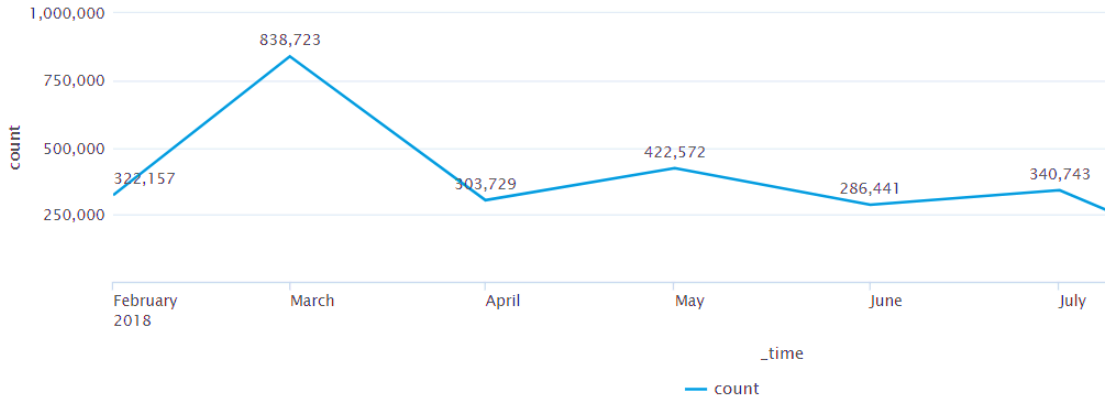
Based on the above the following table shows a matrix of the total internal vulnerabilities by category.

Category	Critical	High	Medium	Low	Total
General		0	23	8	31
Service detection		4	0	0	4
Misc.		0	1	1	2
Windows		0	1	0	1

THREATS

GLESEC uses its MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR and MSS-UTM to determine threat intelligence activity.

The Threats as reported by the MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR, MSS-UTM for this month there are a total of 340,743 attacks denied by the rules of the firewall.



We have noticed an increase in attack activity of 19% since last month. We recommend BANVIVIENDA to review the activity of the devices where these events are recorded.

There was an increase in the number of denials of 19% compared to the previous month (286,441). An important number of attacks that can be considered recognition are scanned.

The denials of access attempts come from countries such as:

- China (29%), Russia (26%), the United States (17%) and Brazil (8%).

During this month the addresses to which access attempts have been denied are:

- 209.97.180.124
- 103.99.2.120
- 62.32.81.84

- 200.46.73.116
- 200.46.239.19
- 200.46.179.178

All attacking addresses tried to access hosts 200.46.19.98 and 200.46.227.227, most attacks are directed to port 23 (Telnet), followed by port 80 (HTTP) and port 22 (SSH).
The attacking addresses 58.218.205.75 and 103.99.82.48 are the ones that have been presented since the previous period.

The network activities are: Network access point, IKE and IPsec, user session, access lists, IP Stack and NAT and PAT, which were noticed during the month.

Equipment monitored during this month:

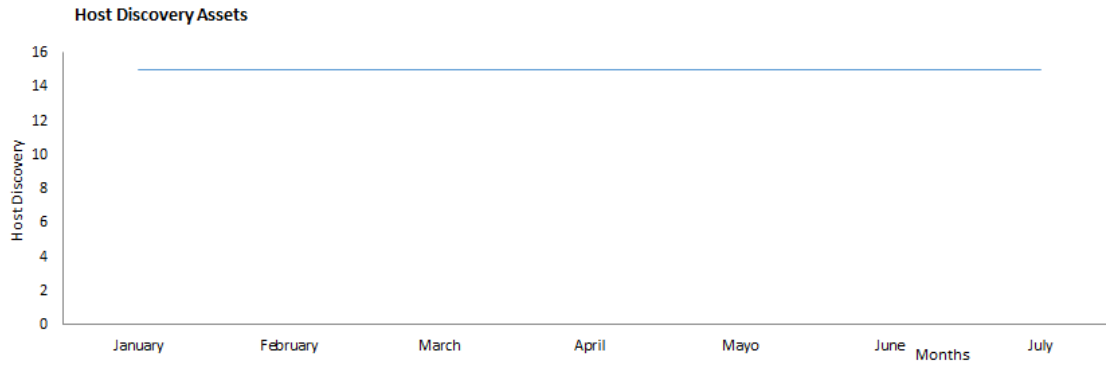
- 200.46.227.227,200.46.19.98,172.16.230.196,150.150.1.147,10.100.202.204, 10.100.210.68, 150.150.1.112, 150.150.1.120, 10.100.201.1 and 192.168.1.1

ASSETS

The MSS-VM(E/I), MSS-EPS conduct weekly testing. The MSS-VM(E/I) identify network assets while the MSS-EPS identify applications. Depending on the contracted services is the listing that can be provided of system or application assets.

We believe that we cannot protect what we don't know and to know the assets (systems and applications) is critical to having a sound cyber security practice. Therefore, we encourage you to verify the information that we provide and let us know if anything is suspicious or just not right. We can work with your organization to create a baseline that can be used to identify deviations. Please contact our GOC for assistance in this matter.

The following histogram shows the total of systems discovered in six months in the perimeter of your organization.



Knowing what's on your network is extremely important. Our monitoring team at our GOC has been keeping track of all these host discovery results and has found nothing unusual.

COMPLIANCE

The MSS-EPS or Managed End Point Security Service is a Compliance and Remediation Service. For compliance we understand the testing, monitoring and alerting of deviations of the parameters of all "hosts" and "servers" in the organization from established baselines. These baselines can be created to support specific outside requirements or internal best-practice guidelines. The MSS-EPS can monitor deviations to these baselines and also "enforce" compliance with these.

The services that provide us with information for this section have not been contracted

CYBER SECURITY VALIDATION

Security Validation implies the validation of the entire security by conducting testing with simulated attacks. This is conducted with the Managed Breach Attack Simulation Service (MSS-BAS). The MSS-BAS is a collection of advanced pre-exploitation, post- exploitation and awareness testing services. The testing is on real targets based on simulated attacks; therefore these provide conclusive (no false positive) results. The different attack vectors test the organization's configurations, countermeasures, implementations and ability to respond in a continuous fashion producing valuable intelligence and recommendations.

The services that provide us with information for this section have not been contracted.

TRUSTED ACCESS

The new IT model brings with it a greater attack surface, comprised by employees

that use their own devices for work, while working remotely. The proliferation of cloud applications for nearly every business need has also contributed to increased technical complexity. These days, attackers can expose much different vulnerability in multiple vectors — in a single attack. Traditional security is designed to address separate, siloes attacks, making these solutions ineffective against modern threats. These new threats center on gaining remote access to your apps and data — whether it's with stolen passwords or exploited known vulnerabilities targeting your users, their out-of- date devices, cloud applications and remote access software.
The Managed Trusted Access Service (MSS-TAS) is a holistic security service to (a) ensure that the users' access is trusted (valid user) and (b) the devices used by the user to authenticate meet the organization's security standards.

The services that provide us with information for this section have not been contracted.

Recommendations

GLESEC recommends for BANVIVIENDA to address the following

1. Take immediate action on the recommendations detailed in this report.

2. Take some time to review the incidents reported during this period, in addition to those included in this and previous reports, and let us know if these are part of the normal function of your systems.

3. Most of the vulnerabilities found can be hardened if the best practices for SSL / TLS implementation are taken into account where old versions of SSL are not allowed, in the same way, the use of known vulnerable encryption suits (eg example, RC4) should not be allowed. Pay special attention to the following hosts: 200.90.137.87, 200.90.137.89, 200.46.227.230 and 200.90.137.83.

4. It is important to set up valid certificates, because there are attack methods that involve falsifying a service such as a web mail and because the official service does not have a valid certificate, it is possible that clients believe that the attackers service is the official one that could cause the theft of credentials, the leakage of data, among others.

5. We strongly recommend not allowing any connection through telnet, (not open, it is always better to be filtered if not used) to any of your systems, regardless of whether the connections are established within the local network or through the Internet. This port is attacked around 57%.

6. If the hosts 200.46.227.227 and 200.46.19.98 are listening on port 80, we strongly recommend migrating to port 443, because even though connection attempts from outside have been interrupted, we have recorded many attempts from several IPs such as: 31.184 .195.108, 35.233.37.65, 47.91.216.243 and 66.74.78.94.

7. Take note of the aggressive Internet Key Exchange (IKE) solution process with pre-shared key, which is described in the section Vulnerabilities by severity of the technical report on hosts 200.46.227.227 and 200.46.19.98.

Intelligence Section Per Service Module

Managed Vulnerability Service (MSS-VM) Intelligence Section

The Managed Vulnerability Service (MSS-VM) enables organizations to minimize the risk of vulnerabilities by quickly discovering weaknesses, measuring the potential risk and exposure, reporting, providing remediation information necessary to mitigate those risks on an on-going basis and facilitating reporting and compliance with regulations and best practices.

The purpose of this section is to highlight intelligence gathered from this and other 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 following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service.

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.

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

Vulnerability Score

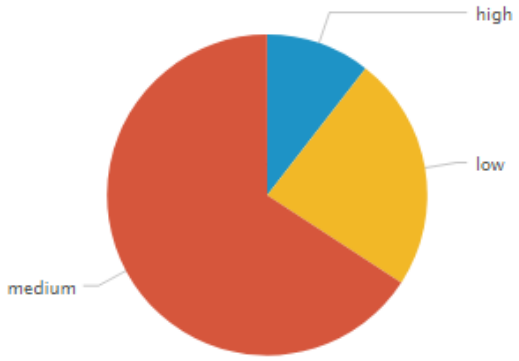
The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed 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 labeled as:

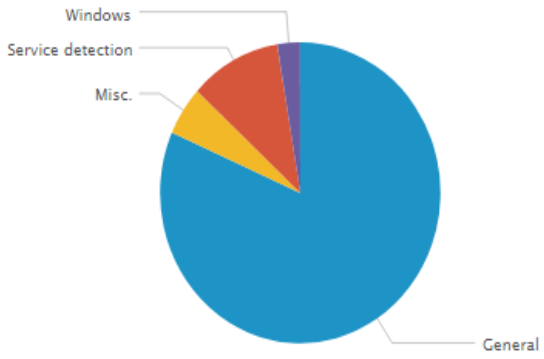
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

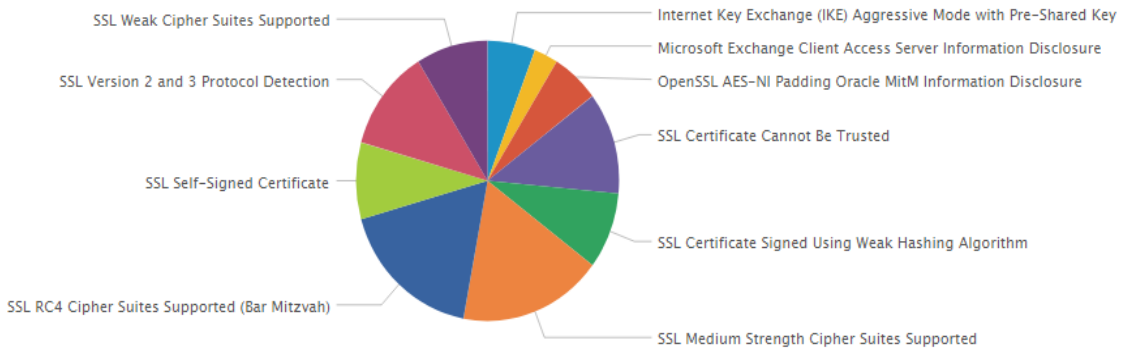
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



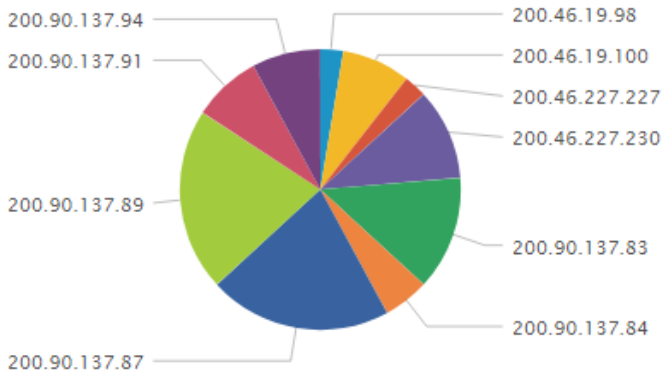
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



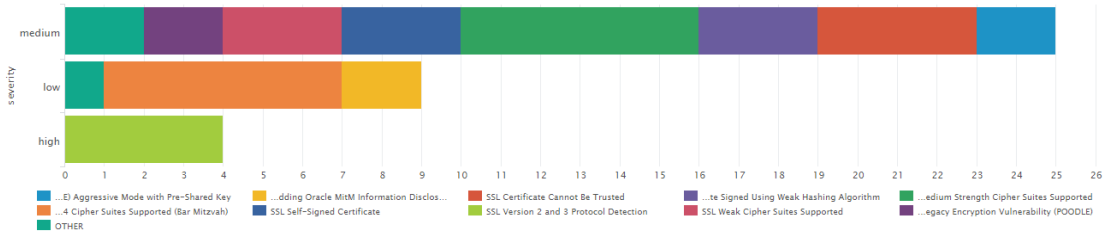
Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



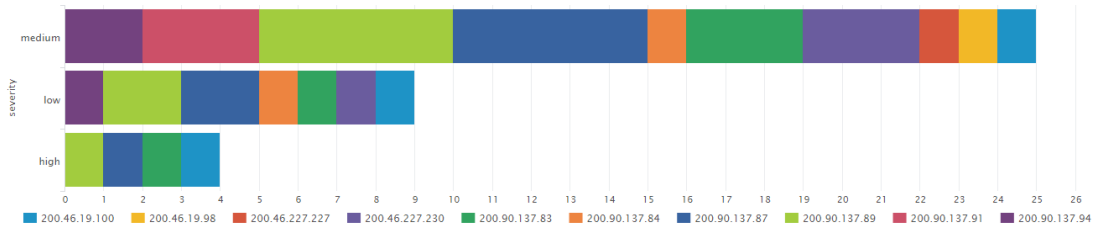
Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period



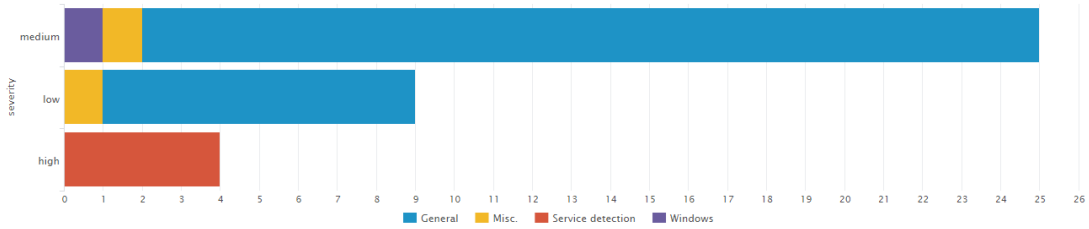
Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



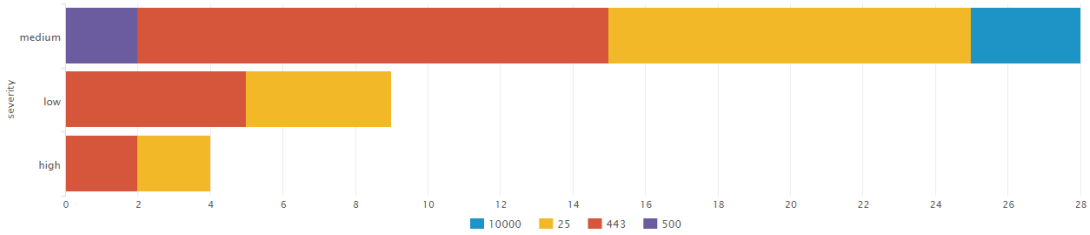
Graph: Vulnerability Risk by Host
This report illustrates the vulnerability risk and count by category discovered this report period



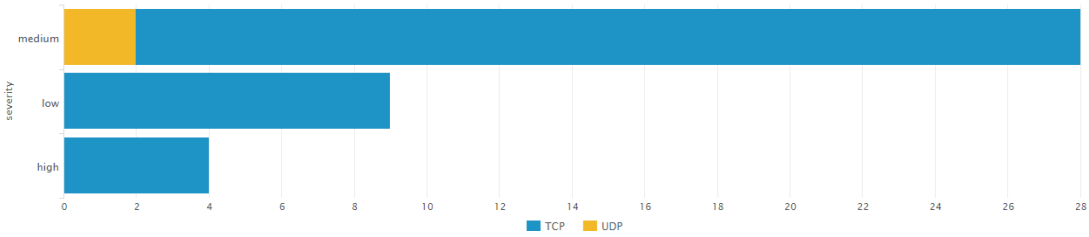
Graph: Vulnerability Risk by Category
This report illustrates the vulnerability risk and count by category discovered this report period



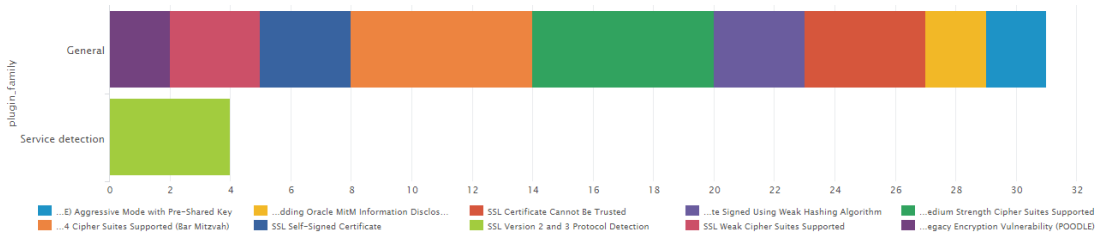
Graph: Vulnerability Risk by Port
This report illustrates the vulnerability risk and count by port discovered this report period



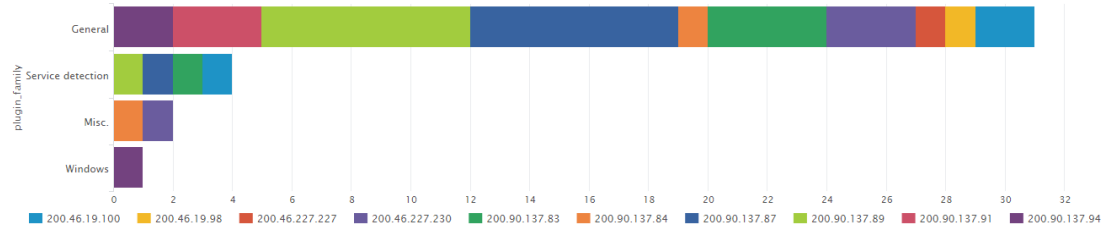
Graph: Vulnerability Risk by Protocol
This report illustrates the vulnerability risk and count by protocol discovered this report period



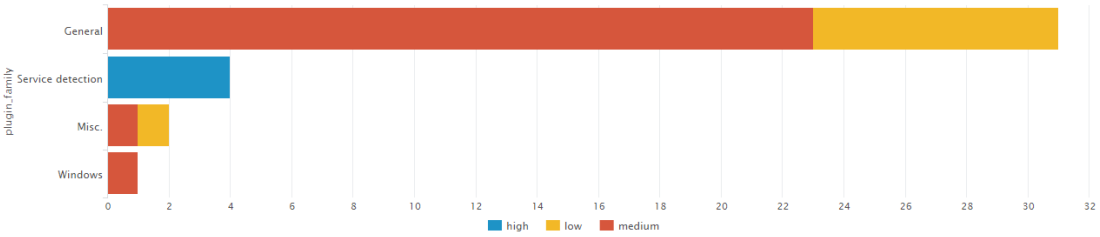
Graph: Vulnerability Category by Vulnerability Name
This report illustrates the vulnerability category and count by vulnerability name discovered this report period



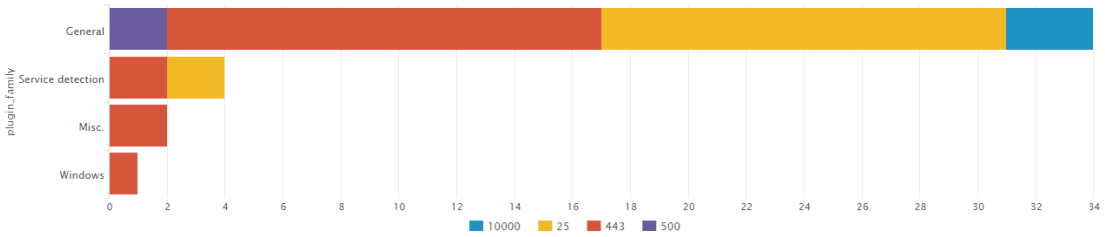
Graph: Vulnerability Category by Host
This report illustrates the vulnerability category and count by host discovered this report period



Graph: Vulnerability Category by Risk
This report illustrates the vulnerability category and count by risk discovered this report period

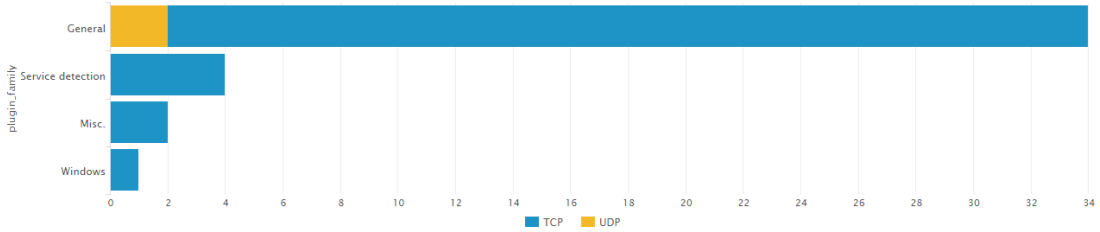


Graph: Vulnerability Category by Port
This report illustrates the vulnerability category and count by port discovered this report period



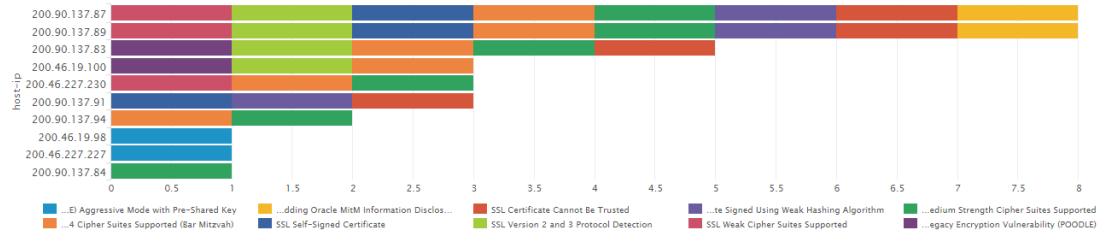
Graph: Vulnerability Category by Protocol

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



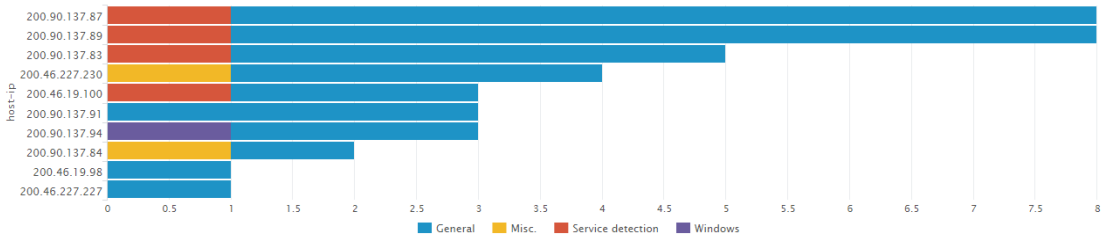
Graph: Host by Vulnerability Name

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



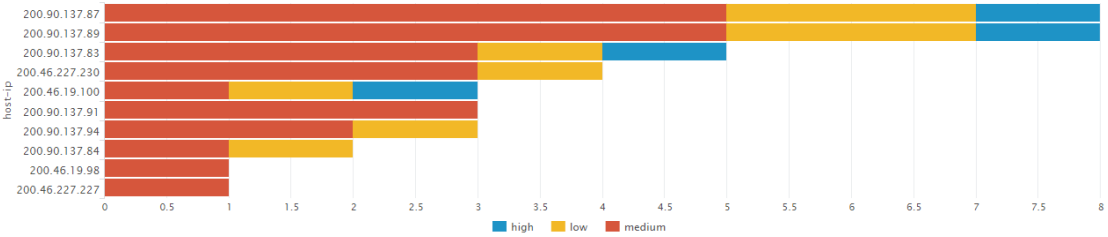
Graph: Host by Vulnerability Category

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

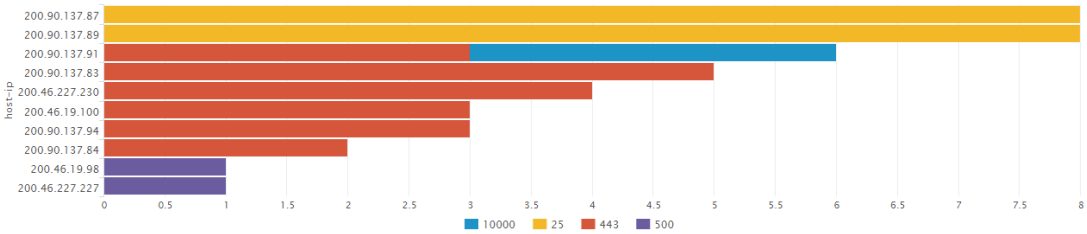


Graph: Host by Vulnerability Risk

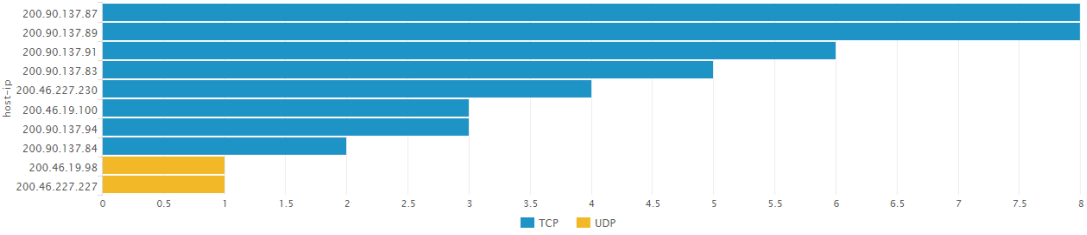
This report illustrates the vulnerability risk and count by hosts discovered this report period



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



USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

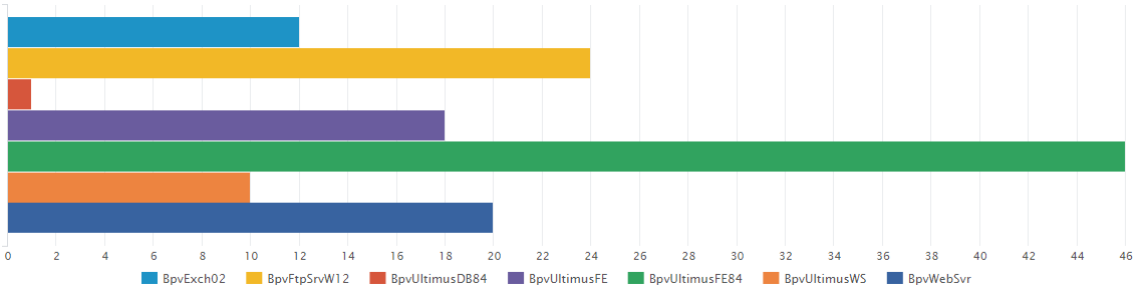
Managed End Point Incident Response Service (MSS-EIR) Intelligence Section

The MSS-EIR is a preventive detection and response and a forensic service to identify without signatures and mitigate an attack to the end-points and servers of an organization. The service works by actively seeking malicious activity in the customer's network based on suspicious behaviors (not based on signatures). This technology allows our analysts to detect malicious software that may have evaded existing security countermeasures. At the same time, we conduct investigations by responding to a security alert – this service is based on leveraging a powerful investigation platform to shorten the investigation time, respond to more incidents and get to the root cause of each incident.

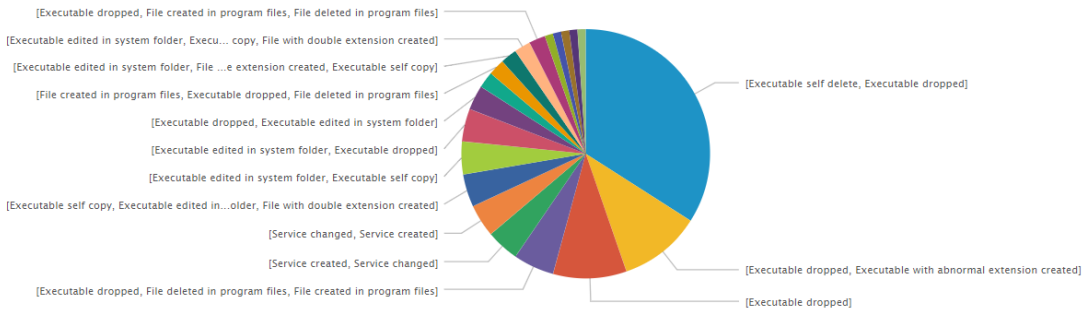
The purpose of this section is to highlight intelligence gathered from this and other services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat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

The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service. The dashboards will be presented in the next report.

Graph: Top Agents With Suspicious behavior
This grafic shows the agents that register the most amount of events



Graph: Top Suspicious behavior List
Next table represents the most frequents suspicious behavior registered from the agents



Top Events Registered

During this period in our GOC, we have received fewer alerts compared to the previous month, a total of 282 alerts received from BANVIVIENDA, these generated by the following agents:

- BpvUltimusDB84
- BpvFtpSrvW12
- BpvUltimusFE
- BpvExch02
- BpvUltimusWS

The most notable behavior during this period is the following:

- Executable self-deletes, Executable dropped
- Executable dropped, Executable with abnormal extension created
- Executable dropped
- Executable dropped, File deleted in program files, File created in program files
- Service created, Service changed

mscorsvw.exe
Behavior of this entity is the following:

- mscorsvw.exe->Executable dropped-> microsoft.windows.design.developer.wpf.ni.dll *
- mscorsvw.exe->File with double extension created-> microsoft.windows.design.developer.wpf.dll*
- mscorsvw.exe->Executable edited in system folder>microsoft.windows.design.developer.wpf.ni.dlll *

MD5: 7761fbd826c16a007d6386fbfb846241
Process directory: *c:\windows\microsoft.net\framework\v4.0.30319*

The target entity changes from one alert to the other, but the behavior is the same. This process corresponds to the .NET Runtime Optimization Service; This behavior was identified repeatedly during certain days of the month of July.

wftptray.exe
It is one of the alerts we receive daily.
MD5: b97ea04bf5b3359e209bb0d73d78730f
Process directory: c:\program files (x86)\wing ftp server\
Severity: Medium
This is a process generated by an FTP server, we believe that it is part of the daily activities of the client.

Tiworker.exe
Behavior of this entity is the following:

- PMtiworker.exe-> Executable with abnormal extension created->Executables
- tiworker.exe-> Executable edited in system folder->Executables

MD5: 2b902ea3056aabf8eccb689d434ae2c9
Agent: BpvWebSvr
Process command line: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.18384_none_fa1d93c39b41b41a\TiWorker.exe –Embedding
Process directory: c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.18384_none_fa1d93c39b41b41a\
User: Local System
6/5/2018 8:58:53

This process is responsible for searching and installing updates in Windows; it is also used when adding or deleting a new feature in Windows systems, we can conclude that this is the reason why this process is executed repetitively in your systems.

lnsscomm.exe
MD5:ee4d8af19d68111fa1b1af39dcb4deca
Process directory: c: \ program files (x86) \ gfi \ languard 12 agent \
Agent: BpvUltimusWS
This is a process generated by languard agent 12

Teamviewer_.exe
It is one of the alerts we receive daily.

- Behavior of this entity is the following:

- teamviewer_.exe-> Executable dropped-> teamviewer_desktop.exe
- teamviewer_.exe-> Executable with abnormal extension created->tvmonitor.sy_
- teamviewer_.exe-> Executable path written to registry-> teamviewer_resource_en.dll
- teamviewer_.exe-> Executable self copy-> userinfo.dll
- teamviewer_.exe-> Executable self copy-> system.dll
- teamviewer_.exe-> Executable self copy-> tvgetversion.dll

MD5: 6f2d7f7e6b1b2af8c04b6ecbc8cb6aa5
Agent: BpvUltimusDB84
Alert: 98
Severity: Medium
Process command line:
C:\Users\BPVSVR~1\AppData\Local\Temp\1\TeamViewer\TeamViewer_.exe /RUN
Process directory: c:\users\bpvsvr~1\appdata\local\temp\1\teamviewer\
User: bpvsvradm

This process is generated in another agent:
MD5: a889e7974a7b9a41af88b77e17627d26
Agent: BpvUltimusDB84
We have received in this period a total of 20 alerts related to this process.

csc.exe
behavioral:

- csc.exe -> Executable Dropped -> app_web_acrnqef2.dll

MD5:eb70bf071ec54bf0c29408ffdb89e3bb
MD5:8d3c9fc98fe9770d6dc2caa289449db7
MD5:95e08f018b0eb4f76ef7368610ce49ce
Severity: Medium
Execution Path: c:\windows\microsoft.net\framework\v4.0.30319\
Process command line:
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths "C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\utimus.persona\c1d3a94e\6f313c81\acrn qef2.cmdline"

Managed Event Correlation Service (MSS-SIEM) Intelligence Section

The MSS-SIEM is an event correlation solution based on GLESEC's Multi-security Appliance ("GMSA") which when connected internally to the network allows sources to receive the data to be correlated and this generates intelligence, alerts and reporting, incident handling and management.

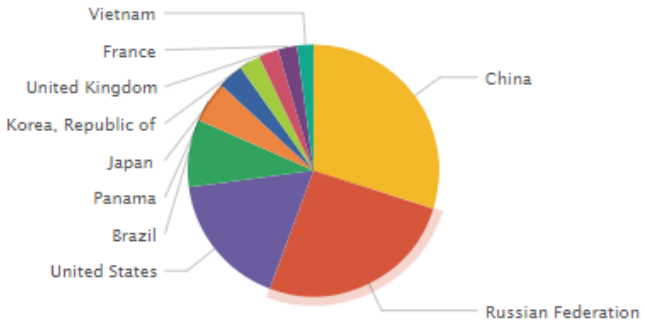
The purpose of this section is to highlight intelligence gathered from this and other services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat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

The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service.

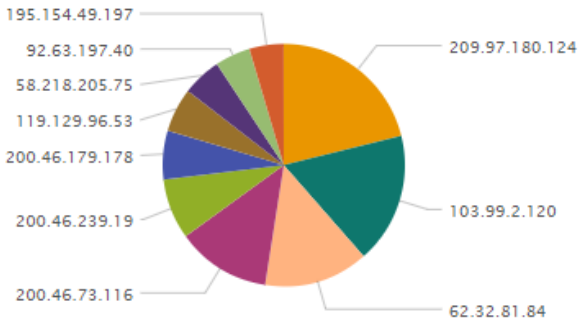
Graph: Denial Connections
This graphic shows the denied connections in the firewall rules

340,743

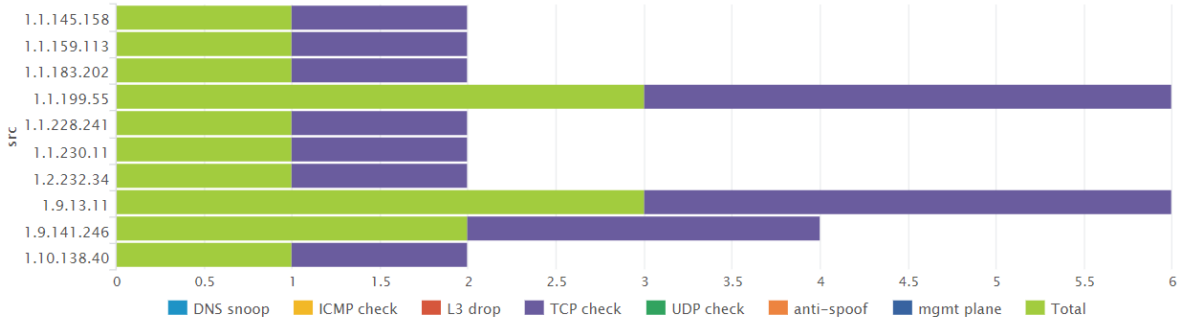
Graph: Top Country Blocked
This graphic shows top attacking countries blocked.



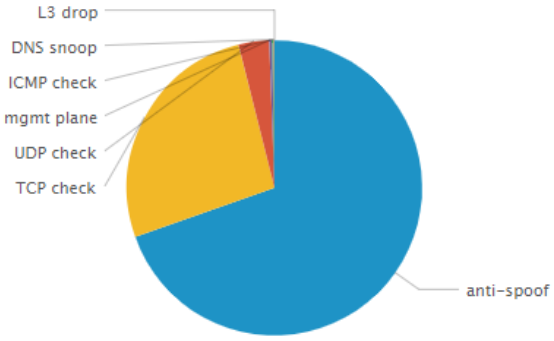
Graph: Top Sources
This graphic shows top attack sources blocked



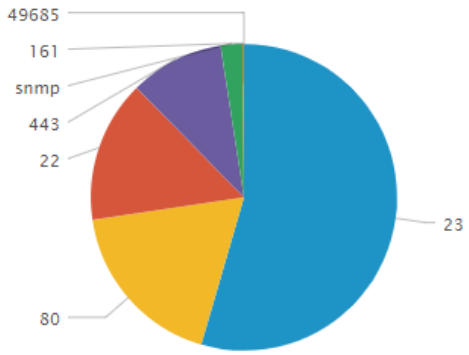
Graph: Top Attacks Blocked by sources
This graph shows the categories of attacks by attack sources.



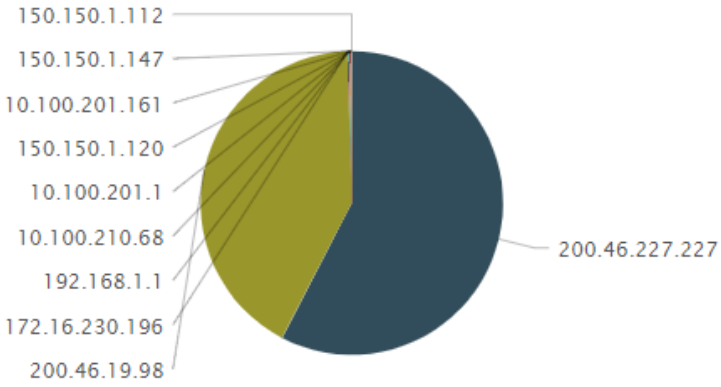
Graph: Top Type Attacks
This graphic shows the top categories of attacks.



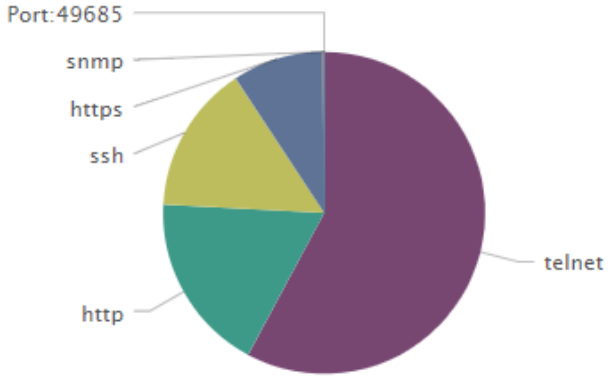
Graph: Top Attacked ports
This graphic shows the top attacked ports.



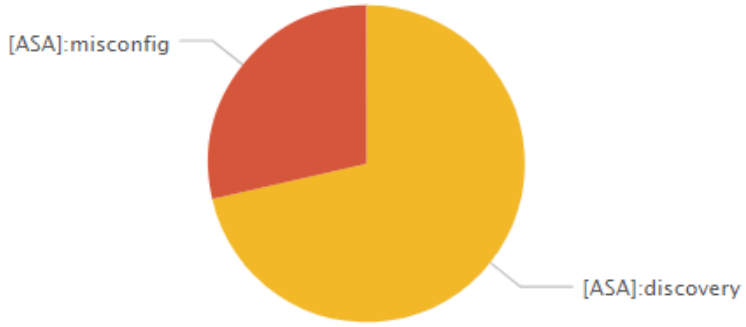
Graph: Top Destinations
This graphic shows the top attack destinations denied



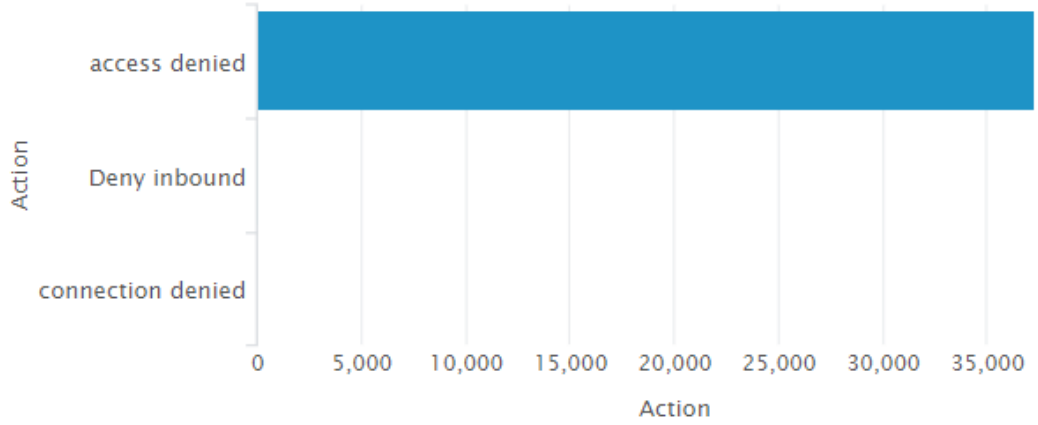
Graph: Top Services
This graph provides the top services blocked by in and out firewall rules.



Graph: Top Threats
This graph shows the top threat category denied.



Graph: Actions Taken
This graph shows the most frequent actions taken in order to deny attacks.



Graph: Network Activity
This graph shows the most frequent traffic categories present in the network.

vendor_definition	count	percent
Network Access Point	49043584	99.303278
IKE and IPsec	49043584	99.303278
User Session	340773	0.689996
Access Lists	303410	0.614344
IP Stack	3232	0.006544
High Availability (Failover)	90	0.000182
NAT and PAT	30	0.000061

Cyber 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 services under contract, Change Management, Incident Response activities and Consulting Activities.

PROFESSIONAL SERVICES ACTIVITY

Below we outline the usage of the consulting retainer of professional services activity for the corresponding month. In this we show the total billable and non-billable hours, the contracted retainer, the total hours used in the month and the hours above the retainer.

Billable consulting hours	Non-billable consulting hours	Contracted retainer hours	Total Hours utilized	Hours above retainer
0	0	1	0	0

TICKET ACTIVITY

In this section we report on all the change management and incidents tickets for the month.

Monthly Reports Banvivienda 2018-07-01[..] printed by De

Ticket#	Title	Created
2018071010000087	Reporte de Operaciones Junio 2018	2018-07-10 16:58:28
2018070510000042	TLP AMBER BANVIVIENDA INCIDENT REPORT 1181	2018-07-05 17:54:50

During this period of the month, our operations center notified an incident report related to the TLS version in some of its systems.
All the services operated normally during the month of July.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Definitions

High Vulnerabilities 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 Vulnerabilities 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 Vulnerabilities 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.

SMB/NetBIOS vulnerabilities could allow remote code execution on affected systems. An attacker who successfully exploits these vulnerabilities could install programs; view, change, or delete data; or create new accounts with full user rights. Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

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

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

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

Authentication and encryption are two intertwined technologies that help to insure that your data remains secure. Authentication is the process of insuring that both

ends of the connection are in fact “who” they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to ensure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well.

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

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com