OPERATIONS & INTELLIGENCE EXECUTIVE CYBER SECURITY REPORT

Fairwinds Credit Union

October, 2018.

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com

Table of Contents

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

About This Report

The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed. The more complete the set of services under contract the more accurate and complete the results will be.

The report is organized in three parts; the first is the Executive Summary with recommendations (as necessary or applicable), the second is the Intelligence Section with more detailed information and analysis dashboards and the last one 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 activism are the very cause of information security exposure and are most commonly driven by financial gain. GLESEC's outsourcing services, based on its proprietary 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		
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS	TEST	
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 is based on the simulations for the MSS-BAS e-mail, Gateway and WAF vectors conducted on October 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

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

Board and Management of the company.

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

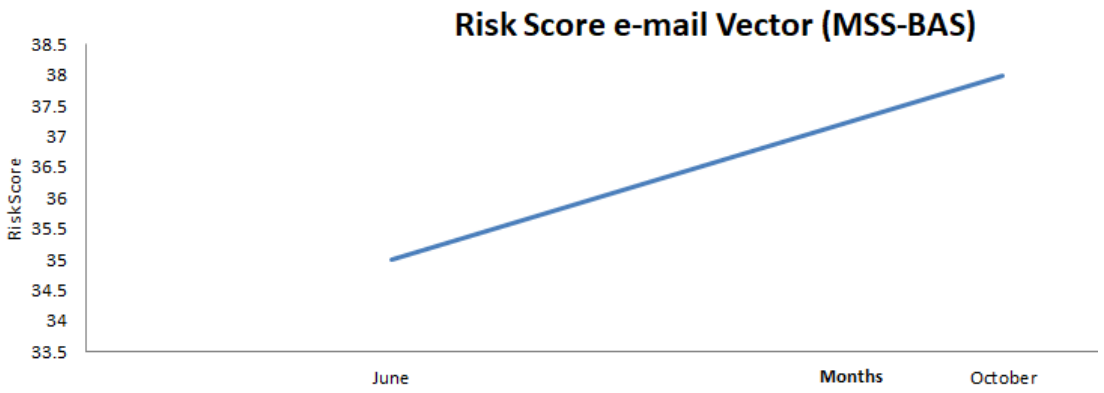
We determine that the risk condition for Fairwinds for the month of October is a concern. This can be seen from the various security indicators as indicated below.

Risk Indicator	Service	Condition	Comments
Risk Score	MSS-BAS email Vector	MEDIUM	While the condition is "medium" this does not mean that it is protected enough. The score is 38% which when it reaches 68% becomes critical. It only takes one malicious application like Ransomware to compromise the organization.
Risk Score	MSS-BAS WAF Vector	MEDIUM	The condition is "medium", there have been improvements since the last test but there are still additional configurations that could reduce the risk level.

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

Risk Score	MSS-BAS Web Gateway Vector	MEDIUM	While the condition is "medium" this does not mean that it is protected enough. The score is 21% which when it reaches 68% becomes critical. It only takes one malicious application like Ransomware to compromise the organization, particularly vulnerable to Wannacry and Petya Ransomware.

The Risk Score based on the simulation for MSS-BAS e-mail vector is: **38%**

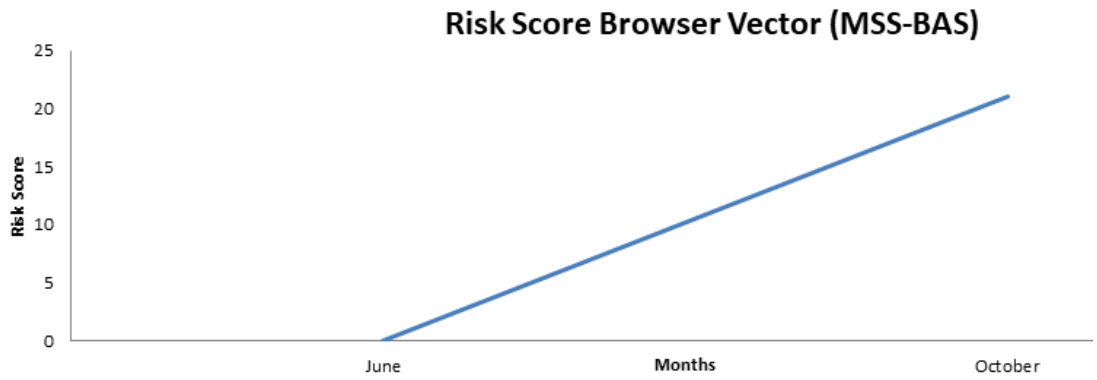


This histogram shows the trend of the risk value for the e-mail vector over several months, there is data from the simulations ran in June and the present simulation; the Risk Score was 38% which is considered "medium". From the 52 e-mails containing malware that were sent, 29 were able to successfully penetrate.

The most relevant types of malware that was able to penetrate were Exploit, Ransomware and Worms.

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

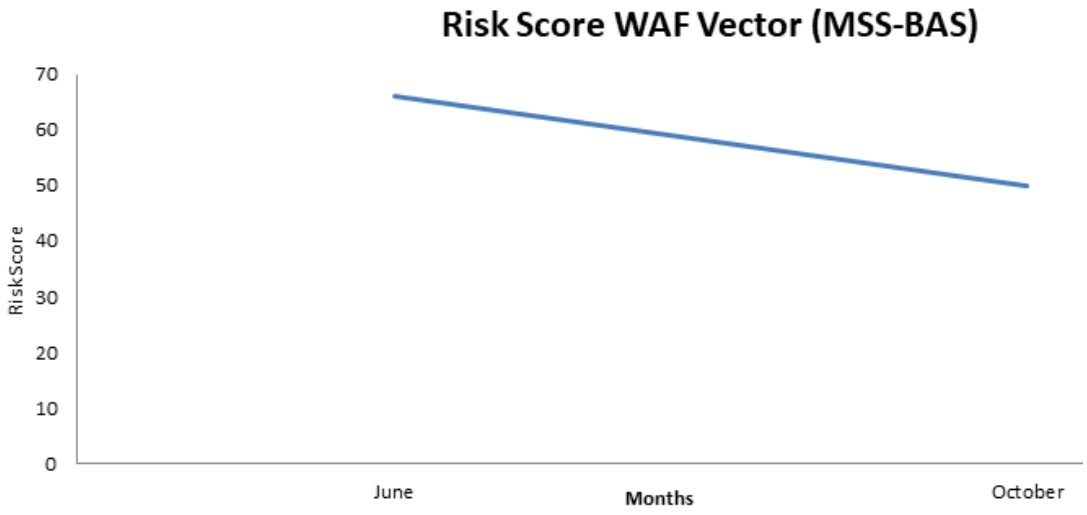
The Risk Score based on the simulation for MSS-BAS Web Gateway vector is: **21%**



The histogram shows the risk score for the simulations in this vector, however at the present, there is only data for the month of September with a score of 21%. Of the 3368 samples sent for inbound connections, 3340 were able to pass and 6 of the 394 samples set for outbound connections were able to pass.

The test showed that most file samples were able to pass the web filter, and that the policies in place are not limiting common malicious URLs.

The Risk Score based on the simulations for the MSS-BAS WAF vector, conducted on the URL: www.fairwinds.org is: **50%** which is considered medium.



The test showed that this site is vulnerable to critical and severe attacks of: Command Injection, XSS and SQL Injection.

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 enables organizations to know different metrics that are used to measure and know your security position: a "Security Exposure Level", and "Risk Score" and types and severity of the malware that you are exposing to, via the different vectors.

The Security Exposure Level can be "low", "medium" and "high" depending on the value of the "Risk Score" which is a percentage. If the Risk Score is: between 1% - 33%, the Security Exposure level is considered "low", between 34% - 67% the Security Exposure is considered "medium" and between 68% - 100%, the Security Exposure is considered "high". 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.

The Risk Score is calculated based on different parameters. For instance when considering the e-mail vector, one of the parameters considered is the number of e-mails containing malicious software that are able to penetrate your security. Other factors are the type of malware and the "risk" for that malware. Taking ransomware as an example, 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 following table summarizes the current security posture of your organization according to our MSS-BAS service.

Simulation Summary

Vector	Sent	Penetrated
Mail	52	29
Web Gateway	3785	3368
Hopper	-	-
Web Application	502	220
Data Exfiltration	-	-

From the table, something notable is that for the Web Gateway vector the ratio of successful penetrations is high. For the mail vector, at least half of the samples were able to penetrate the security measures in place and for the web application the number of successful penetrations is significantly lower than the total sent samples. For all the vectors tested there is room for lowering the risk.

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

Mail Attack Summary

The **"e-mail Security Exposure Level"** for your company for this simulation was classified as "medium" based on the "Risk Score" of 38%.

38/100

Mail

In the **e-mail simulation** shows that 12 different file types, holding a malicious-payload within, were able to penetrate your security measures (See "Files detected as ALLOWED"). This is something that the organization must take immediate action, because this means that, as right now, you do not have a proper set of security measures in place that are analyzing, blocking or dropping any e-mails, with those file types, leaving them as a potential path to infection with malware that leverages these files types.

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

Low

File: DummypayloadBatPdfHtmlscript.html

The payload consists of a .bat script embedded in a PDF file that is downloaded from a HTTP/S server. The link to the PDF file is sent to the user via email inviting the user to download the PDF file.

Medium

File: MscomctlbofDocPdf.pdf

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

High

File: cryptovarExeVcs.vcs

The VCS file a calendar type file that fetches an executable ransomware in a remote server. This 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 Summary

For this simulation, the risk score of your organization is considered **low risk**. The risk score for this month is 21%. But it is important to consider the amount of high risk simulated attacks that were successful.

Risk Score:

21/100

Web Gateway

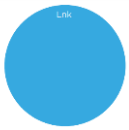
Test Your HTTP/HTTPS Outbound Exposure to Malicious Websites.

Riskiest file types that were 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: MscomctlbofDoc.doc

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. This file is a .doc file that exploits a stack overflow vulnerability using a malicious RTF. This exploit affects Office 2007 and 2010.

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

High

File: wormmacroDocm.docm

This is a worm that attempts to use Lateral Movement to spread through the network, exploiting the current primary user token. This worm comes packed in a macro file for Word.

WAF Attack Summary

For this simulation, the risk score of your organization is considered **medium risk**. The risk score for this month is 50 %, which is considered a "medium" risk level.

Risk Score:

Observations

This report made to an URL of your organization determined that 50% of the simulated attacks of the WAF vector were successful. It is very important to clarify the following points:

1. We are assuming that the WAF protecting your websites is fully operational.

2. Please check if the URL that was supplied to us: https://www.fairwinds.org is being protected with the Web Application Firewall, WAF.

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. The service MSS-BAS e-mail vector, 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:

To detect malicious file that could be hidden within another file type, solutions such as Sandbox/**Content-Disarm & Reconstruct** can be implemented. A Sandbox solution 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.

2. The WAF simulation showed that half of the samples used in the test were able to pass. The types that had most success were: Command Injections, SQL injections and Cross-site Scripting (XSS).These types of attack can be mitigated by validating untrusted inputs (character sets, length), using regular expressions to neutralize characters that have meaning in the command-line and also implementing least privilege in the web applications to limit the potential damage in case an attack is successful. Keeping the WAF signatures up to date also help to mitigate common patterns of attacks

that target web applications.

3. 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.

4. 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.

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.

Graph: Risk Score Vector E-mail

38 %

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

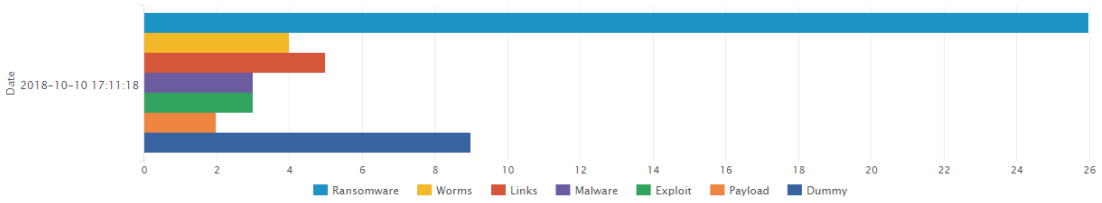
Graph: Attack Type Summary Vector E-mail

Ransomware	Worms	Links	Malware
65 %	50 %	0 %	0 %
17 / 26	2 / 4	0 / 5	0 / 3

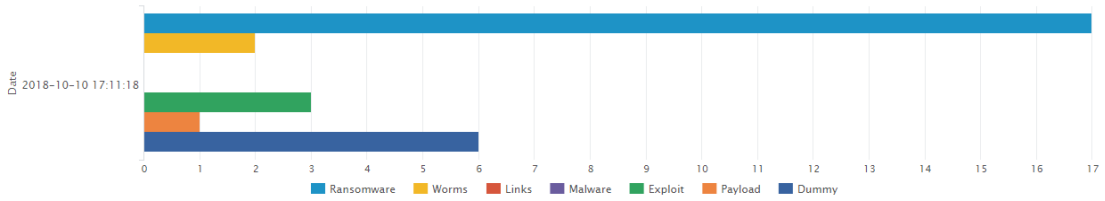
Exploit	Payload	Dummy
100 %	50 %	67 %
3 / 3	1 / 2	6 / 9

Graph: e-mails Sent

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



Graph: e-mails Penetrated



Graph: E-mails Sent / Penetrated

Desc	Ransomware	Worms	Links	Malware	Exploit	Payload	Dummy
Penetrated	17	2	0	0	3	1	6
Sent	26	4	5	3	3	2	9

Definitions

Links refers to files from the internets, that incite the user to visit a malicious website 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

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