OPERATIONS & INTELLIGENCE CYBER SECURITY REPORT

BANVIVIENDA

March, 2018

CONFIDENCIAL

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 hacktivism 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	August 1, 2018
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM	YES	August 1, 2018
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EIR	YES	August 1, 2018
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 March 01 to March 31, 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 / RIESGO
	VULNERABILITIES / VULNERABILIDADES • MSS-VM Service
	THREATS / AMENAZAS • MSS-APS; MSS-EPS; MSS-SIEM; MSS-EIR; MSS-UTM
	ASSETS / ACTIVOS • MSS-VM; MSS-EPS
	COMPLIANCE / CUMPLIMIENTO • MSS-EPS
	SECURITY VALIDATION / VALIDACION • MSS-BAS
	TRUSTED ACCESS / ACCESS CON CONFIABILITIDAD • MSS-TAS

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.

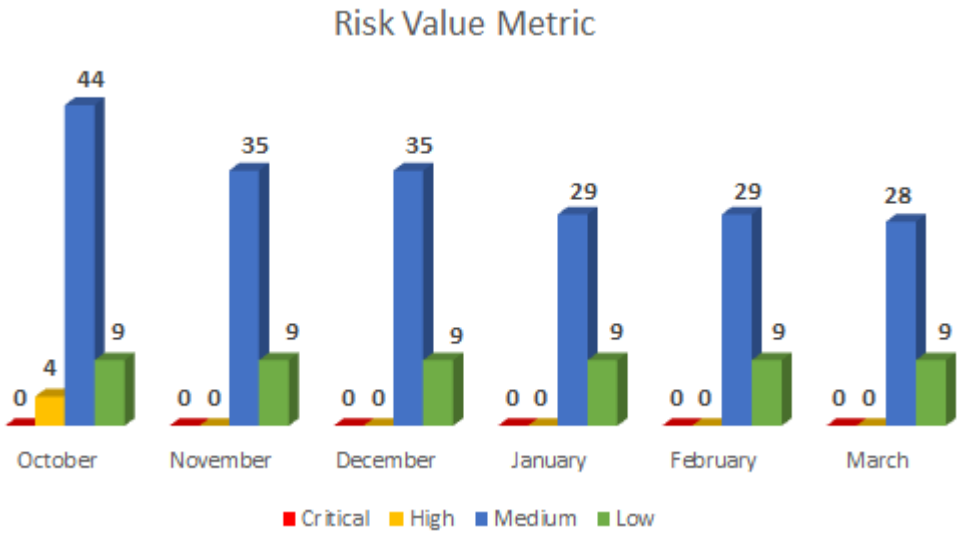
One of GLESEC's foundational columns is basing all its activities to support RISK determination and mitigation. What any organization should want to know if what is their level of RISK, and in this case in particular to cyber-security. Cyber-Security RISK has a direct impact to the business and as such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

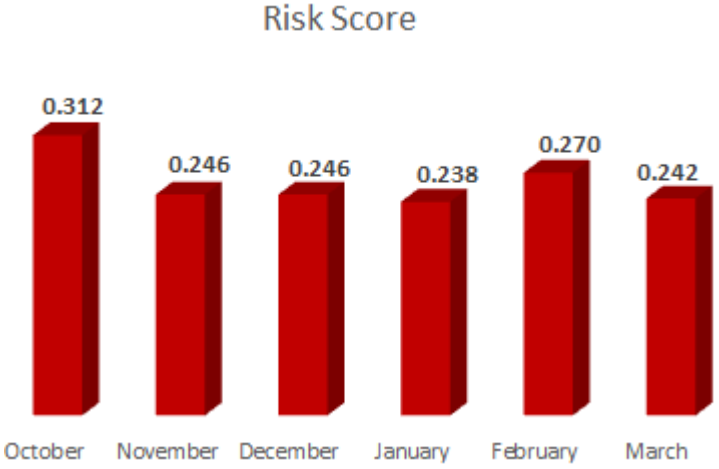
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

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.

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



This vulnerabilities are very similar, as the ones reported in past months



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.

Overall the vulnerabilities for BANVIVIENDA this period have been 0 critical, 0 high, 28 medium and 9 low risk. There are many medium risk vulnerabilities which were found on many hosts, please refer to MMS-VM intelligence section for more detail about specific hosts. Medium risk vulnerabilities found were classified as SSL Medium Strength Cipher Suites Supported, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah), and SSL Certificate Signed Using Weak Hashing Algorithm. This means that attackers could take advantage of any of those and attempt to cause and negative impact to your Organization.

Ports 443 and 25 are the most vulnerable ports for this period; this is because many vulnerabilities were found which are related to them and categorized as medium risk.

<u>Risk Value Metric</u>

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.

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

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	9

Risk Distribution				
Critical	High	Medium	Low	Total
0	0	28	9	37

According to the metrics:

RV= 0.241621622

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	Critical	High	Medium	Low	Total
200.90.137.87			6	2	8
200.90.137.89			6	2	8
200.90.137.83			4	1	5
200.46.227.230			3	1	4
200.46.19.100			2	1	3
200.90.137.91			3	0	3
200.90.137.94			2	1	3
200.90.137.84			1	1	2
200.46.227.227			1	0	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	
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	

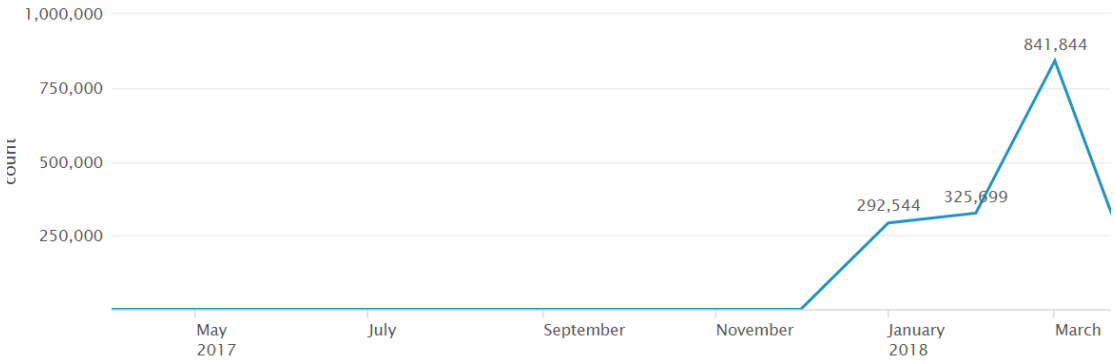
Based on the above the following table shows a matrix of the total internal vulnerabilities by category.

plugin_family	low	medium
General	8	22
Service detection	0	4
Misc.	1	1
Windows	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 are a total of 841,844 attacks denied by the rules of the firewall.



For this month we see an increase in attack activity of 158.47% from last month. We have noticed in the last three months an increase in failed attacks. We recommend Banvivienda to review the activity of the devices where these activities are generated

Most of the attacks are targeting port 23(Telnet), followed by port 80 (HTTP) and port 443 (HTTPS). About 53% of the attacks are targeting SMTP ports. Having this port open might allow attackers to spread worms and trojans through the network and gain control of network devices.

Attacks were blocked mostly by denying access to the attacker and in other cases, the packets were dropped immediately.

The blocked attacks are, mostly from Brazil, China and United States as the three top sources. A significant number of attacks are scanning which can be considered reconnaissance and is what precedes further attacks.

The host 172.16.230.66 has an activity unusual and persistent to the DMZ-BANVIVIENDA, specifically towards the IP addresses 10.100.201.161, 10.100.201.129 and 10.100.201.169 to port 443 / tcp.

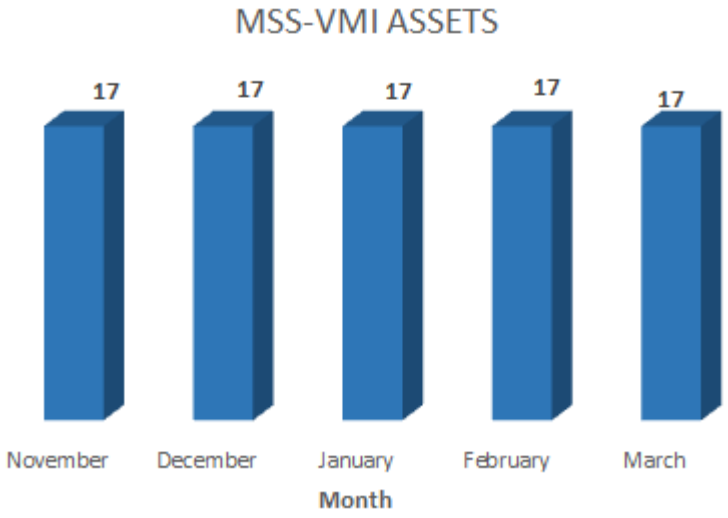
ASSETS

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 past six-month total of number of systems discovered in the perimeter of your organization.

MSS-VME-Host Discovery



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.

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

Recommendations

GLESEC recommends for BANVIVIENDA to address the following

1. Take immediate actions to the detailed recommendations in this report.

2. The majority of the vulnerabilities found can be hardened by taking into consideration the best practices for SSL/TLS implementation where old versions of SSL are not allowed, the same way, the use of known vulnerable cipher suits (e.g. RC4) are not permitted.

3. Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later, in the affected hosts.

4. Create firewall rules that block outside connections to unregistered port 10000, and also take in consideration that port 25 (SMTP) was a frequent attack target. Port 10000 is sometimes used by Webmin and other administration tools, it is also known for being a port used by some worms that use the infected machines to spread spam through the network. Having these ports open might allow attackers to take control of network devices and a way to penetrate the network. This month, both ports have been a frequent target of attacks, this can suggest that the attackers wanted to infiltrate malware that could later send spam campaigns to the network.

5. Change all the active telnet connections to SSH. Telnet is an insecure protocol that sends the information in plain test, SSH encrypts the information before sending it, reducing the risk of a remote attacker obtaining sensitive information.

6. We found vulnerability related to Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key, in our GMP there are more details about the mentioned vulnerability.

7. We recommend conducting the “breach-attack-simulation” to determine the behavior of your organization’s firewalls and other defenses.

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

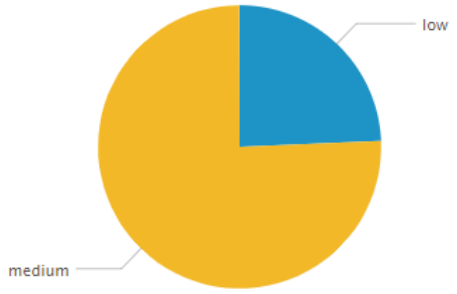
The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed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

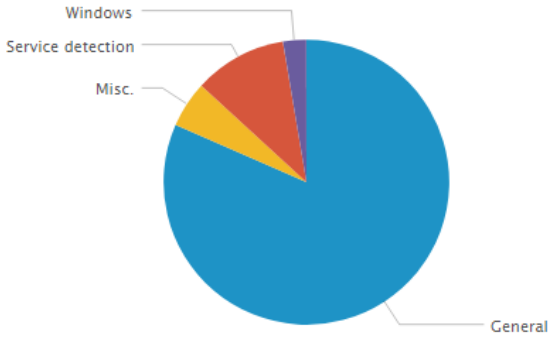
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

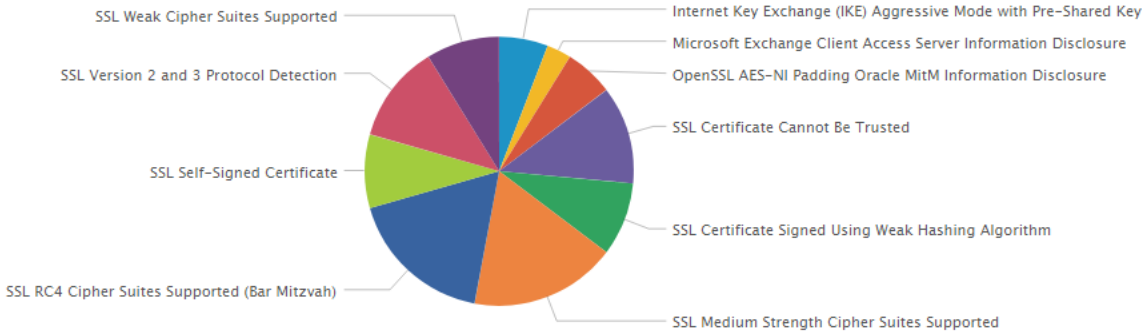
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



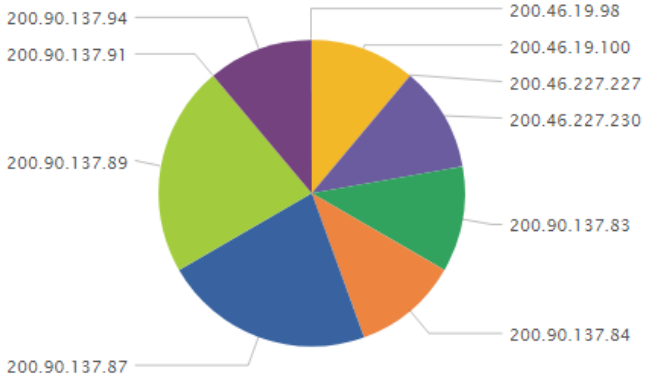
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



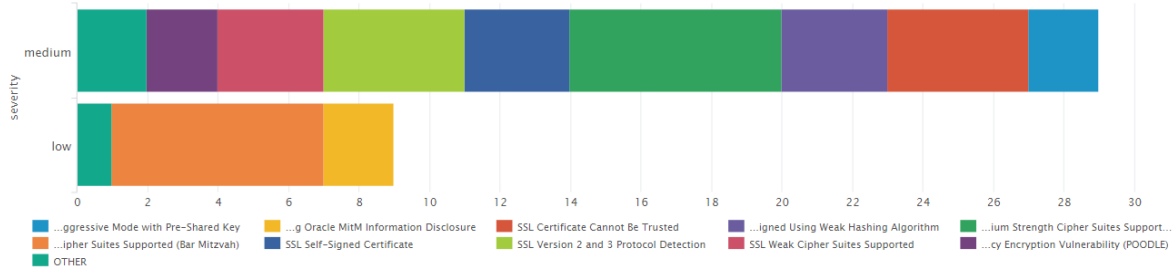
Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



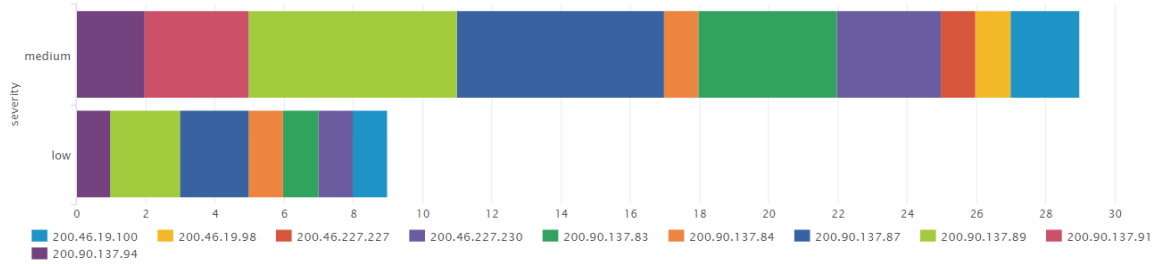
Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period



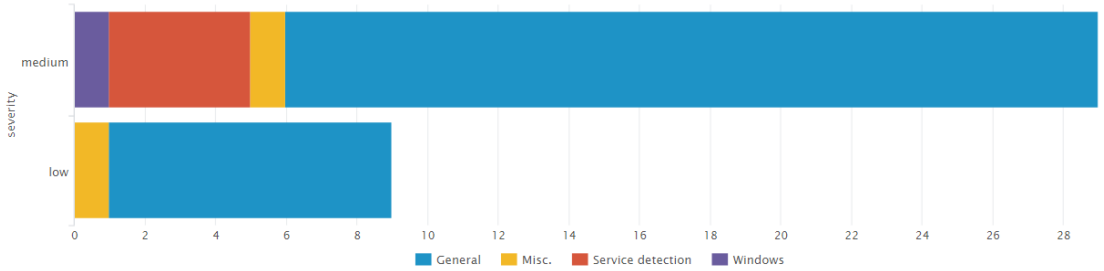
Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



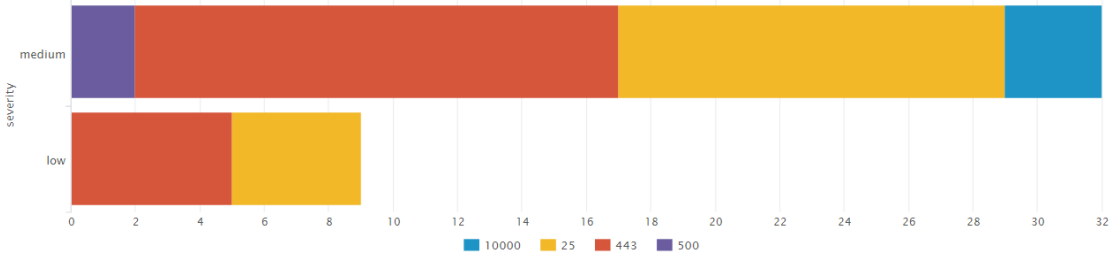
Graph: Vulnerability Risk by Host
This report illustrates the vulnerability risk and count by category discovered this report period



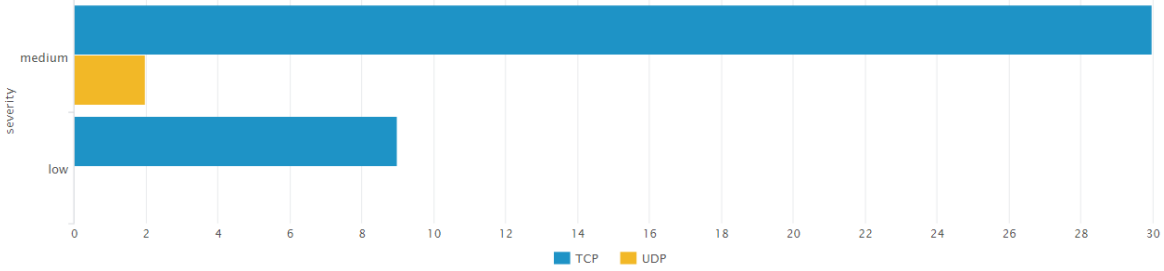
Graph: Vulnerability Risk by Category
This report illustrates the vulnerability risk and count by category discovered this report period



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

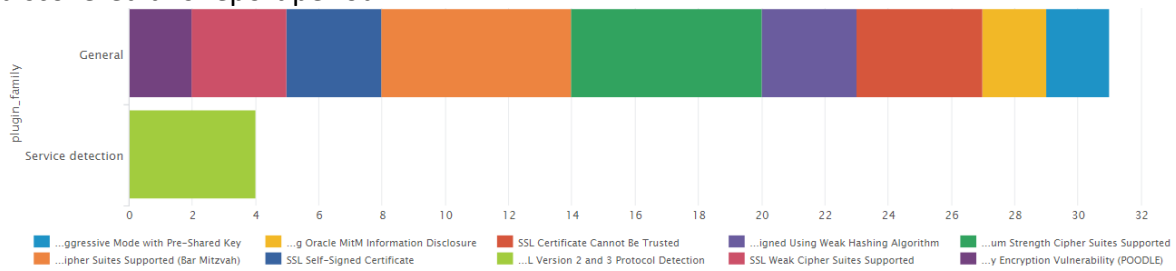


Graph: Vulnerability Risk by Protocol
This report illustrates the vulnerability risk and count by protocol discovered this report period



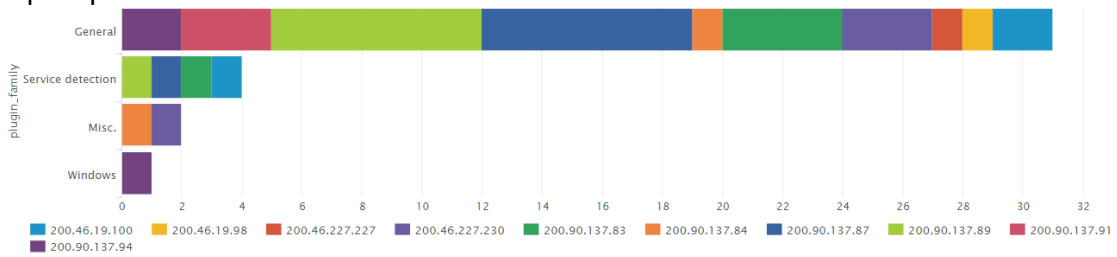
Graph: Vulnerability Category by Vulnerability Name

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



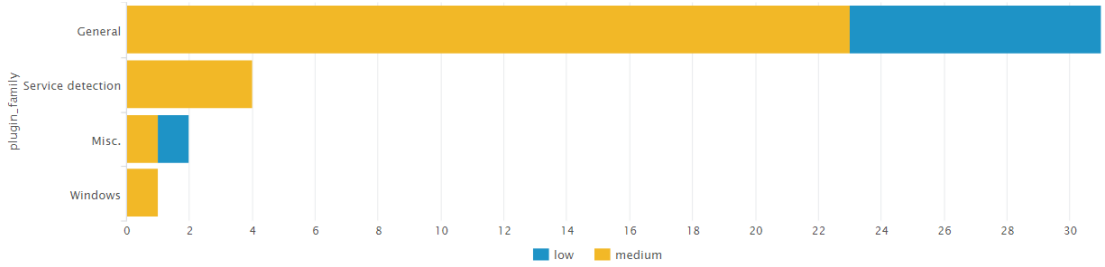
Graph: Vulnerability Category by Host

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



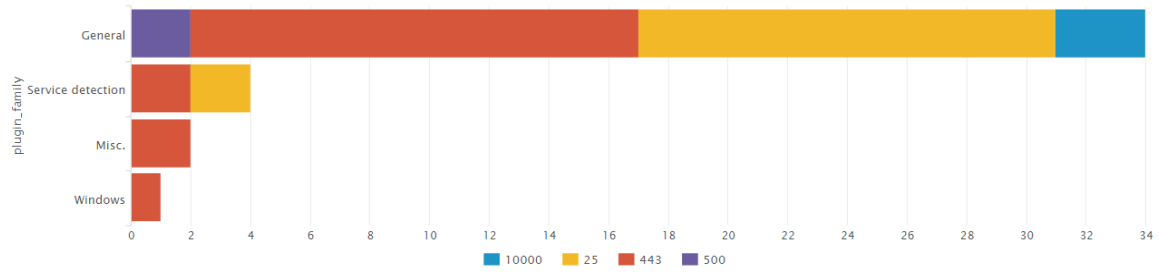
Graph: Vulnerability Category by Risk

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

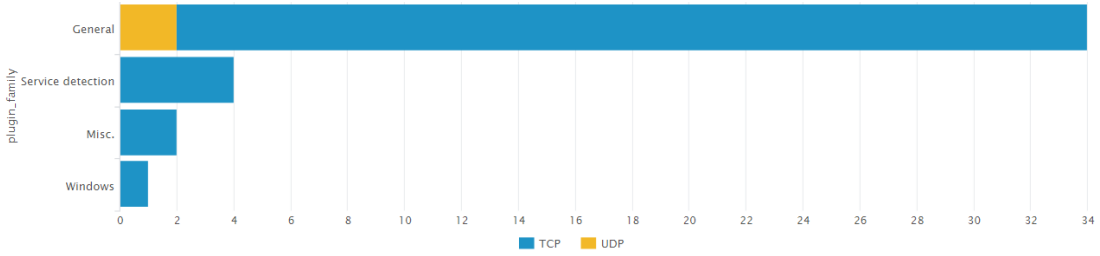


Graph: Vulnerability Category by Port

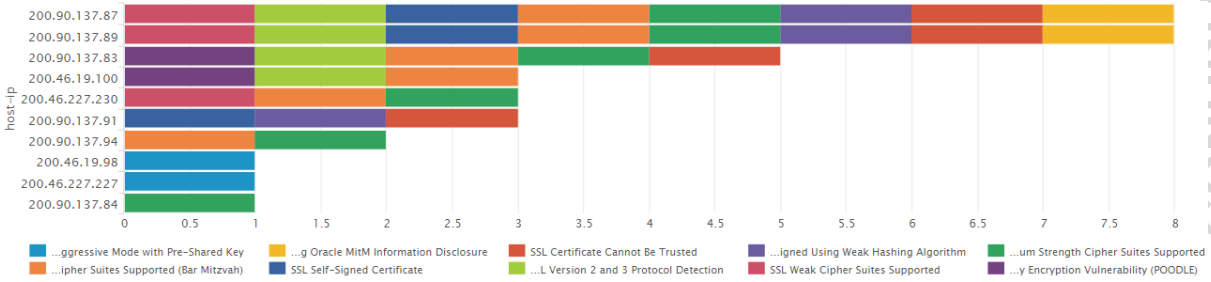
This report illustrates the vulnerability category and count by port discovered this report period



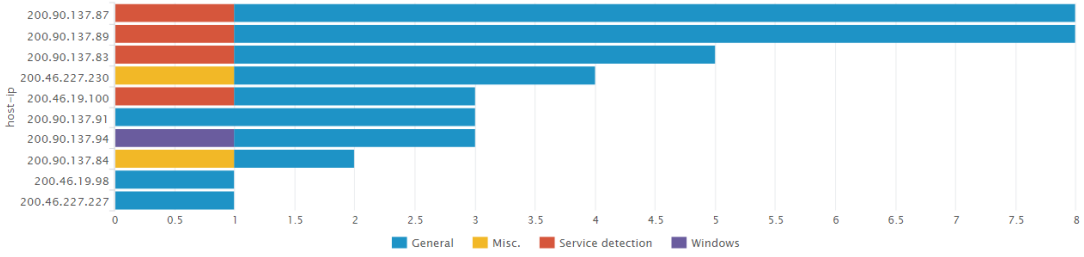
Graph: Vulnerability Category by Protocol
This report illustrates the vulnerability category and count by protocol discovered this report period



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

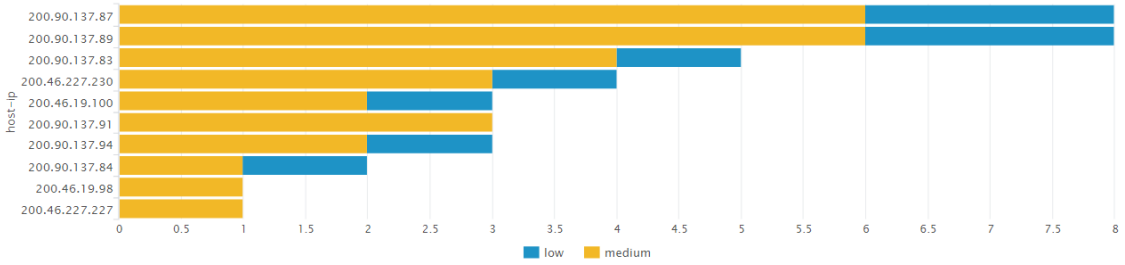


Graph: Host by Vulnerability Category
This report illustrates the vulnerability category and count by hosts discovered this report period



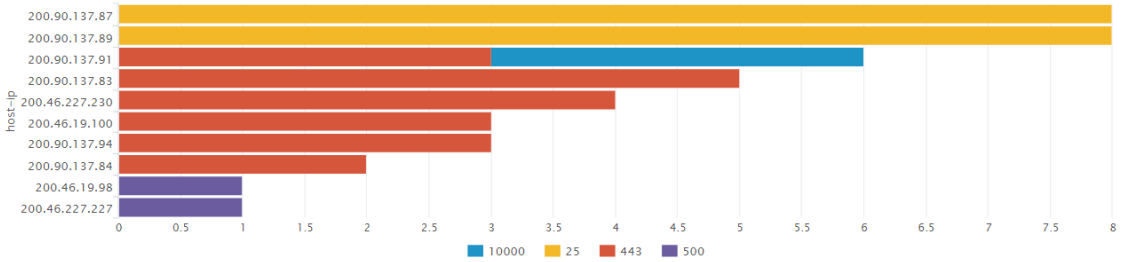
Graph: Host by Vulnerability Risk

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



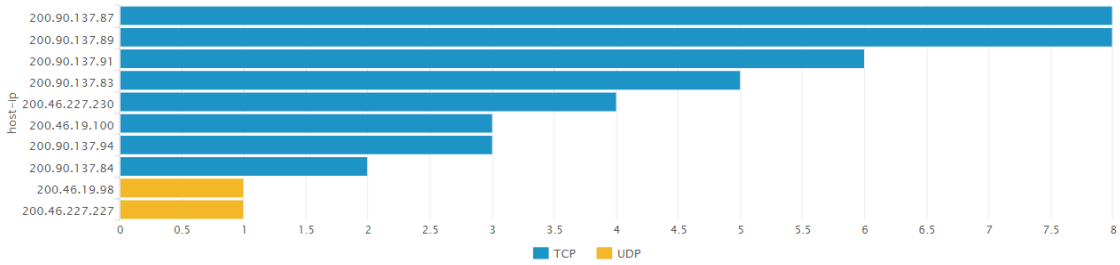
Graph: Host by Port

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



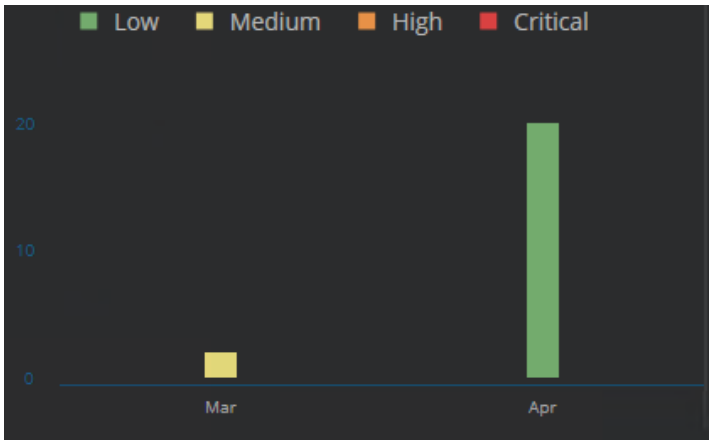
Managed End Point Incident Response Service (MSS-EIR) Intelligence Section

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.

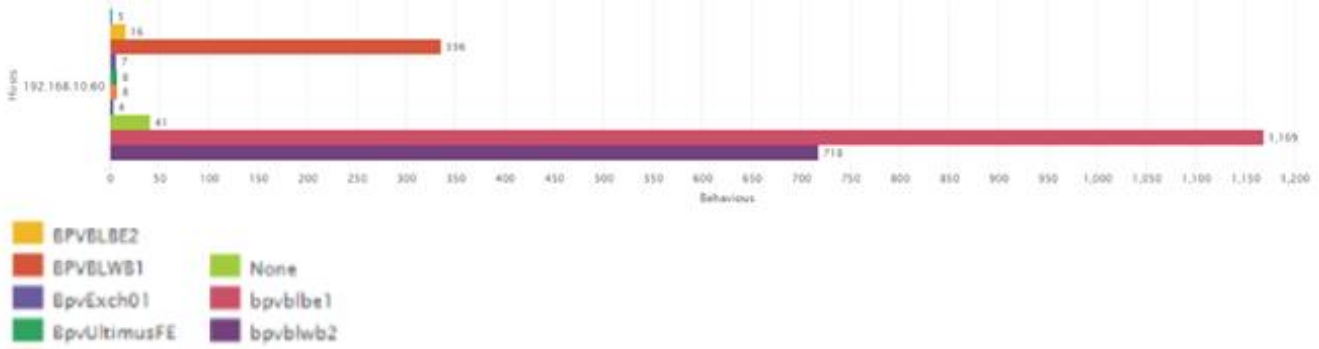
The following graphs are dashboards generated by GLESEC's TIP™ platform. These dashboards are representative of metrics for this service. The dashboards will be presented in the next report.

Graph: Severity by Month



Graph: Top Entities by Severity
This graphic shows the entities found by severity

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

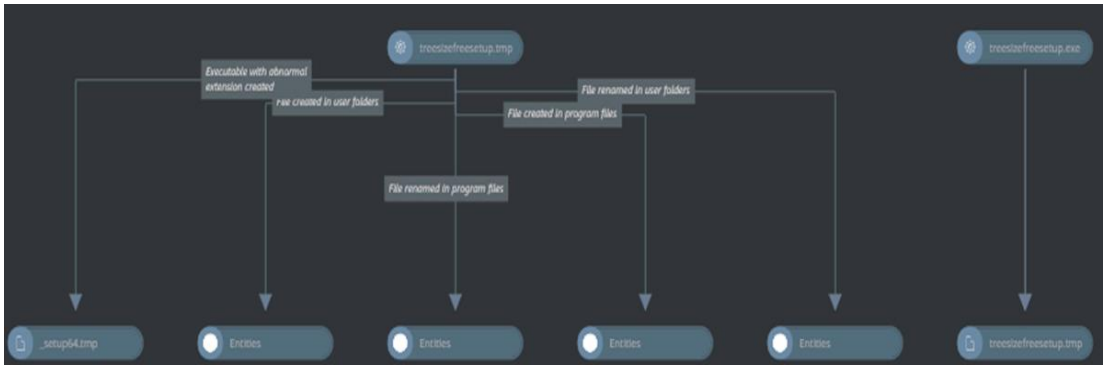
	Behaviors_list	count	percent
1	[]	1532	65.582192
2	[u'Executable dropped', u'Executable edited in system folder']	244	10.445205
3	[u'Executable edited in system folder', u'Executable dropped']	189	8.090753
4	[u'Executable self delete', u'Executable dropped', u'Executable edited in system folder', u'Executable self copy']	57	2.440068
5	[u'Executable dropped', u'Executable edited in system folder', u'File with double extension renamed']	51	2.183219
6	[u'Executable dropped', u'Executable edited in system folder', u'File with double extension created']	35	1.498288
7	[u'Executable edited in system folder', u'Executable dropped', u'File with double extension created']	20	0.856164
8	[u'Executable dropped', u'File with double extension renamed', u'Executable edited in system folder']	19	0.813356
9	[u'Executable edited in system folder', u'Executable dropped', u'File with double extension renamed']	16	0.684932
10	[u'Executable self delete', u'Executable dropped', u'Executable edited in system folder']	15	0.642123
		2276	97.431505

Top Events Registered By High Severity Level

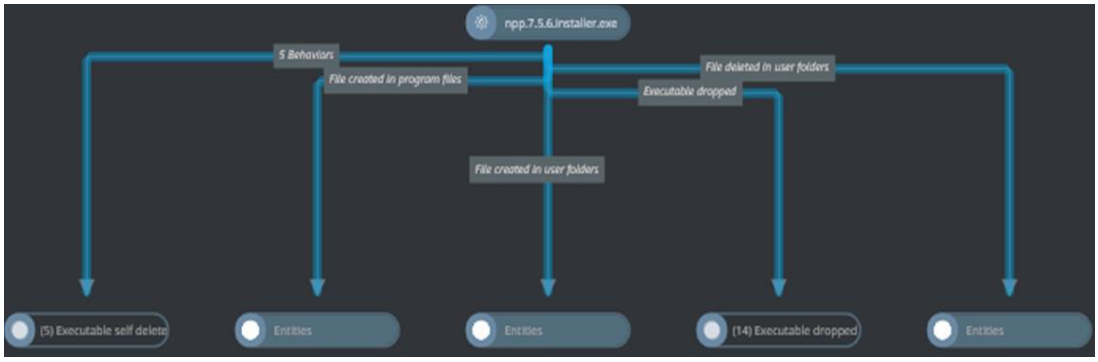
Wireshark
Our Operation Center found that on agent BPVBLBE1, installed on your computer, user gmadm00 on the 29th of march,2018 at 12:14 PM performed Wireshark uninstallation from file in "D:\Program Files\Wireshark\uninstall.exe". As part of Wireshark uninstallation process also WinPcap was uninstalled from file in "C:\Program Files (x86)\WinPcap\uninstall.exe". GLESEC considers this event as high priority since installs/uninstalls/upgrades on production servers can cause high impact if it was not intended to happen. If this is part of regular procedures or you were aware of this, please let us know.

Note: WinPcap is very common traffic capturing tool regularly installed/uninstalled along with Wireshark.

Wireshark, TreeSizeFree
Our Operation Center found that agent BPVBLBE1, installed on your computer, at approximately 12:20 of the 29th of march 2018, user gmadm00 performed installation/uninstallation on this server of the following applications: Wireshark, TreeSizeFree, npp++ and 7-Zip. GLESEC considers this event as high priority since installs/uninstalls/upgrades on production servers can cause high impact if it was not intended to happen. If this is part of regular procedures or you were aware of this, please let us know.
TreeSizeFree uninstallation from file in "c:\program files\jam software\TreeSize Free\unins000.exe" with MD5 2d3665b200d4b8983e0114bedab1d4a7



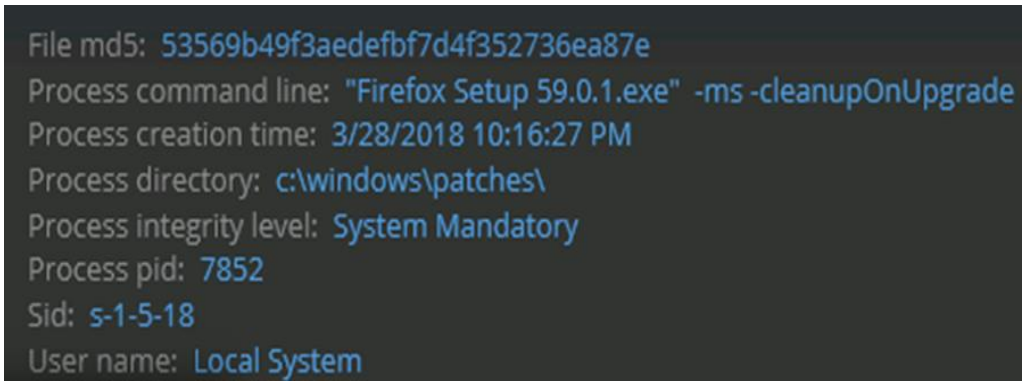
npp++ uninstallation from file in "d:\Program Files (x86)\Notepad++\uninstall.exe with MD5ed65b3ea722d605b1016bea3d06db491



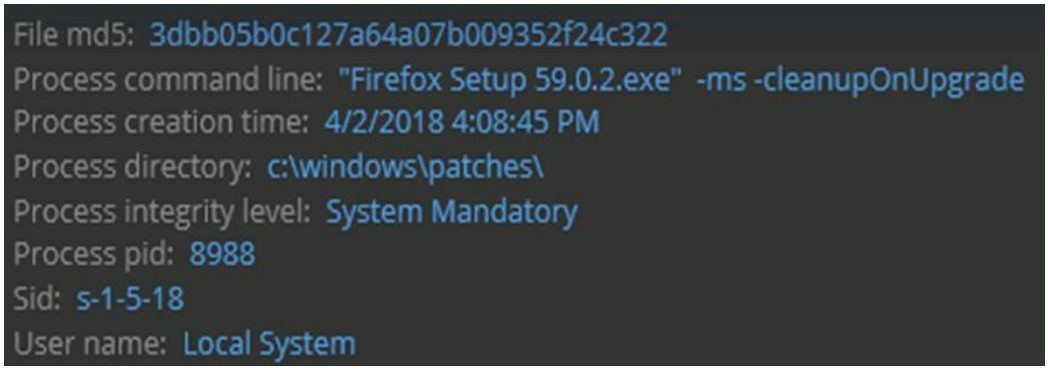
Mozilla Firefox

It was found that on agent bpvblbbe1, installed on your computer, there was an automatic upgrade by Local System user for Mozilla Firefox web browser on two different dates as follows:

•28/03/2018 at 10:16 pm: Upgrade to Firefox v 59.0.1 from file in "c:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice_tmp.exe"→ "c:\windows\patches\Firefox Setup 59.0.1.exe"



•02/04/2018 at 4:10 pm: Upgrade to Firefox v 59.0.2 from file in ":\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice_tmp.exe" → "c:\windows\patches\Firefox Setup 59.0.2.exe"

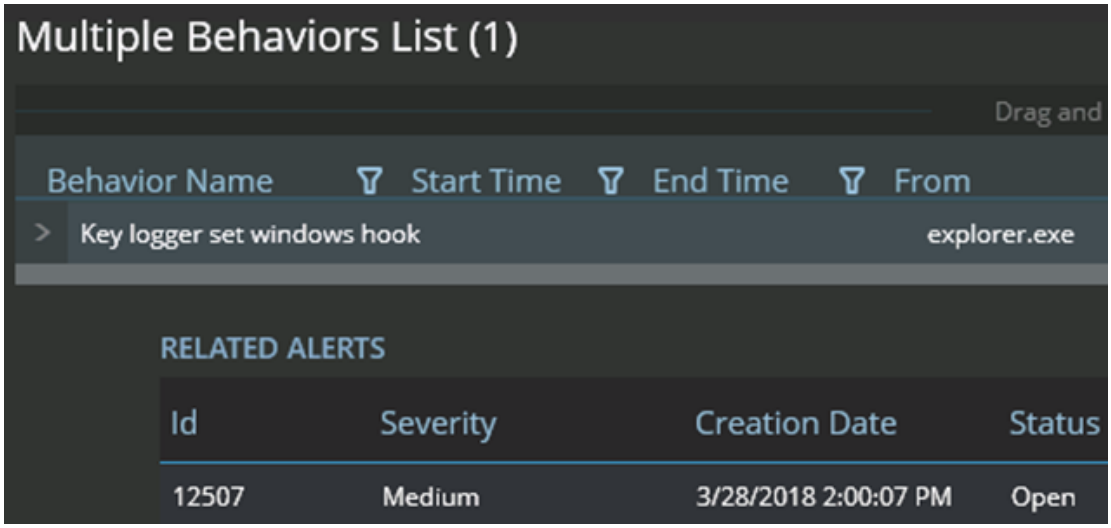


If this is part of regular procedures or you were aware of this, please let us know.

Top Events Registered By Medium Severity Level

key logger

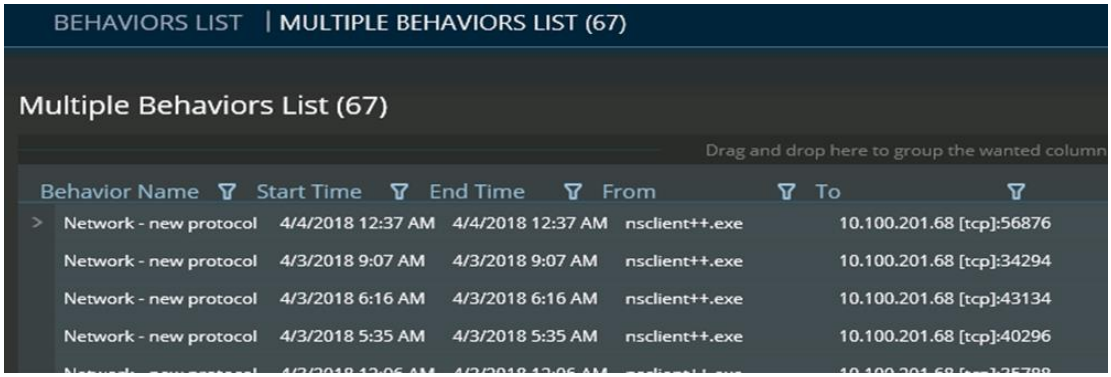
Our Operation Center found that agent BPVBLBE1, installed on your computer, at 09:59 PM of the 26th of march 2018, using user gmadm00, key logger set a Windows hook from "exploerer.exe". After follow up investigation on this event we found that it was part of a regular windows process.



nsclient++.exe

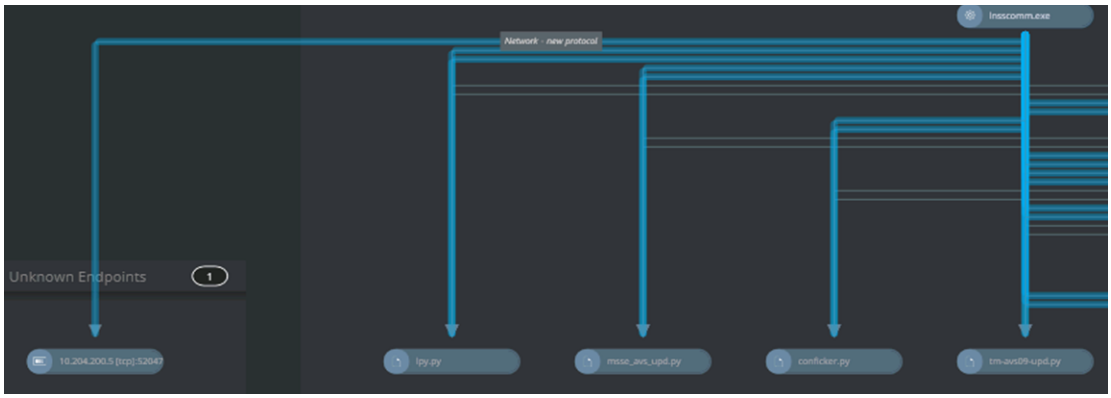
It was found that on agent BPVBLBE2, installed on your computer, from 31/03/2018 until Current time, a new connection is established to local address 10.100.201.68, this occurs many times a day. This connection is not initiated by a regular user but by "nsclient++.exe". This behavior is suspicious unless this is a monitoring agent configured to send data to previous mentioned address which should be the official

collector of that information. If this is the regular monitoring agent for this server or you were aware of this, please let us know.

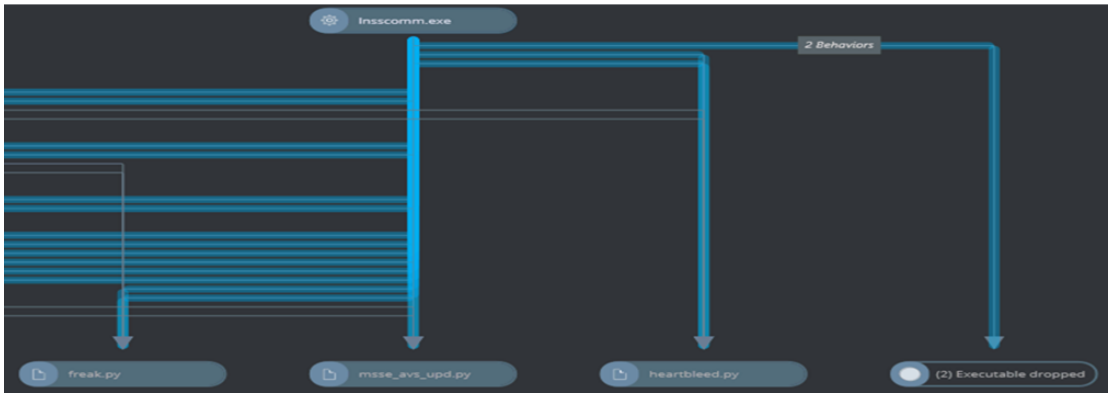


LanGuard 12 Agent

Our Operations Center was able to recognize that on computer BPVBLBE2, on 29/03/2018, from Local System user, a connection to host 10.204.200.5:52047 from 10.204.200.5:61301 was initiated from process command line "C:\Program Files(x86)\LanGuard 12 Agent\lnsscomm.exe" also, many python files were executed as a result of this action as can be seen below. If this agent is installed officially and under network administrator's awareness, please let us know.



On 02/04/2018 Same event was repeated with the only difference that this time it did not start a connection to other entity, only executed many python files.



We noticed that 2 of the files executed by lnsscomm.exe are named "heartbleed.py" and "freak.py" as shown above. We strongly recommend to inspect the content of these files for better awareness.

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

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.

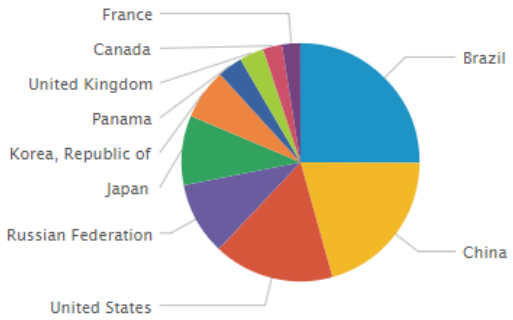
The purpose of this section is to highlight intelligence gathered from this and other services under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat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

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

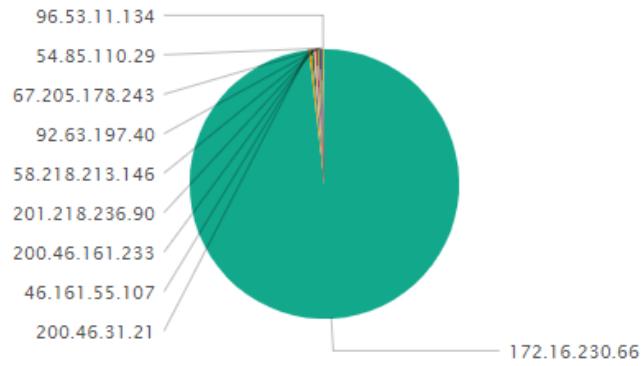
Graph: Denial Connections
This graphic shows the denied connections in the firewall rules

841,844

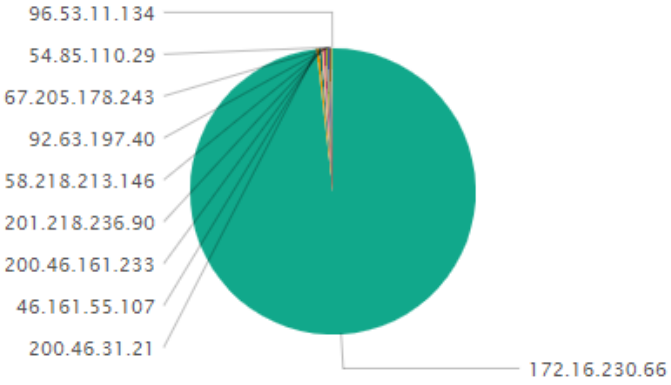
Graph: Top Country Blocked
This graphic shows top attacking countries blocked.



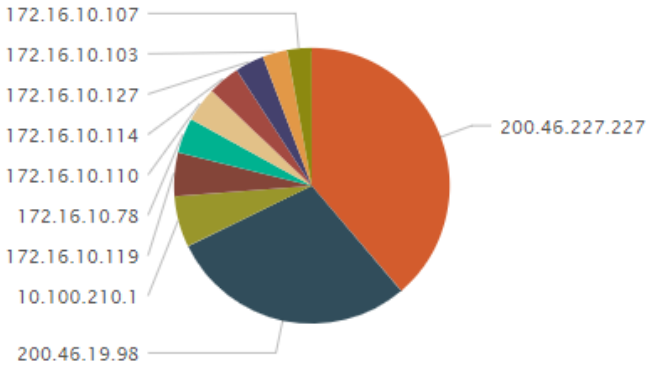
Graph: Top Attacks Blocked by Country
This graphic shows the top attacker's IP blocked



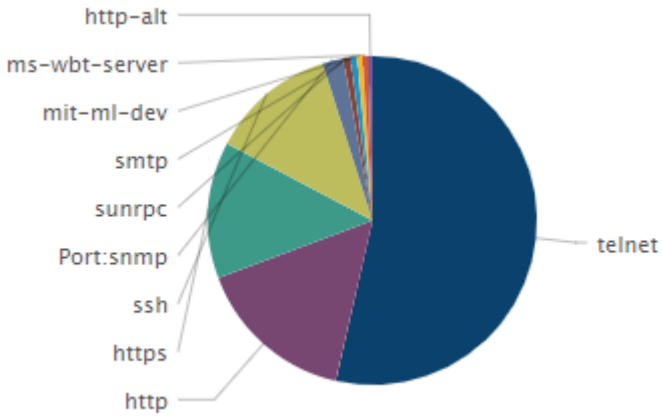
Graph: Top Sources
This graphic shows top attack sources blocked



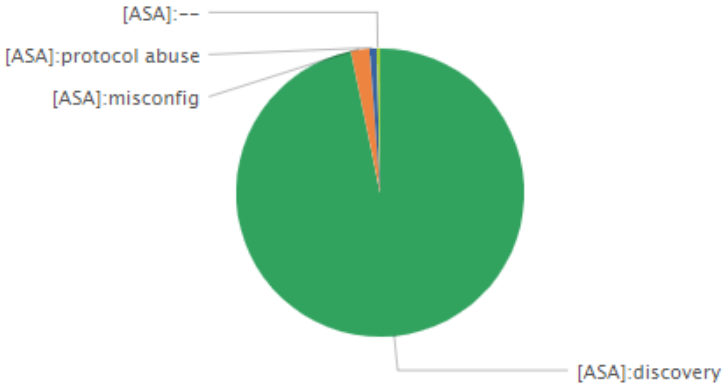
Graph: Top Destinations
This graphic shows the top attack destinations denied



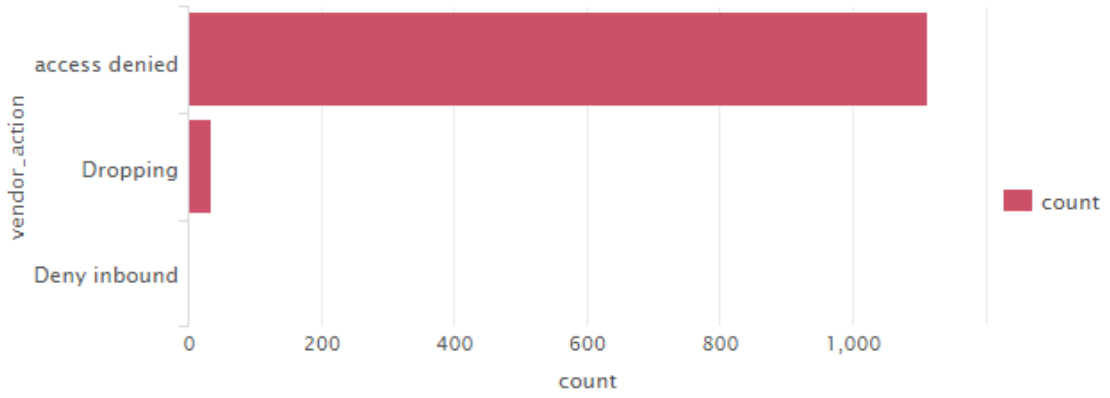
Graph: Top Services
This graph provides the top services blocked by in and out firewall rules.



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	40962562	97.932826
IKE and IPsec	40962562	97.932826
User Session	843369	2.016317
Access Lists	800590	1.914041
IP Stack	20341	0.048631
NAT and PAT	2456	0.005872
SNMP	931	0.002226

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.

TICKET ACTIVITY

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

All the services operated normally during the month of March.
Our GOC has reported an incidence in the month of April related to the DMZ of BANVIVIENDA.

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 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.

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

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

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

Info@glesec.com
www.glesec.com