OPERATIONS & INTELLIGENCE CYBER SECURITY REPORT

Institute of Electrical and Electronics Engineers

March 2018.

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com

Table of Contents

About This Report 3
Scope of this Report 4
Executive Summary 5
Recommendations 20
Intelligence Section Per Service Module 23
Cyber Security Operations 35
Definitions 36

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	04/30/18
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS	YES	11/30/18
Threat Mitigation	MSS-EIR		
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

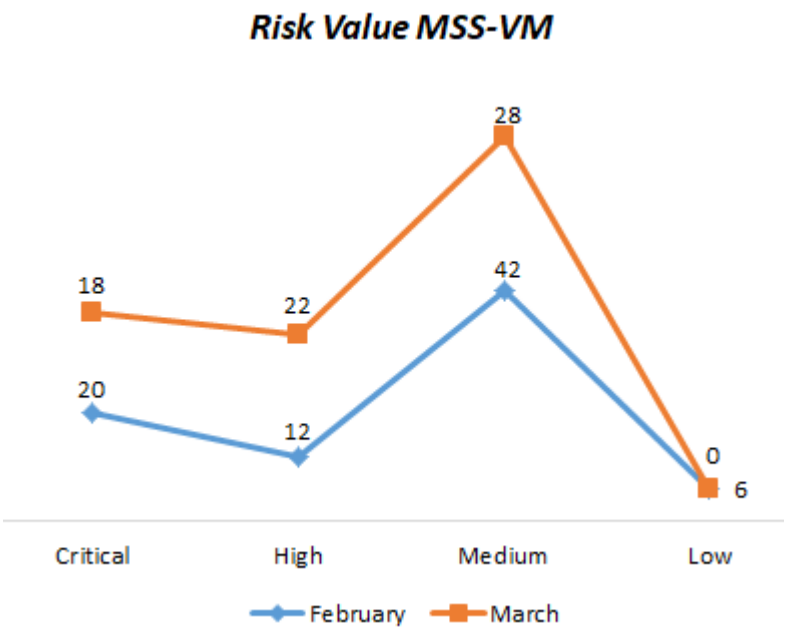
Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services 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.

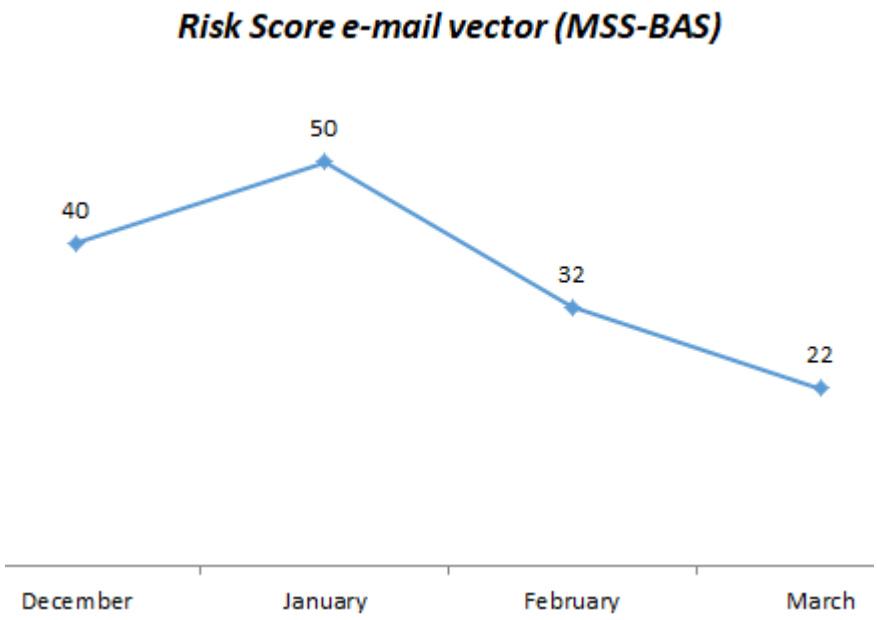
Risk conditions based on the contracted services MSS-VM



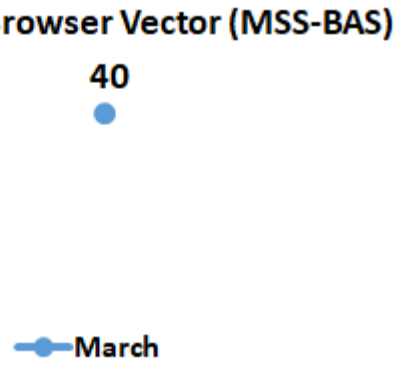
During this period we have noticed a decrease in the vulnerabilities discovered. This may be caused by a restriction in the access we have to test and is being investigated.

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

Risk conditions based on the contracted services MSS-BAS e-mail vector:



Risk conditions based on the contracted services MSS-BAS Browser vector



The Risk Score varies according to the latest simulated attacks and shows the security posture of your organization against this attack vector.

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

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.

Overall the vulnerabilities for Institute of Electrical and Electronics Engineers this period has been of 18 critical, 22 high and 28 medium risk and we found 14 critical vulnerabilities on host 208.99.166.235 related to PHP, as was reported last month.

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.

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

The following external network ranges for Institute of Electrical and Electronics Engineers were scanned for vulnerabilities.

The following table indicates the external vulnerability metric.

Total IP's Scanned	IP's Vulnerable
23	12

Risk Distribution				
Critical	High	Medium	Low	Total
18	22	28	0	68

According to the metrics:

RV= 0.372122762

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
208.99.166.235	18	22	7		47
208.99.166.243	0	0	5		5
208.99.166.228	0	0	2		2
208.99.166.229	0	0	2		2
208.99.166.233	0	0	2		2
208.99.166.234	0	0	2		2
208.99.166.236	0	0	2		2
208.99.166.240	0	0	2		2
208.99.166.247	0	0	2		2
208.99.166.251	0	0	2		2

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

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	11	0	17	1	29
CGI abuses	9	11	2	0	22
General	0	0	17	0	17
FTP	0	1	5	0	6
Misc.	0	0	1	5	6

THREATS

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

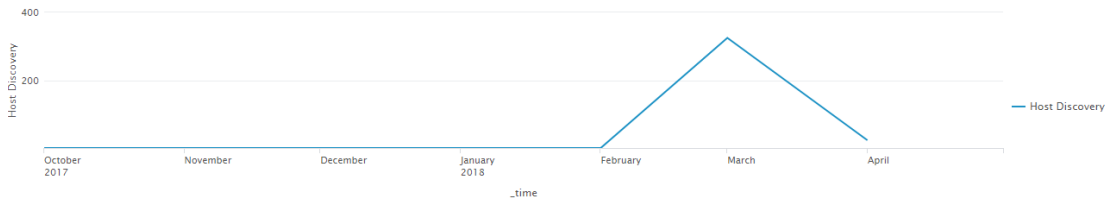
The services that provide us with information for this section have not been contracted.

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.

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



Knowing what's on your network is extremely important. During this period we have noticed a drastic drop in reachable assets. This is currently being investigated.

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 MSS-BAS e-mail Vector enables organizations to know different metrics that are used to measure and know your e-mail security position: an "e-mail Security Exposure Level", a "Risk Score" and types and severity of the malware that you are expose to, via the e-mail attack vector.

The e-mail Security Exposure Level can be "Low", "Medium" and "High" and it is

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

based in the "Risk Score" which is a percentage. The Risk Score is a Key Parameter Indicator, KPI, and it is used as an indicator of an increase/decrease from report to report, of how is the "overall" security in your organization. In this case related to the e-mail attack vector.

The Risk Score is calculated based on different parameters like the number of e-mails containing malicious software that are able to penetrate your security and other factors that are taken into consideration based on the type of malware and the "risk" for that malware. For instance for Ransomware, the Risk is calculated evaluating also parameters like number of "double clicks" needed to open the malicious file sent to the organization and the impact for your organization, of this type of malware if it is able to penetrate your security. The "Risk" for each malware is also classified as High Probability, Medium Probability and Low Probability depending in the type and probability of occurrence. For instance, Ransomware has a very high impact to the organization, but there is Low, Medium and High probability Ransomware, depending of the probability of occurrence.

The **"e-mail Security Exposure Level"** for your company this month was classified as "Low" based on the "Risk Score" of 22%. The "**web gateway (browser vector) Security Exposure Level"** for your company this month was classified as "High" based on the "Risk Score" of 40%.

In the **email simulation** 69% of the different file types, holding a malicious-payload within, were able to penetrate your security measures (see "Top 10 Penetrated File Types). This is something that should be of concern to the organization because this means that, as right now, you do not have a proper set of security measures in place that are blocking or dropping any e-mails, containing the type of malware that we used in this simulation.

In the **web gateway simulation** 99% of the different file types, holding a malicious payload within, were able to penetrate your security measures (see "Top 10 Penetrated File Types). This is a situation of high relevance to the organization because this means that, as right now, the current Security Web Gateway, has no measures or rules that detect and drop or filter the payloads and URL used in this simulation.

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

MSS-BAS e-mail vector Simulation Summary 688/4147

Risk Level	*Sent*	*Penetrated*
High	550	57
Medium	1222	230
Low	2375	401

MSS-BAS e-mail vector Risk Summary Matrix

E.g: Vulnerable to a Medium Probability Ransomware like WannaCry	**6%**	**8%**	E.g: Vulnerable to a High Probability Ramsoware like WannaCry
E.g: Vulnerable to a Low Probability Payload like Meterpreter Shell	**58%**	**28%**	E.g: Vulnerable to a High Probability Payload like Meterpreter Shell

Impact →

Probability →

MSS-BAS Browser vector Simulation Summary 3332/4970

Risk Level	*Sent*	*Penetrated*
High	1014	505
Medium	474	466
Low	3482	2361

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

MSS-BAS Browser vector Risk Summary Matrix

E.g: Vulnerable to Exploit and Ransomware like WannaCry	**10%**	**15%**	***Impact →***	E.g: Vulnerable to Malicious Websites High Probability Ramsoware like WannaCry
E.g: Vulnerable to Spam Websites And payload like Meterpreter Shell	**71%**	**4%**		E.g: Vulnerable to Phishing websites Payload like Meterpreter Shell

Probability →

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

Assessment Result for Email Simulation:

23%	**31%**	**28%**	**17%**
Dummy	**Exploit**	**Payload**	**Links**
Dummy category is code execution proof of concept without actual damage to the system.	Known and signed exploits of commonly used software that leads to code execution because of vulnerabilities discovered.	Common attacks delivered to clients like: Data extraction attacks or Stagers downloading the real malware.	A malicious website is a site that attempts to install malware onto your device.
11%	**17%**	**10%**	
Worm	**Ransomware**	**Malware**	
Software using Common techniques in order to spread itself inside a Windows based network.	Software encrypting user files and denies access until ransom is paid.	Malware, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.	

A very important detail that can be observed in the Assessment Result shown above is that the highest percentage penetration for the **email vector** this month comes from exploits at 31%. These exploits are present in outdated versions of Microsoft Office and present in Windows itself. This Medium risk factor indicates that your organization is very vulnerable via e-mail to these types of attacks. Exploits vector can be mitigated by keeping all the software up to date with the latest hotfixes.

Assessment Result for Browser Simulation:

17%	**5%**	**0%**
Ransomware	**Phishing**	**C&C**
Software encrypting user files and denies access until ransom is paid.	The activity of defrauding an online account holder of financial information by posing as a legitimate company.	Command and control servers (C&C servers) are computers that issue commands to members of a botnet.
98%	**100%**	**56%**
Files Downloadable Malicious Files such as: Exploits, Malwares, Ransomwares, Payloads, Worms.	**Exploits** An exploit kit is a software kit designed to run on web servers, with the purpose of identifying software vulnerabilities.	**Policy** Using categories for URL filtering is the quickest and easiest way to block access to productivity-sapping or harmful websites and avoid potential HR issues.

A very important detail that can be observed in the Assessment Result shown above is that the highest percentage penetration for the **web gateway vector** this month comes from exploits at 100%, it is also worth mentioning that there are two additional high penetration rate simulations, Files (98%) and Policy (56%).

Simulation with High risk that penetrated your organization:

Malware with 33 Payloads in high risk, Ransomware with 15 Payloads in high risk, Worm with 9 Payloads in high risk.

505 of the files used in the web gateway vector that penetrated successfully are of high risk.

Simulation with Medium risk that penetrated your organization:

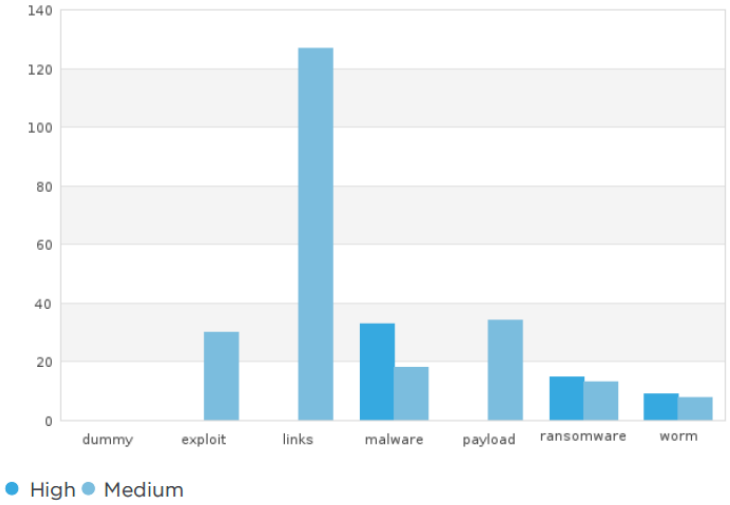
Links with 127 Payloads in Medium risk, Payload with 34 Payloads in Medium risk, Exploit with 30 Payloads in Medium risk, Malware with 18 Payloads in Medium risk,

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

Ransomware with 13 payloads in medium risk, worm with 8 Payload in Medium risk.

453 of the files used in the web gateway vector that penetrated successfully are of medium risk.

Below is shown the severity of vector-email penetration by categories

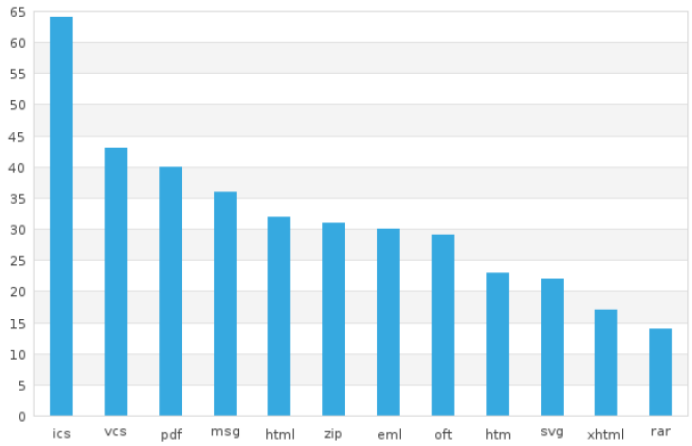


On the chart above, it is possible to recognize which simulated type of attack was successful, how many files were able to enter the perimeter.

Below is the 10 Top of Files Types that were able to penetrate your security.

Top 10 Penetrated file types

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



The chart above illustrates the file types that were used on the simulated attack, and were able to access the network, we can also see the count for each one.

Executive Action Items

40% of Risk Reduction with no business impact	**Maximize your Security** **Effectiveness** Mitigation is possible by only reconfiguring your current security products without impacting the business. See the Recommendations below.
9% of Risk Reduction with business impact	**Budget Re-Allocation** Consider purchasing a third party solution in order to reduce risk and not impact the business : 1. Sandbox. 2. File Content Disarm and Reconstruction. See the Recommendations below.

69% files that penetrated

Check if your network is already compromised

The MSS-BAS showed that various attacks could compromise your local network. Scan your local network to see if it's already has been compromised by this type of attacks in the next days.

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.

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.

This simulation showed that various attacks can compromise your local network.

1. Short term recommendations, that must be implemented immediately to reduce the exposure in the e-mail vector: Mail Relay, Content disarm and reconstruction or sandbox solutions:
   For ics files it will solve 11% of the flaws

   For vcs files it will solve 8% of the flaws

   For pdf files it will solve 7% of the flaws

   For msg files it will solve 6% of the flaws

   For html files it will solve 6% of the flaws

   For zip files it will solve 6% of the flaws

   For oft files it will solve 5% of the flaws

   For html files it will solve 4% of the flaws

   For svg files it will solve 4% of the flaws

   For xhtml files it will solve 3% of the flaws

   According to the simulation, the file extensions that are most able to enter the network are the .ics and .vcs Both of these extensions refer to a calendar format, commonly used by calendar applications such as Microsoft Outlook, Apple Calendar and Android Calendar.

2. 4 % and 5 % of the e-mails containing malware that penetrated the security are considered as High and Medium probability of occurrence, respectively. An example of this type of High to Medium Probability of occurrence is the

WannaCry Ransomware. This type of ransomware is of high impact to the organization. *Contact your GLESEC representative for assistance with effective protection against ransomware.*

3. This month, some e-mails containing malicious files that use exploits for Microsoft Office Suite 2007 and 2010, WinRAR, Firefox 50.0.1, among others were allowed through, as was reported last month. Also, at the Gateway level a number of exploits that affect Adobe Flash Player, Internet Explorer and Firefox under Windows and Linux were able to bypass it. Old versions of software are vulnerable to many exploits which can be hidden within files that should be allowed because they are of regular usage. It is important to keep the software updated with the latest patches to prevent attackers from using these exploits, this process can be done manually or automated using an endpoint manager to check and enforce compliance policies. *Contact your GLESEC representative for assistance with this.*

4. This month, in the Web Gateway vector simulation detected a large number of URL that were able to bypass the Gateway; also, the majority of files sent in the simulation were able to penetrate the Gateway. If the issues at the Gateway are corrected, it is possible that this also lowers the risk level in the email vector.

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. *Contact your GLESEC representative for assistance with the more effective ways to handle this.*

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. Contact your GLESEC representative for assistance with this.

7. There are obsolete cipher suites, such as SSL RC4, SSLv2 and v3, in use that

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

should be disabled to minimize the amount of vulnerabilities that could be exploited. We recommend the use of TLS v1.2 as it's the latest stable version.

8. The version of PHP running on http://208.99.166.235/ is 5.6.x or lower, it is recommended to update to the version 7.2, as is the latest stable version.

GLESEC
www.glesec.com
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 57 threats that have a higher level of impact as a High risk, which are Worm, Malware and Ransomware.

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: 33 files that await remote commands from a command and control server.
- Ransomware: 15 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.

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

- Worms: 9 files disguised as Office Macros that attempt to spread through the network to infect other computers.

Please refer to the recommendations number 5.

Successful Medium level simulated attacks

Email vector: 230 files within this severity indicator were able to penetrate the perimeter and they can be broken down into 3 different categories:

- Ransomware: 13 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. Please refer to the recommendations section, items number 2 and 3.

- Exploit: 30 files targeting five different vulnerabilities. The first one aims to instigate a stack overflow attack MSCOMCTL.OCX, this attack targets Microsoft Office 2007 and 2010. The second vulnerability refers to a flaw in email gateways that allow an external agent to bypass them by inserting Object linking and embedding in a PowerShell environment. The third vulnerability used, makes uses of Microsoft Word macro to gain access to a power shell command line. The fourth vulnerability allow remote code execution in older Firefox versions (50.0.1 or lower). The fifth vulnerability uses an undocumented feature in Microsoft Word that allows malicious attackers to collect information about the OS and software versions remotely. Please refer to the recommendations section, item number 1.
- Worms: 8 files that are run automatically by the Office Macro scans ports and infects other computers in the network.
- Links: 127 payloads that redirect to webpages that host malware attempting to download it to the victim's computer.
- Payloads: 34 infected files that periodically take screenshots of the user's desktop and attempts to read input from the user.

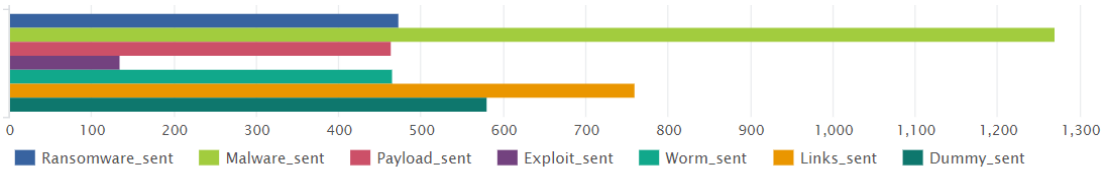
The other types of attacks sent by this simulation were blocked by your Organization security countermeasures.

Successful Low level simulated attacks

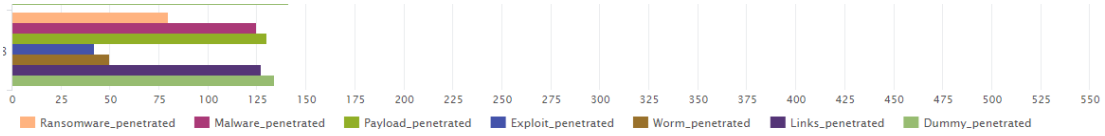
401 out of 2375 low risk malicious codes were able to access your network. These types of files are considered of low risk because (a) they require many clicks to execute or (b) even if they were executed they don't cause a high impact. By securing the network against higher severity criteria mentioned before in this report, it is likely that the amount of low risk malware that penetrated is also reduced.

Graph: e-mails Sent

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



Graph: e-mails Penetrated



Graph: e-mail Vector Attack Summary

Here are the number of e-mails containing malware sent during the attack simulation Vs. the ones that penetrated your organization: 474 Ransomware sent, 80 penetrated; 1270 Malware sent, 125 penetrated; 464 Payload sent, 130 penetrated; 135 Exploit sent, 42 penetrated; 465 Worm sent, 50 penetrated; 759 Links sent, 127 penetrated and 580 Dummy sent, 134 penetrated.

email	Ransomware_sent	Malware_sent	Payload_sent	Exploit_sent	Worm_sent	Links_sent	Dummy_sent	Total
cymulate.test@ieee.org	474	1270	464	135	465	759	580	4147

email	Ransomware_penetrated	Malware_penetrated	Payload_penetrated	Exploit_penetrated	Worm_penetrated	Links_penetrated	Dummy_penetrated	Total
cymulate.test@ieee.org	80	125	130	42	50	127	134	688

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>

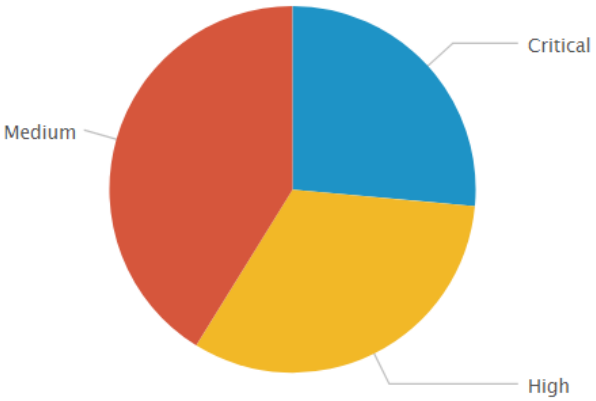
The score of a vulnerability is determined by its risk factor; Critical, High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed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

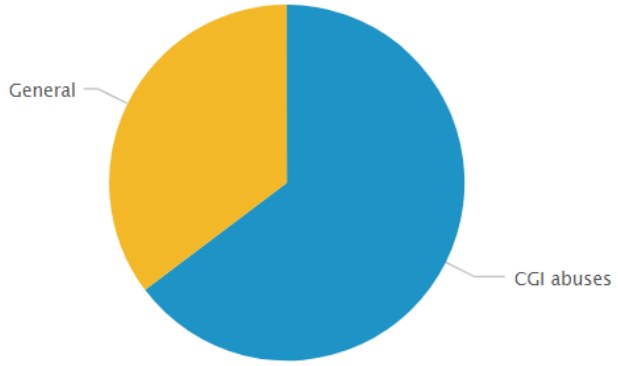
Low risk if they have a CVSS base score of 0.0 – 3.9
Medium risk if they have a CVSS base score of 4.0 – 6.9
High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerability Information

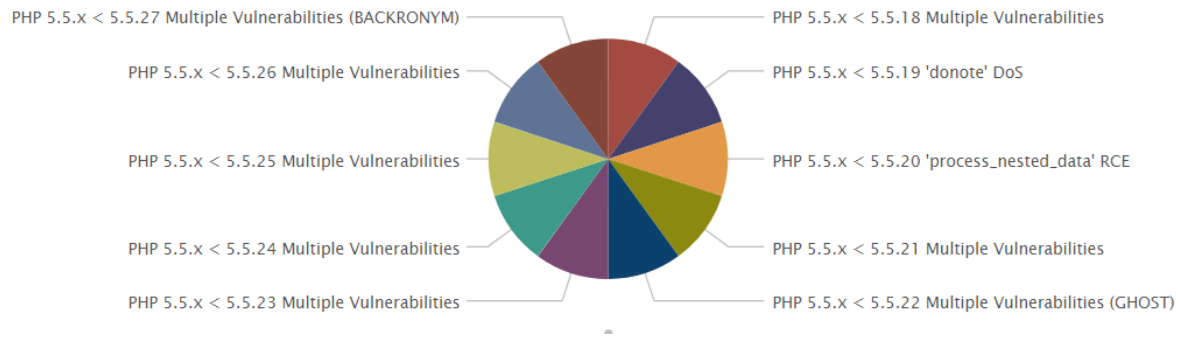
Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period



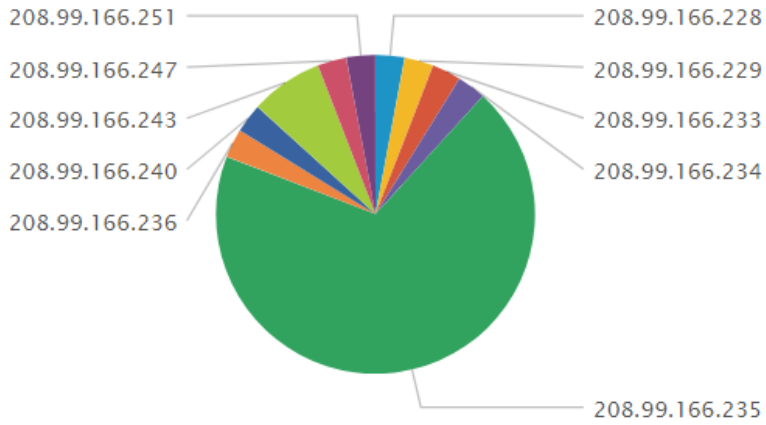
Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



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

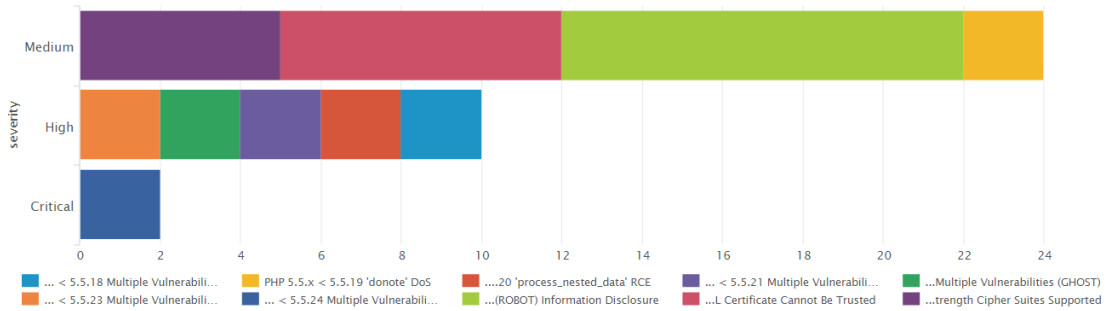


Graph: Most Vulnerable Host
This report depicts the most vulnerable hosts discovered this report period



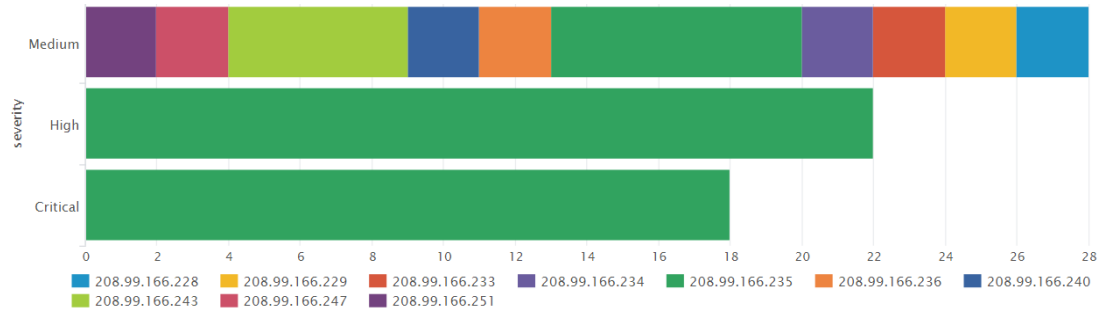
Graph: Vulnerability Risk by Vulnerability Name

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



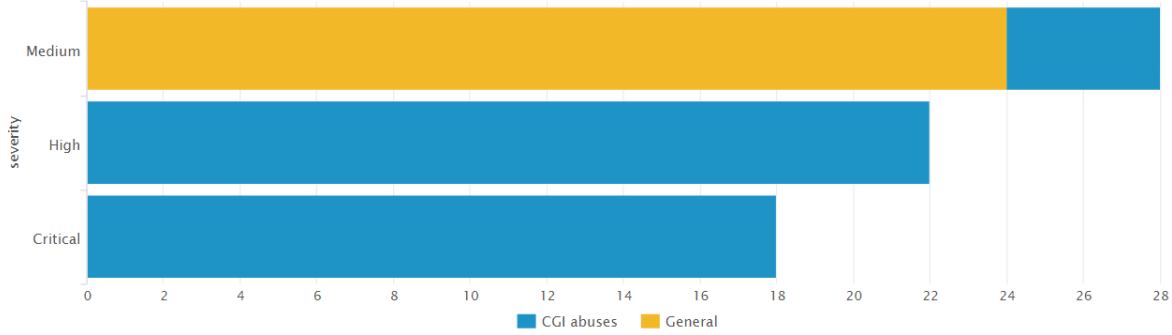
Graph: Vulnerability Risk by Host

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



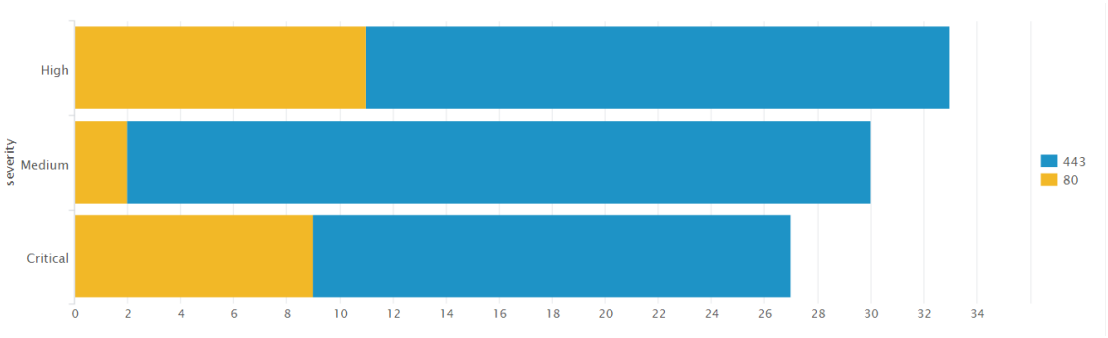
Graph: Vulnerability Risk by Category

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



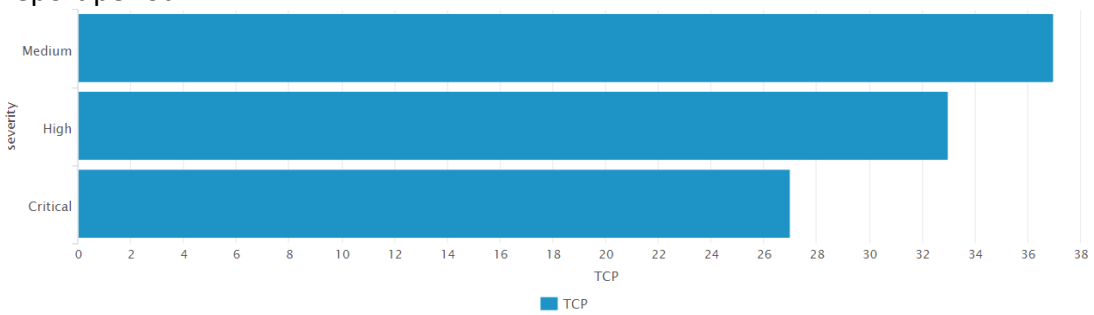
Graph: Vulnerability Risk by Port

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



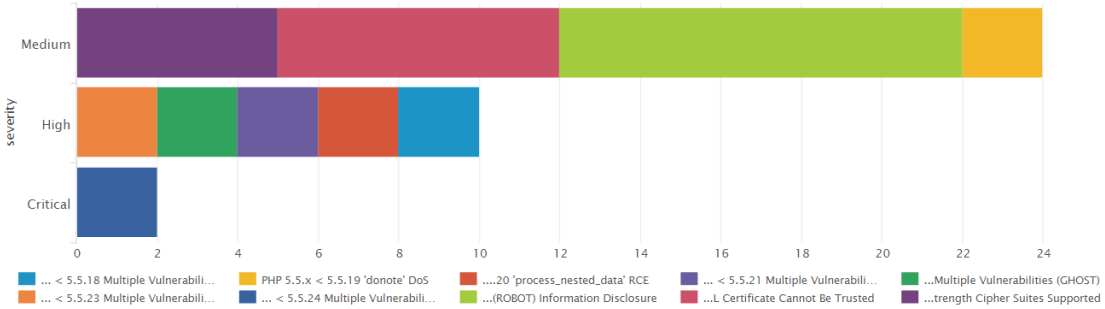
Graph: Vulnerability Risk by Protocol

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



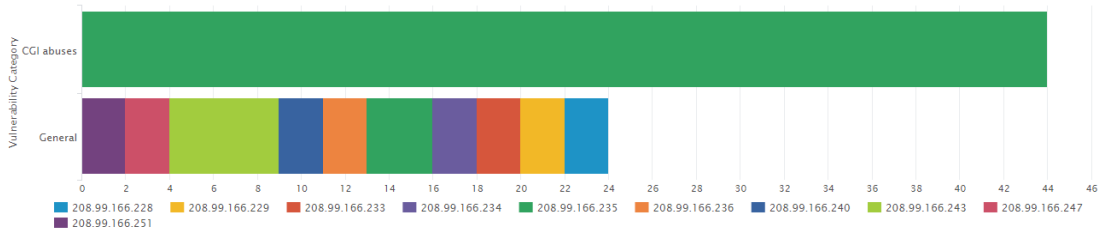
Graph: Vulnerability Category by Vulnerability Name

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



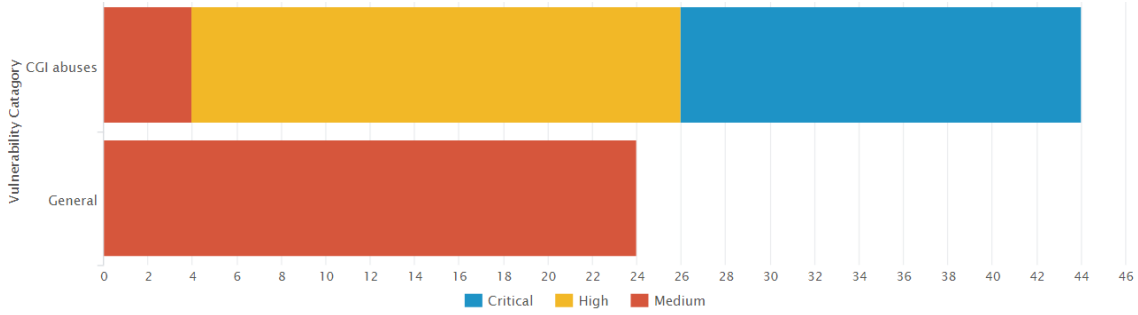
Graph: Vulnerability Category by Host

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



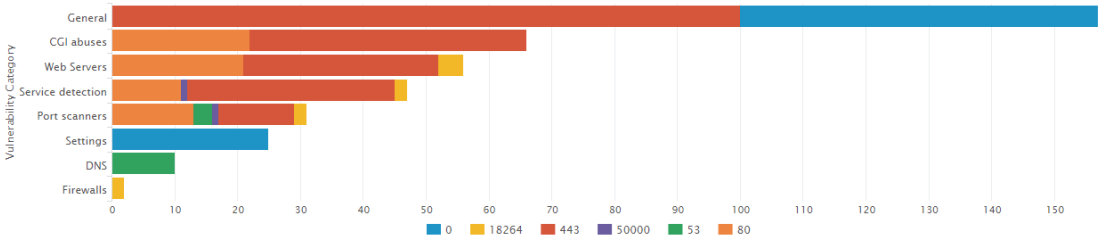
Graph: Vulnerability Category by Risk

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



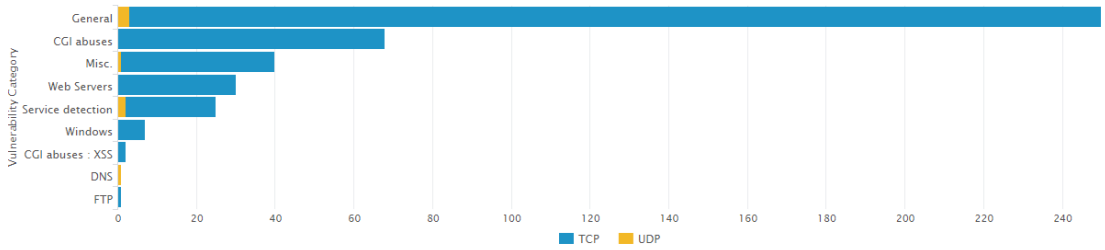
Graph: Vulnerability Category by Port

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

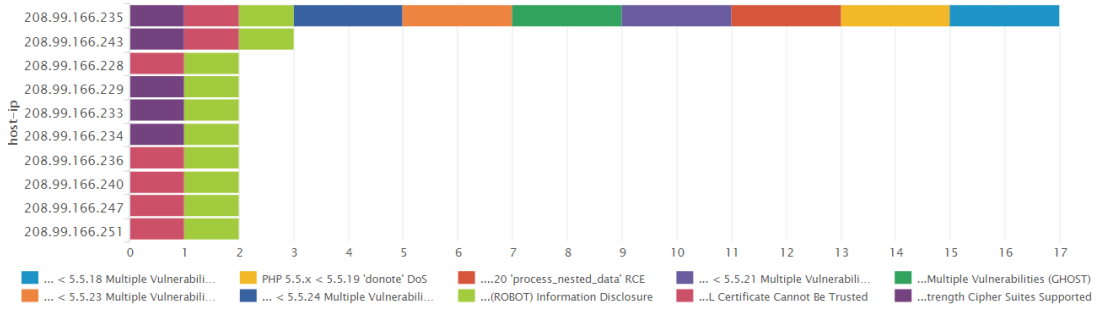


Graph: Vulnerability Category by Protocol

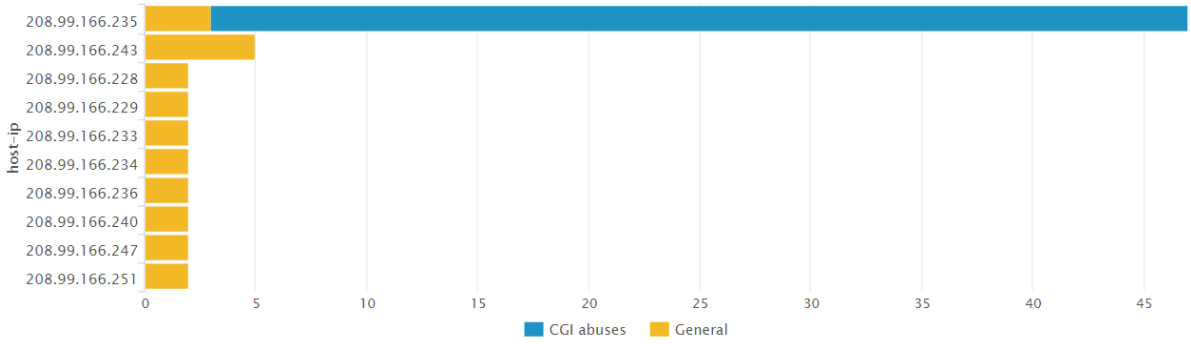
This report illustrates the vulnerability category and count by protocol discovered this report period



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

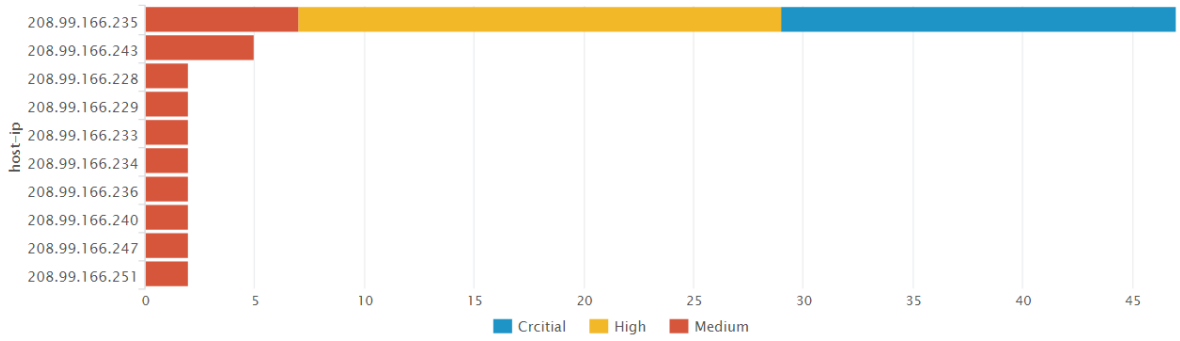


Graph: Host by Vulnerability Category
This report illustrates the vulnerability category and count by hosts discovered this report period.



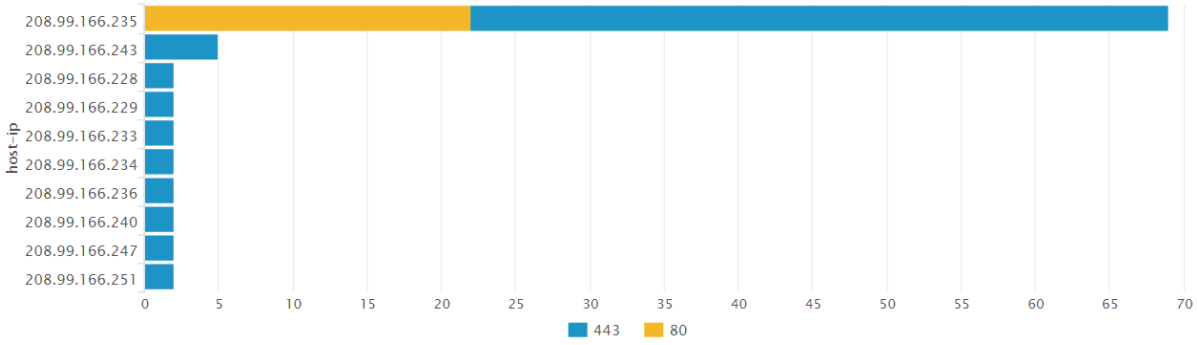
Graph: Host by Vulnerability Risk

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



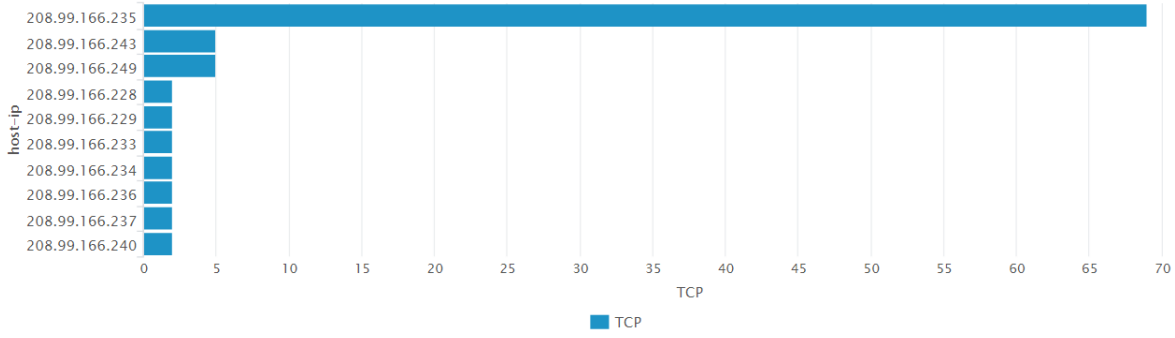
Graph: Host by Port

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.

Ticket#	Title	Created
2018011210000021	Fwd: MSS-BAS Activation	2018-01-12 11:00:05

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

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

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

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

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

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