OPERATIONS & INTELLIGENCE EXECUTIVE CYBER SECURITY REPORT

Institute of Electrical and Electronics Engineers

December 2018.

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com

Table of Contents

GLESEC
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 the 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, skilled 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 TIP™ 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.

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

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	12/12/19
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS - email	YES	12/12/19
Risk assessment	MSS-BAS - web	YES	12/12/19
Risk assessment	MSS-BAS - WAF	YES	12/12/19
Threat Mitigation	MSS-EDR		
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS		

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

Executive Summary

This report corresponds to the period of December 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: 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.

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

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 the defenses of the organization to the latest threats are. 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 determined that the risk condition for the IEEE for the month of December is of concern. This can be seen from the various security indicators as indicated below.

Risk Indicator	Service	Condition	Comments
Risk Value Metric	MSS-VME	HIGH	1 critical vulnerability and 8 high risk vulnerabilities were found. Any one of these can cause an impact to the IEEE.
Risk Score	MSS-BAS email	HIGH	The risk score for the email vector, during this period, is considered high. This due to the fact that out of 587 simulated malware emails sent, 97 of them successfully penetrated the security countermeasures put in place in your organization.
Risk Score	MSS-BAS WAF	CRITICAL	The WAF is not configured to protect the IEEE at this point, which leaves the organization exposed. The score for this month is 87%.

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

Risk Score	MSS-BAS EDR vector	CRITICAL	We consider this serious for this vector. The score is 45% which when it reaches 35% becomes critical. Based on our testing Ransomware and other Malware is not being stopped by the current anti-malware of the organization.
Risk Score	MSS-BAS browser	MEDIUM	While the condition is "medium" this does not mean that it is protected enough. The score is 19% which when it reaches 35% becomes critical. It only takes one malicious application like Ransomware to compromise the organization, particularly vulnerable to Wannacry and Petya Ransomware.

Risk conditions based on the contracted services MSS-VME

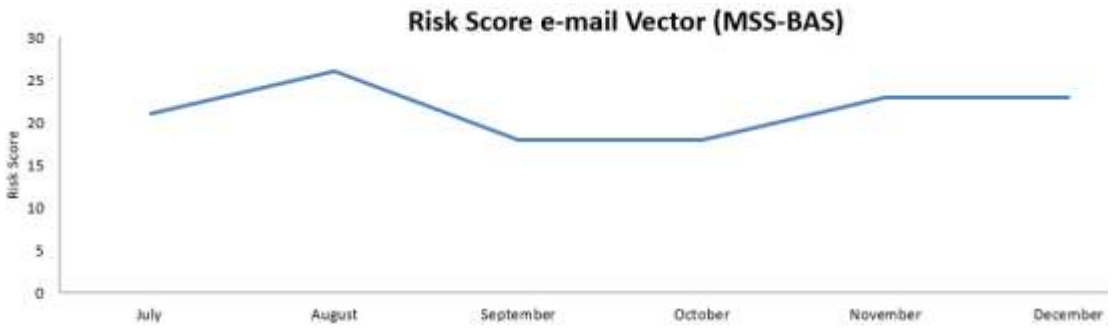
During this month, 215 hosts were inspected, several hosts less than last month. Additionally, the number of vulnerable hosts in the last scan is 7, 4 less than last month. The most common vulnerabilities discovered for this month are related to SSL Certificate problems, vulnerabilities in SSH protocol and Outdated versions of Oracle GlassFish Server.

The critical vulnerability present comes from Oracle GlassFish Server 3.1.2.x < 3.1.2.15. The high-risk vulnerabilities present, refer to the use of SSL v2 or v3; this

protocol has been deprecated and TLS is recommended instead, also some high-risk vulnerabilities are from Oracle Glass Fish Server.

In conclusion, for this period, the Risk Value with little change from last month, due to many of the vulnerabilities reported last month still present in the hosts.

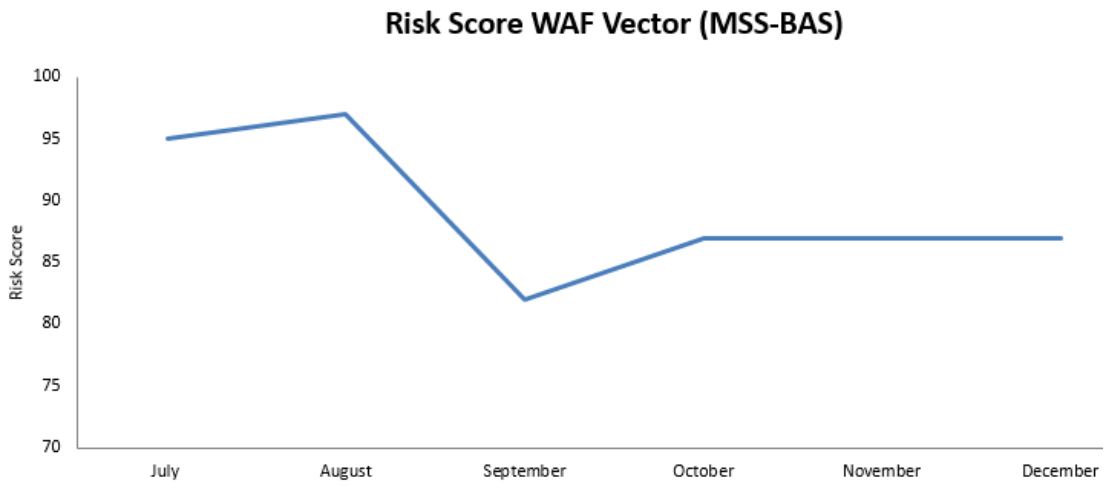
Risk conditions based on the contracted services MSS-BAS e-mail vector is **HIGH** 23%



The risk score for the email vector, during this period, is considered high. This due to the fact that out of 587 simulated malware emails sent, 97 of them successfully penetrated the security countermeasures put in place in your organization. Considering that only 1 malware/Ransomware can cause high impact to the organization 97 of them is an important amount.

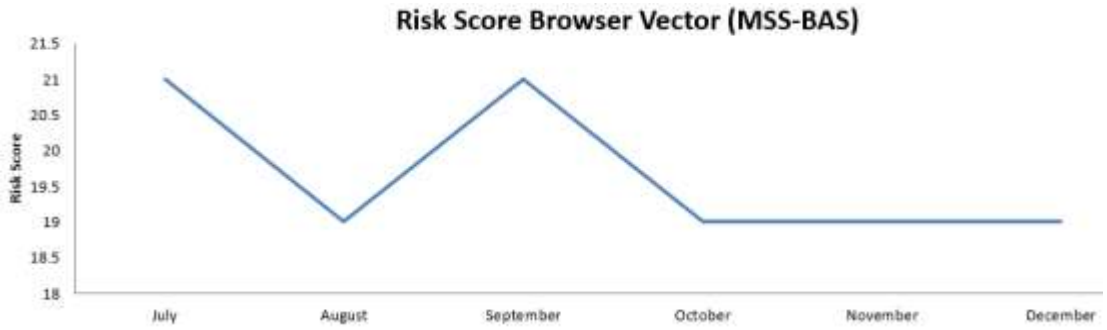
Risk conditions based on the contracted services MSS-BAS WAF vector is **CRITICAL** 87%

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



The risk score for the WAF vector, during this period, is considered critical. This since out of 1,966 simulated malware sent 1,903 of them successfully penetrated the security countermeasures put in place in your organization, which is around the 97% of them. Considering that only 1 type of SQL injection can possible cause a high impact the company they should all be stopped.

Risk conditions based on the contracted service MSS-BAS Browser vector is **MEDIUM** 19%



For this month, the risk score remains at 19%, which is the same value as last months, but there is room to improve.

The single MSS-BAS EDR test vector showed 45% penetration. This was specifically of Ransomware and other malware that does not have signatures. The anti-virus operated very well for viruses and malware with signatures but did not work at all to

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

protect against other attacks.

VULNERABILITIES

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.

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). Progress can be determined by weekly testing.

In general, the vulnerabilities present in the Institute of Electrical and Electronics Engineers computer systems can be divided in the following categories:

- Critical (1),
- High (8),
- Medium (11),
- Low (5).

It was discovered that 7 of the 215 hosts analyzed have at least one problem of vulnerability, the 10 most frequent vulnerabilities found this month by name are:

- SSL Medium Strength Cipher Suites Supported
- SSL Version 2 and 3 Protocol Detection
- SSH Server CBC Mode Ciphers Enabled
- F5 BIG-IP Cookie Remote Information Disclosure

- HTTP TRACE/TRACK Methods Allowed
- SSH Weak MAC Algorithms Enabled
- SSH Weak Algorithms Supported
- Oracle GlassFish Server Embedded Server Vulnerabilities (January 2016)
- Oracle GlassFish Server Unspecified Information Disclosure (October 2015 CPU)
- Oracle GlassFish Server Multiple Vulnerabilities (October 2013 CPU)

The port considered most vulnerable for this period were 443 (HTTPS) followed by port 21 (FTP) and 80 (HTTP), this is due to many of the vulnerabilities found are related to them.

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 these 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 table indicates the external vulnerability metric.

Total IP's Scanned	IP's Vulnerable
215	7

Risk Distribution				
Critical	High	Medium	Low	Total
1	8	11	5	25

According to the metrics:

RV= 0.016930233

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:

Vulnerable Hosts	Critical	High	Medium	Low	Total
140.98.193.170	0	0	0	1	1
140.98.193.235	0	0	1	0	1
140.98.194.3	0	0	1	0	1
140.98.194.12	0	1	1	0	2
140.98.194.15	0	1	1	0	2
140.98.194.119	0	0	1	0	1
140.98.196.36	1	7	5	1	14
140.98.196.190	1	7	5	1	14
140.98.200.22	0	0	1	1	2
140.98.200.215	0	0	1	2	3
140.98.202.205	0	0	1	0	1

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 external vulnerabilities by category.

Category	Critical	High	Medium	Low	Total
Web Servers	2	14	12	3	31
General	0	0	5	0	5
Misc.	0	0	1	3	4
Service detection	0	2	0	0	2

THREATS

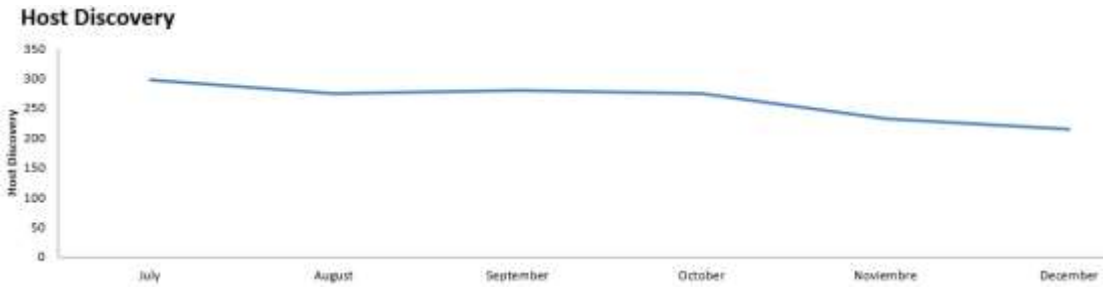
GLESEC uses its MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR and MSS-UTM to determine threat intelligence activity.

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

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 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. The MSS-VM(E/I), MSS-EPS conduct weekly testing.



During this period, 215 hosts were discovered. 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 found these results as normal.

We have requested to update our list of CRITICAL ASSETS so that we can correlate this information with our DISCOVERY, VULNERABILITY TESTING and THREATS.

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 **"e-mail Security Exposure Level"** for your company this month was classified as

"HIGH" based on the "Risk Score" of 23%.

In the **email simulation** 55 of the different file types, holding a malicious-payload within, were able to penetrate your security measures (See "Files detected as ALLOWED"). The number of filetypes that are allowed have been increasing with each scan. A review of the allowed file types should be done to determine which filetypes could be blocked or dropped, leaving only authorized files type to be sent or received by email.

Riskiest file types that were able to penetrate for each severity level

Low

File:DummydownloaderDocxHtmlXhtml.xhtml

The .docx file is a Word document that downloads its template online from an external HTTP/S server. The template is a Macro Enabled Word Template that will execute a MessageBox to show code execution This consists in a payload hidden within a docx file linked to a HTML file which was linked from a XHTML file.

Medium

File: MscomctlbofDocPdf.pdf

This one consists on a hidden payload within a PDF document which links to a doc file.

High

File:cryptomacroAccdb.accdb

The .macro enabled accdb file is a Crypto Ransomware that encrypts all the files in the current logged on user. This is a type of ransomware which is can affect your system from a direct execution.

Web Gateway Attack Summary

For this month's test, the risk score of your organization is considered medium risk. The risk score for this month is 19%. But it is important to take into account the amount of high risk simulated attacks that were successful.

Risk score:

19 /100

Riskiest file types that was able to penetrate for each severity level

Low

File: DummycommandLnk.lnk

The ".lnk" file is a Command Line execution file. This consists in .lnk file carrying a payload which could affect your systems.

Medium

File: payloadBat.bat

The Payload of this file is a set command files that could or not be allowed to execute on your systems, but it was able to penetrate.

High

File:wormComDocx.docx

This is a type of ransomware that can affect your system from a direct execution.

WAF Attack Summary

For this month's simulations, the risk score of your organization is considered critical risk. This situation is of concern and should be addressed as soon as possible; additionally, the fact that the successful simulations percentage was very high, and with the information we have, could point that the countermeasure in place is not stopping many of the common attacks that target web applications.

The risk score for this month is 87 %, which is considered a CRITICAL-risk level.

87/100

Endpoint

The **"Endpoint Security Exposure Level"** for your company was classified as "HIGH" based on the "Risk Score" of 45%.

Risk Score:

45/100

Penetration Ratio

11%

Percentage of samples that were able to bypass security measures in place.

GLESEC

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR

Tel: +1 (609)-651-4246 / +(507)-836-5355

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 user 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

Despite the growing investment in cyber security, sophisticated attackers still manage to bypass even the most advanced security systems, including next-generation, non-signature based security. The reason is that advanced threats are coded to look like legitimate behavior. Therefore, they are extremely difficult to identify using conventional systems and can proceed unimpeded within the target networks.

1. Additional details about these vulnerabilities are presented in the Technical report of Institute of Electrical and Electronics Engineers in severity section of the Managed Vulnerability Service (MSS-VM). GLESEC can help in the remediation of the identified vulnerabilities.

2. The service MSS-BAS used a group of sample files to simulate the attacks, most of this samples were contained in one or several file types, the following table illustrates which embedded file types were able to successfully infiltrate your network:

.ics	.html	.docx	.pdf	.xhtml	.msg	.vcs	.zip	.xsl	.xlsx	.eml	.wav	.oft	.htm
.doc	.potm	.pptm	.xls	.xlk	.xlsb	.pptx	.svg	.xltm	.ppt	.pot	.wbk	.slk	.xla
.docm	.dotm	.xlsm	.pps	.xll	.xlw	.xml	.ppa	.dot	.rtf	.ppam	.sldx	.mdb	.pwz
.sldm	.ppsm	.accdb	.7z	.gz	.arj	.rar	.lha	.mcl	.pub	.tar	.one	.google	

To detect malicious file that could be hidden within another file type solutions such as Sandbox or even better a **Content-Disarm & Reconstruct solution (CDR)** can be implemented (if need more information please let us know), this kind of solution is very effective in today's environment. A Sandbox solution is more limited than CDR and contains the suspicious file in an isolated environment and attempt to execute it in several ways behaving like an end-user, if the payload is triggered, the sandbox can use Content disarm, removing the malicious code embedded in the file and leaving the original file cleansed.

3. During this month, most of vulnerabilities come from SSL vulnerabilities and outdated versions of OracleGlassFish Server. In case the servers with the

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

outdated software are used for tests and research or there is no possibility of upgrading the software, it would be advisable to limit the connections from the outside to those servers, only to the authorized parties and filter the rest of the connections. For SSL most of the vulnerabilities refer to the use cipher suites and protocols that are no longer considered secure by modern standards; TLS 1.2 with strong cipher suites is the minimum recommended protocol to use in SSL connections.

4. The results for the MSS-BAS vectors tested, shows that the WAF that is currently in place is no dropping or stopping many of the threats that are used in the simulations. Proper configuration of the WAF is necessary to ensure the web applications are not affected with SQL injection, XSS or other techniques.
5. Due to the fact that a penetration could have already compromised the internal systems it is recommended to conduct a forensic evaluation of your local network and/or critical systems.
6. It is also important to take a pro-active approach to avoid infection by deployment of technology or contracting a service that can identify an attack without signatures and mitigate this before it causes harm to the organization. We recommend considering a true EDR solution and to this effect recommend that we activate for testing on the perimeter our MSS-EDRe (External Managed End Point Detection and Response) as a proof of value (POV).

For any question about any of the recommendations above or to request assistance please contact our GOC.

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

Intelligence Section

Managed Breach Attack Simulation Service (MSS-BAS) Intelligence Section

The Managed Breach Attack Simulation Service (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 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.

Successful high level simulated attacks

We found 51 threats that have a higher level of impact as a High risk, which are Malware, Worm and Ransomware and Exploits in the email vector.

This malicious code can be hidden within several different file types, the usual security countermeasures do not recognize it or stop it once it has been executed.

The successful penetrations are broken down in the following categories:

- Malware: 15 files that await remote commands from a command and control server or try to obtain elevated privileges by disrupting the user activities with pop-ups.
- Ransomware: 20 files were able to penetrate the perimeter at this level. These are considered as high risk due to the low number of clicks required to execute them and the fact they are using common extensions to disguise

themselves, so users are more prone to execute them by mistake.

- Worms: 10 files disguised as Office Macros that attempt to spread through the network to infect other computers.
- Exploits: 8 files or scripts that are designed to exploit vulnerabilities present in software, sometimes outdated versions such as Office 2010, Firefox v50.0 and older.
- Dummy: 2 files, dummy files are proof of concept of attacks, they are not real malware.

Successful Medium level simulated attacks

Email vector: 167 files within this severity indicator were able to penetrate the perimeter, these are the highlighted categories:

- Ransomware: These files were able to penetrate the perimeter at this level as well, what this means is that using different combinations for containing this malicious code were successful in entering the network. These types are considered medium risk because they require more clicks to be executed, as contained in more different types of files. The ones that were able to access your network were:
  - ICS-VCS-XLK
  - XHTML-ICS-MDB
  - LHA-PDF-ACCDB
  - ARJ-PDF-ACCDB
  - RAR-PDF-ACCDB
  - ZIP-ICS-XLL
  - GZ-PDF-ACCDB
  - VCS-ICS-XLM
  - LZH-PDF-ACCDB

- MSG-VCS-XLT
- CAB-PDF-ACCDB
- TAR-PDF-ACCDB
- 7z-EML-PDF-ACCDB

This ransomware has the same impact to your Organization if executed as a "High risk" ransomware, but it is little less accessible for the end user.

- Exploit: The files that could enter the network target different vulnerabilities. The most common targets are undocumented feature in Microsoft Word that allows malicious attackers to collect information about the OS and software versions remotely and a vulnerability in CSV files that allow remote code execution with specially crafted formulas.
- Worms: files under this category, are run automatically by the Office Macro scans ports and infects other computers in the network.
- Links: files under this category are payloads that redirect to webpages that host malware attempting to download it to the victim's computer.
- Payloads: files under this category, periodically take screenshots of the user's desktop and attempts to read input from the user.

The other types of attacks sent by this simulation were blocked by your Organization security countermeasures.

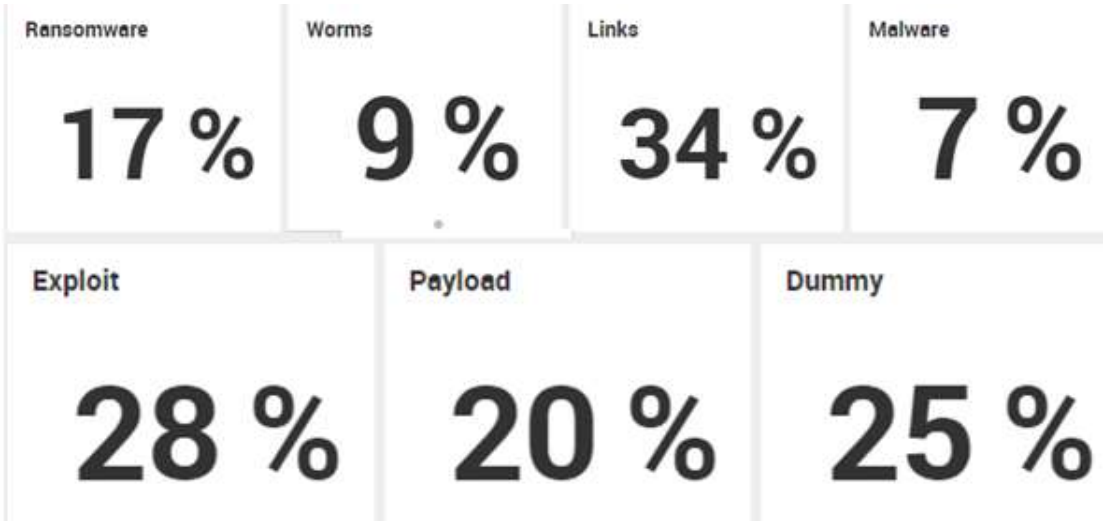
Successful Low level simulated attacks

376 out of 2468 low risk malicious codes were able to access your network. These types of files are considered of low risk because (a) they require many clicks to execute or (b) even if they were executed they don't cause a high impact. By securing the network against higher severity criteria mentioned before in this report, it is likely that the amount of low risk malware that penetrated is also reduced.

Graph: Risk Score Vector E-mail

Graph: Simulation Summary Vector E-mail

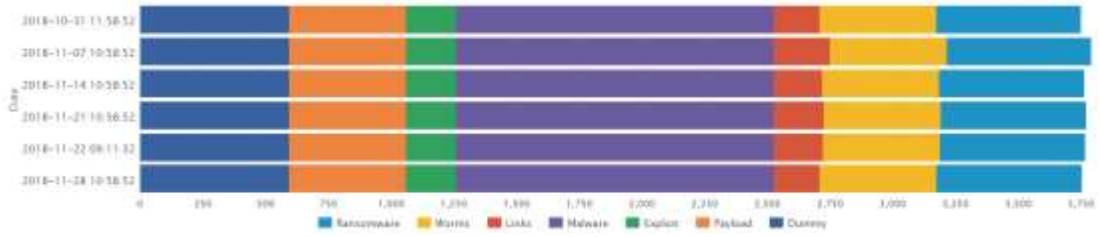
Graph: Attack Type Summary Vector E-mail



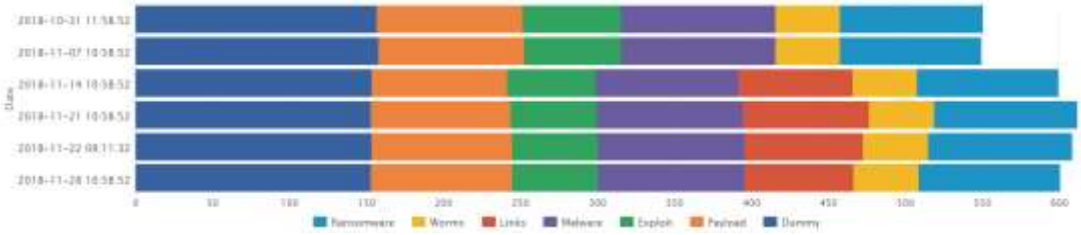
Graph: e-mails Sent

This graph shows a comparison of the malware and Ransomware sent and accepted

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



Graph: e-mails Penetrated



Graph: Risk Score Vector Web Gateway

19 %

Graph: Simulation Summary Vector Web Gateway

Arrived : 3213 / Sent : 3213

GLESEC

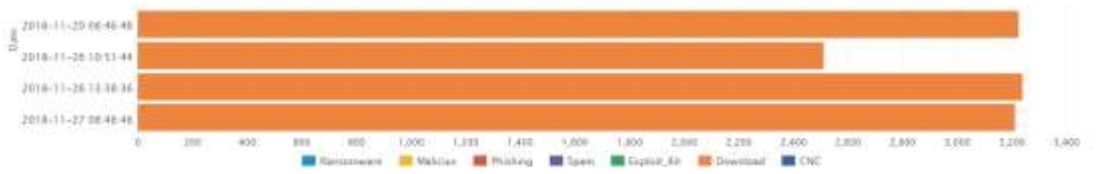
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Graph: Attack Type Summary Vector Web Gateway

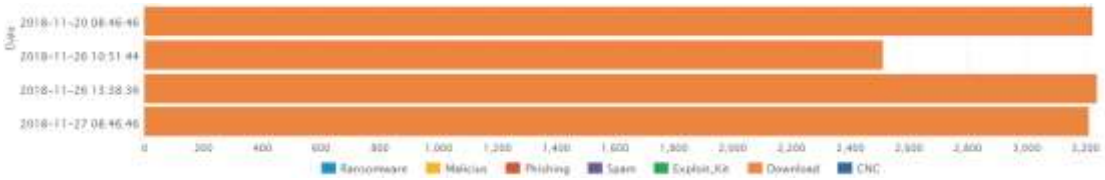
Ransomware	Malicious	Phishing	Spam	Exploit-kit	Download	CNC
0 %	0 %	0 %	0 %	0 %	100 %	0 %
0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	3213 / 3213	0 / 0

Graph: Web Gateway Sent

This graph shows a comparison of the malware and Ransomware sent and accepted



Graph: Web Gateway Penetrated



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/.

<u>Vulnerability Score</u>

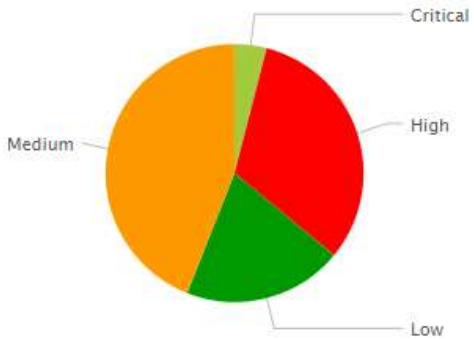
The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed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

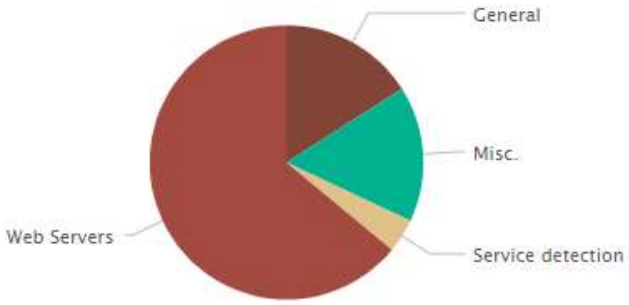
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

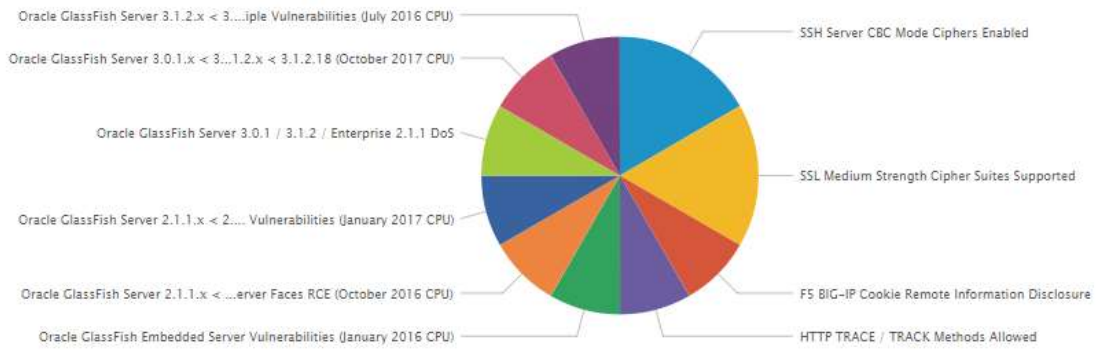
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



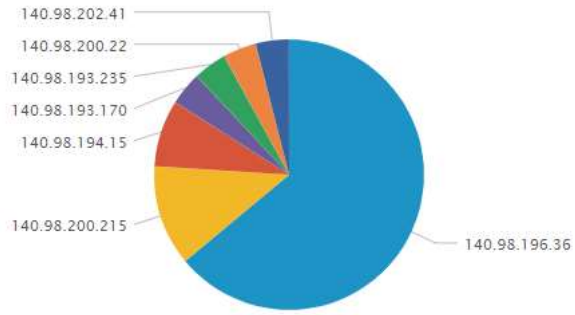
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



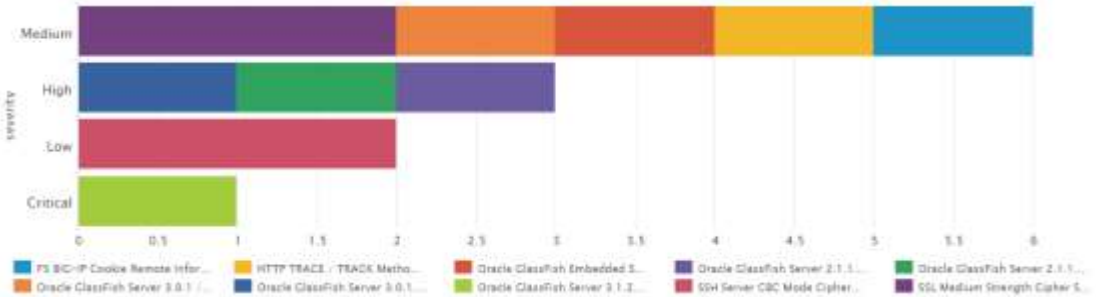
Graph: Most Frequent Vulnerability Name
This report depicts the most frequent vulnerabilities discovered this report period



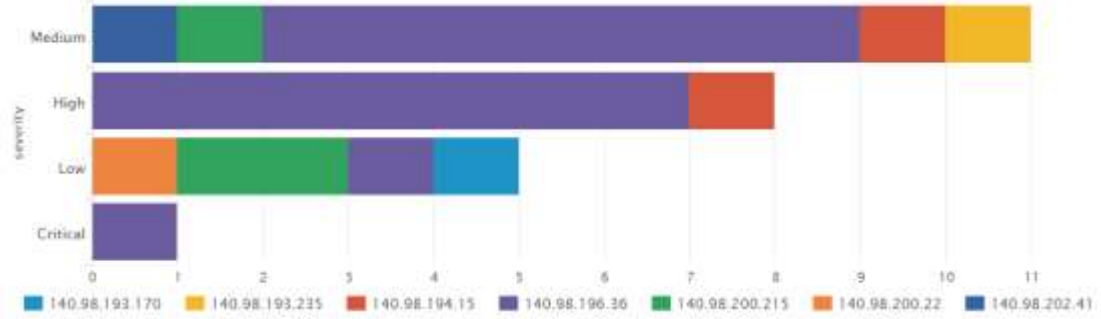
Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period



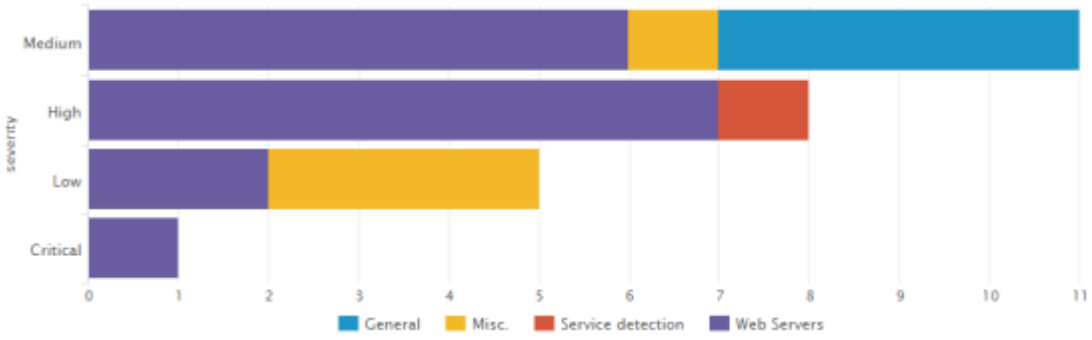
Graph: Vulnerability Risk by Vulnerability Name
This report illustrates the vulnerability risk and count by vulnerability name discovered this report period.



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



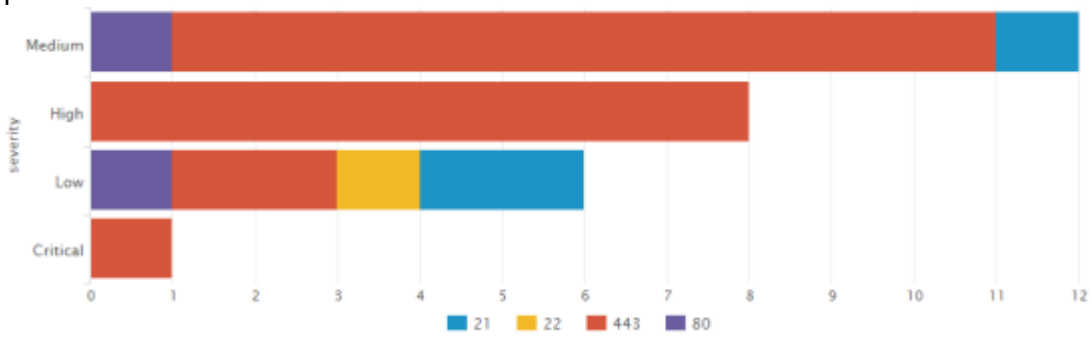
Graph: Vulnerability Risk by Category
This report illustrates the vulnerability risk and count by category discovered this report period



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

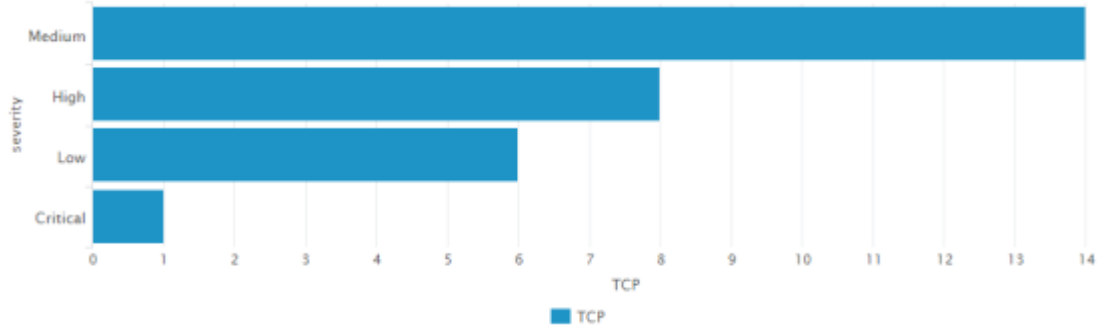
Graph: Vulnerability Risk by Port

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



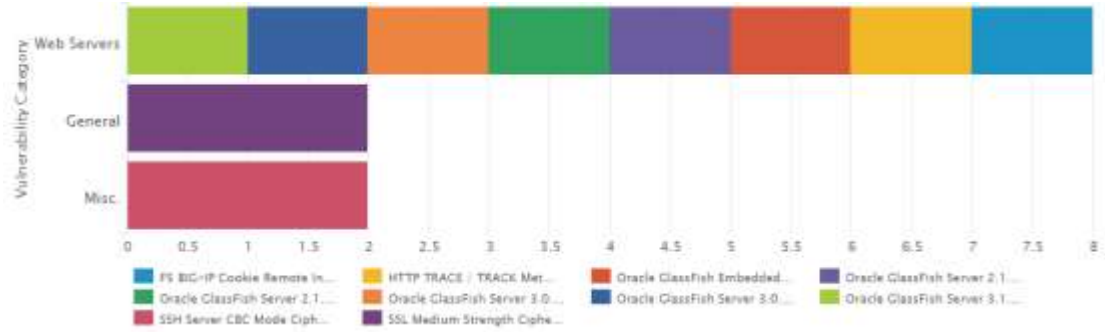
Graph: Vulnerability Risk by Protocol

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



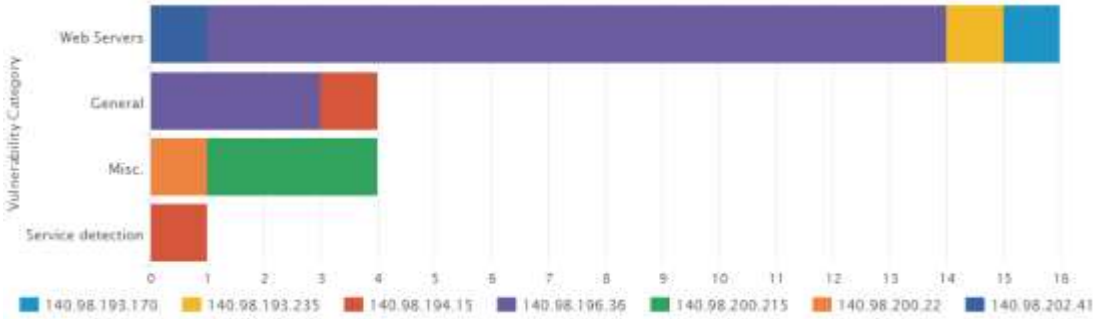
Graph: Vulnerability Category by Vulnerability Name

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



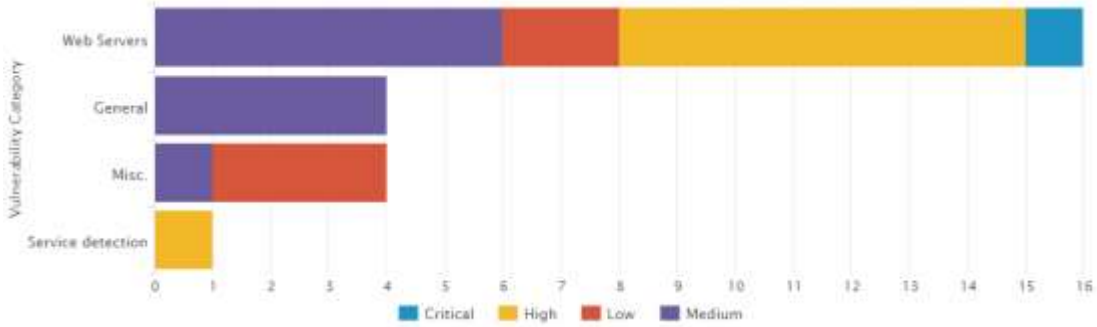
Graph: Vulnerability Category by Host

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



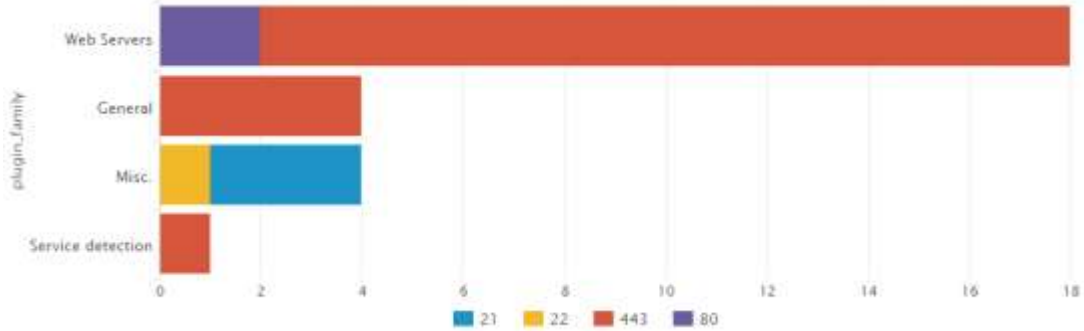
Graph: Vulnerability Category by Risk

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



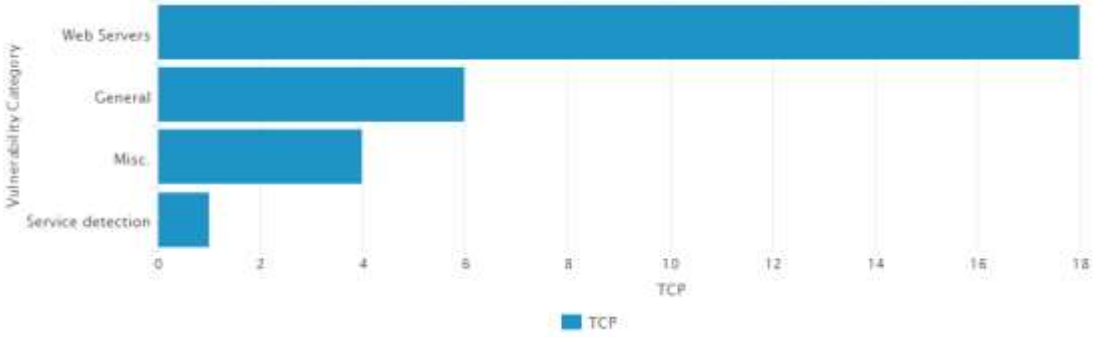
Graph: Vulnerability Category by Port

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



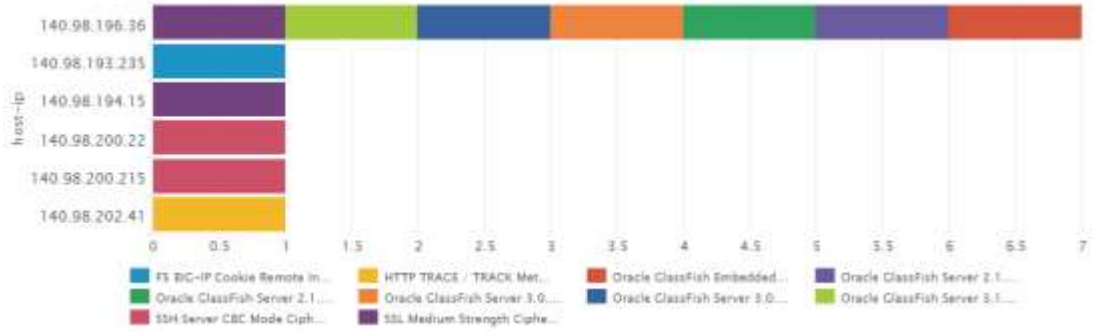
Graph: Vulnerability Category by Protocol

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



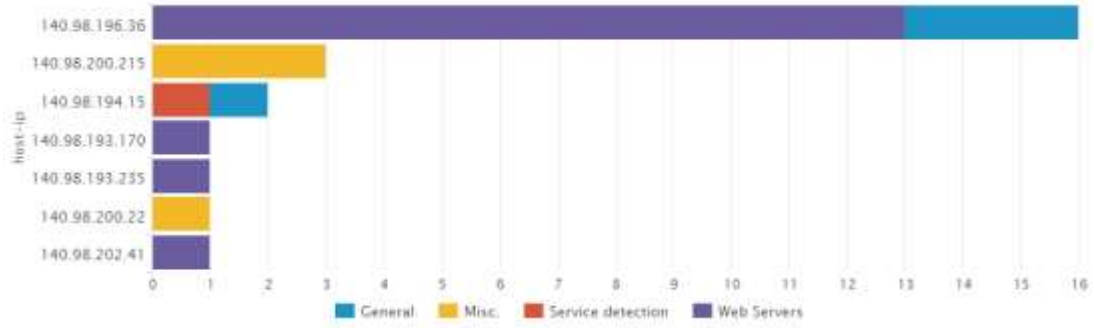
Graph: Host by Vulnerability Name

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



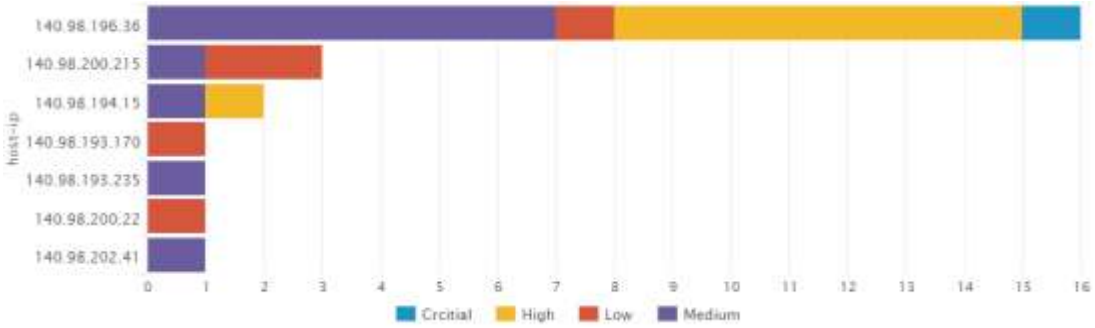
Graph: Host by Vulnerability Category

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



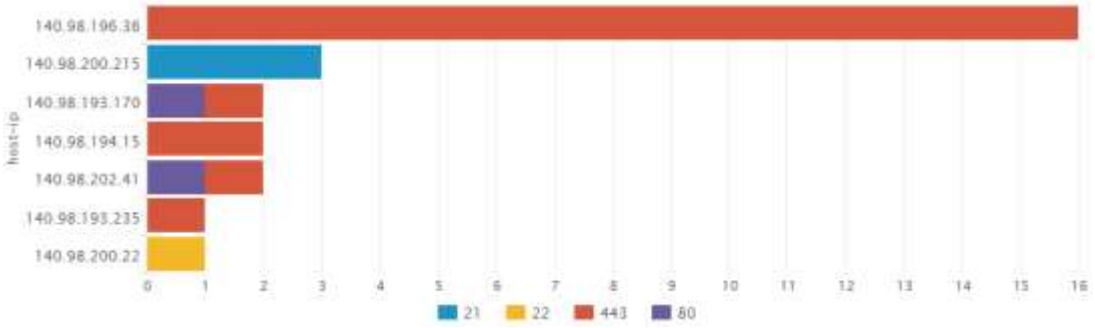
Graph: Host by Vulnerability Risk

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



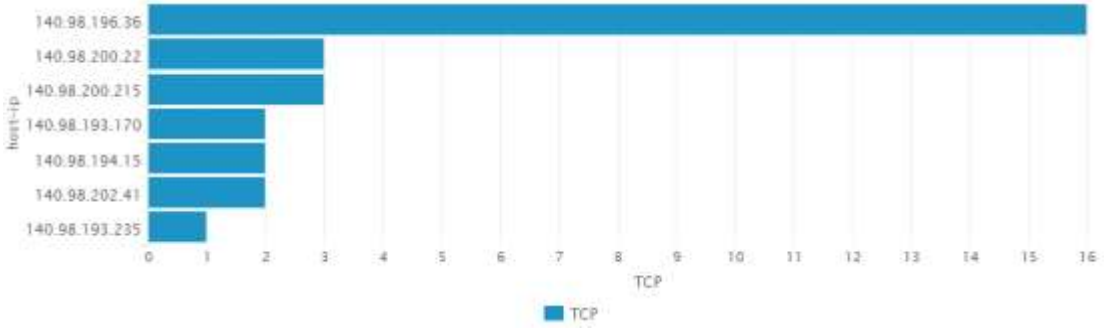
Graph: Host by Port

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



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	2	0	0

TICKET ACTIVITY

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

Number	Ticket#	Title
1	2018121410000113	Follow up for Critical and high serverity vulnerabilities
2	2018121310000044	Monthly Report of Operations & Intelligence, November 2018
3	2018120310000018	INFORMATION GATHERING CRITICAL ASSETS DATABASE

The tickets for this month are presented in the summary above. The tickets show all the activity pertaining to the organization throughout the month. For this month the activity included delivery of the Monthly Reports of Operation and Intelligence, a ticket doing a follow up on the vulnerabilities found on the client and lastly a ticket was opened to gather information about the critical assets of the client.

Definitions

Links a malicious website is a site that attempts to install malware onto your device.

Payload the payload is the part of malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data. In addition to the payload, such malware also typically has overhead code aimed at simply spreading itself, or avoiding detection. Payload can be A small software that downloads the more advanced Payload from the remote C&C.

Worm malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth.

Ransomware is computer malware that installs covertly on a victim's computer, executes a crypto virology attack that adversely affects it, and demands a ransom payment to decrypt it or not publish it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, and display a message requesting payment to unlock it. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Malware is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. The fragment may be machine code that infects some existing application, utility, or system program, or even the code used to boot a computer system. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. Malwares are often referenced to Trojans, C&C, credential Theft Software.

Dummy The dummy files are Windows Message Box, code execution proof of concept. Malicious files are coded very often (thousands a day) and therefore relying on Signatures to block malicious files is outdated. Dummy files can prove the code execution is possible and share the same aspect of new unsigned malicious

files.

Exploit An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computers. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service

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.

USA-ARGENTINA-PANAMA

México-Perú-Brasil- Chile

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com