



MANAGED BREACH ATTACK SIMULATION
Inspira Health Network
December 2017

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

Info@glesec.com
www.glesec.com

CONFIDENTIAL

Table of Contents

About This Report	3
Scope of this Report	4
Executive Summary	5
Cyber Security Validation	6
Recomendations.....	10
Definitions	11

CONFIDENTIAL



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.



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		

CONFIDENTIAL



Executive Summary

This report corresponds to the period December 2017.

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

	RISK / RIESGO
	VULNERABILITIES / VULNERABILIDADES • MSS-VM Service
	THREATS / AMENAZAS • MSS-APS; MSS-EPS; MSS-SIEM; MSS-EIR; MSS-UTM
	ASSETS / ACTIVOS • MSS-VM; MSS-EPS
	COMPLIANCE / CUMPLIMIENTO • MSS-EPS
	SECURITY VALIDATION / VALIDACION • MSS-BAS
	TRUSTED ACCESS / ACCESO CON CONFIABILIDAD • MSS-TAS

RISK

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

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

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

CONFIDENTIAL



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

Risk conditions based in test MSS-BAS e-mail vector
December 2017
E-mail Security Exposure Level: High
Risk Score



Within the set of threats that can penetrate via email, exists a high percentage of penetration in critical threats mainly of Ransomware, exploits, followed by dummy. For our analysts the Risk Score for your organization is of High level.

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

CONFIDENTIAL



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 y High probability Ransomware, depending of the probability of occurrence.

The "e-mail Security Exposure Level" for your company this month was classified as "High" based on the "Risk Score" of 48%.

In this simulation 62% 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.

Simulation Summary 24/44

<u>Risk Level</u>	<u>Sent</u>	<u>Penetrated</u>
High	15	3
Medium	8	7
Low	21	14

CONFIDENTIAL



MSS-BAS e-mail vector Risk Summary Matrix

E.g: Vulnerable to a Medium Probability Ransomware like WannaCry	21%	13%	E.g: Vulnerable to a High Probability Ransoware like WannaCry
E.g: Vulnerable to a Low Probability Payload like Meterpreter Shell	58%	8%	E.g: Vulnerable to a High Probability Payload like Meterpreter Shell

Probability →

Impact ↑

Assessment Result

33% Worm Software using Common techniques in order to spread itself inside a Windows based network.	58% Ransomware Software encrypting user files and denies access until ransom is paid	0% Malware Malware, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.
56% Dummy Dummy category is code execution proof of concept without actual damage to the system.	100% Exploit Known and signed exploits of commonly used software that leads to code execution because of vulnerabilities discovered.	50% Payload Common attacks delivered to clients like: Data extraction attacks or Stagers downloading the real malware.
		N/A Links A malicious website is a site that attempts to install malware onto your device.

A very important detail that can be observed in the Assessment Result shown above is that the penetration of files containing malicious Exploits was of 100% and

CONFIDENTIAL



Ransomware 58%. After these threats enter the network they can be executed in many different ways causing high impact to the organization. This high risk factor indicates that your organization is very vulnerable via e-mail to these types of attacks.

Executive Action Items

13% 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.

35% 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.

62% 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 been compromised by this type of attacks in the next days.



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. It's been detected that many of e-mail containing malicious files that use exploits were able to penetrate the network in 100% of the ones used for this evaluation. Old versions of software are vulnerable to many known exploits, malicious code can be hidden within files that should be allowed because they are of regular usage, and bypass many security measures. 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.
2. 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.
3. 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.



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