OPERATIONS & INTELLIGENCE TECHNICAL 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 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

Managed Breach Attack Simulation Service (MSS-BAS)

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.

Summary

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 expose 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.

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

MSS-BAS RISK SCORE- COMPARISON WITH LAST TEST

MONTH	EMAIL	GATEWAY	WAF	MOST VULNERABLE TO
OCTOBER	38%	21%	50%	Exploits, Command Injection
JUNE	35%	N/A	66%	Exploits

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

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.

Mail Attack Summary

Within the set of threats that can penetrate via email, during this test the most successful vector of attack is exploits, followed by ransomware, and lastly worms and payloads. For our analysts the Risk Score for your organization is of Medium level. The proof of concept for this vector is based on real threats. All vectors, in a continuous cycle have to be considered to give an idea of the security state of all your infrastructure.

Risk conditions based in test MSS-BAS e-mail vector. October 2018
E-mail Security Exposure Level: Medium

Risk Score:

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

Least vulnerable to:

links

*links to bad websites.

Most vulnerable to:

exploit

*i.e: adobe, office, browsers exploits.

E-Mail vector Attack Summary: 29/52

Risk Level	Sent	Penetrated	%
High	16	5	31%
Medium	13	4	31%
Low	23	20	87%

Attack Type Simulation

Here is a description of the attacks by attack category.

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

Attack Type	Sent	Penetrated	%
Exploit	3	3	100%
Ransomware	26	17	65%
Malware	3	0	0%
Worm	4	2	50%
Payload	2	1	50%
Dummy	9	6	67%
Links	5	0	0%

A very important detail that can be observed in the Summary is that the highest percentages of penetration for the **email vector** come from exploits, ransomware and worms at numbers between 100% through 50% success rate. These exploits are present in outdated versions of Microsoft Office, Adobe Software Suite and present in Windows itself. Exploits vector can be mitigated by keeping all the software up to date with the latest hotfixes.
After these threats enter the network they can be executed in many different ways causing high impact to the organization.

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

Top 2 successful simulations for email vector – comparison with the last test

MONTHS	RANSOMWARE	WORMS	EXPLOIT
OCTOBER	65%	50%	100%
JUNE	47%	54%	55%

The table summarizes the percentage of successful simulations for the three categories we consider the most relevant for each vector compared with the results of the previous test. The results for the present test show that all the categories are above 50% of successful penetration. Compared to the previous test in June, exploits had the most increase in success.

Infected Simulated File types

The following charts show the infected simulated files by filetype, with the percentage of successful infiltrations.

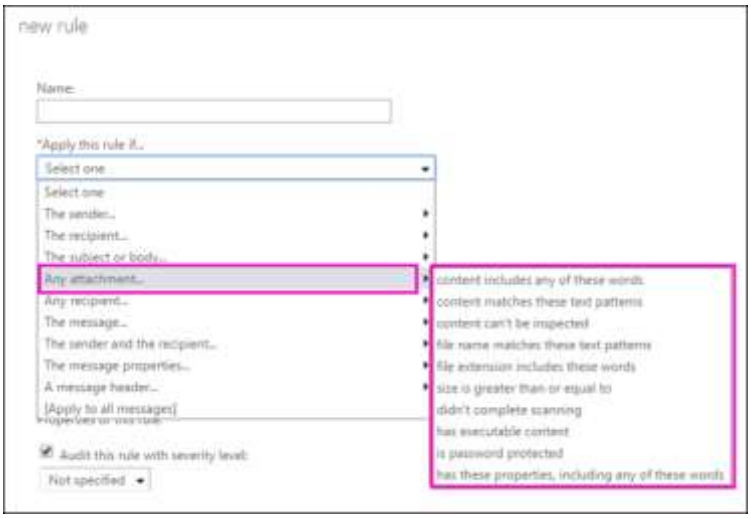
Files types detected as ALLOWED.

The chart above illustrates the file types that were used on the simulated attack and were able to access the network.

Remediations for the most popular mail servers

If any of the file extensions shown, is not part of the allowed file types in your organization, it would be recommended to create a rule in the antispam filters and/or the email server. Based on the results and the information provided there are some adjustment that can be done on the most popular mail servers (Exchange, Postfix and Send mail) to reduce the number of file types that can penetrate the network.

Microsoft Exchange, comes with several options to analyze mail with attachments that arrives to the Exchange Server, these rules can be created in Exchange Admin Center (EAC).



Microsoft Exchange can analyze various common file types and verifies if the file extension match with the content of the attachments. Microsoft has a list of all the supported file types in the following link.

https://technet.microsoft.com/en-us/library/jj919236(v=exchg.150).aspx

Other common mail server solutions are Postfix and Sendmail. Sendmail comes integrated with some measures of anti-spam features in version 8 and later but not with anti-malware. Postfix also comes integrated with anti-spam filters but not with antimalware scanners/filters as Exchange. Both platforms can be integrated with software that fulfill those roles, common examples are *Spamassassin* and *ClamAV*. Integration of the software depend on the OS that is running the mail server.

Successful high level simulated attacks

We found 5 threats that have a higher level of impact as a High risk, which are Worm 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:

- Ransomware: 5 files were able to penetrate the perimeter at this level. These are considered as high risk due to the low number of clicks required to execute them and the fact they are using common extensions to disguise themselves, so users are more prone to execute them by mistake.
- Worms: 1 file, a compressed file that contains a specially crafted doc file that attempt to spread through the network to infect other computers using the token of the user that executes the payload.

Successful Medium level simulated attacks

Email vector: 4 files within this severity indicator were able to penetrate the perimeter, these are the highlighted categories:

- Ransomware: This file was able to penetrate the perimeter at this level as well, what this means is that using different combinations for containing this malicious code was successful in entering the network. This type is considered medium risk because it requires more clicks to be executed, as contained in more different types of files. The one that was able to access your network was:

- SVG-ZIP-EXE

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

- Exploit: The files that could enter the network target different vulnerabilities. For example, one aims to instigate a stack overflow attack MSCOMCTL.OCX, this attack targets Microsoft Office 2007 and 2010. There is another exploit that makes use of a vulnerability present in the Adobe Software Suite that allows a user to execute arbitrary code by using a specially crafted PDF file, this exploit affects Adobe versions lower than 8.1.3.
- Worms: files under this category, are run automatically by the Office Macro scans ports and infects other computers in the network.

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

Successful Low level simulated attacks

20 out of 23 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.

Web Gateway Attack Summary

For this month's test, 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.

21/100

Web Gateway

Test Your HTTP/HTTPS Outbound Exposure to Malicious Websites.

Least vulnerable to:

Exploits

*i.e: adobe, office, browsers exploits.

Most Vulnerable to:

Files

*i.e: WannaCry, Petya.

The following table summarizes the threat level of the tests done, how many simulated attacks were sent and how many accessed the network. As seen below, a high percentage medium threats and more than half of the high-risk threats were able to access the network along with all the low risk samples sent.

Simulation summary: 3346/3789

Risk Level	Sent	Accessed	%
High	874	551	63%
Medium	541	457	84%
Low	2347	2338	100%

Assessment Result

Attack Type	Sent	Accessed	%
Exploits	12	0	0%
Ransomware	149	0	0%
C&C	176	3	2%
Phishing	69	3	4%
Policy	23	22	96%
Files	3356	3340	100%

The table above, classifies the simulated attacks in the categories shown with their percentage of access to the network. Most files were able to access, and the table shows that known common malicious URL are not being filtered by the Policies in place.

Top 2 successful simulations for web gateway vector – comparison with the last test.

MONTHS	PHISHING	FILES	POLICY
OCTOBER	4%	100%	96%
JUNE	N/A	N/A	N/A

The table summarizes the percentage of successful simulations for the three categories we consider the most relevant for each vector compared to the last test. Since this is the first time this vector is used for your organization there is no more data. The data collected in the present test show that most infected files are accessible by the browsers and the policies in place are not blocking common malicious URLs.

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

WAF Attack Summary

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

Least vulnerable to:

File Inclusion

Most Vulnerable to:

Command Injection

The following table summarizes the successful penetrations by risk level. The table shows that at least half of the simulated high-risk attacks used in the test were able to bypass the security measures in place:

Simulation summary: 220/502

Risk Level	Sent	Penetrated	%
High	112	67	60%
Medium	39	0	0%
Low	351	153	44%

Assessment Result

Attack Type	Sent	Penetrated	%
XSS	351	153	44%
File Inclusion	39	0	0%
SQL Injection	84	41	49%
Command Injection	28	26	93%

The samples used are classified in the categories showed above, along with their successful entries to their target. Summarizing, the ratio of penetration of most attack types are lower than 50% except for command injection that has a very high ratio of penetration at 93% and File inclusion is at 0% in this test.

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation. To prevent these attacks, web applications should be avoided where possible, user input should be always avoided unless is necessary. In some programming languages there is the option to separate the execution of the process from the input parameters.

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

Top 2 successful simulations for web application firewall vector – comparison with the last test

MONTHS	COMMAND INJECTION	XSS	FILE INJECTION
OCTOBER	93%	44%	0%
JUNE	60%	60%	100%

The table summarizes the percentage of successful simulations for the three categories we consider the most relevant for each vector compared to the last test. All the percentages of samples tested for the WAF vector have lowered compared to the last test, specially the file injection category which was reduced to 0%. The exception is the command injection category that had a surge in successful penetrations against the WAF configuration.

Whole Compiled 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 may compromise your local systems.

1. The service MSS-BAS **email 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 files 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. For the MSS-BAS **WAF vector** tested, it was found that the WAF has stopped more of the samples tested than the last test, but there is still room for improvement. Proper configuration of the WAF is necessary to ensure the web servers are not affected with SQL injection, XSS and other techniques.
3. For the MSS-BAS **Web Gateway vector**, we found that the policies in place are not blocking the access to malicious file samples used in the present simulation or blocking common malicious URLs. Proper configuration of the web gateway restricts the access to non-productive websites such as social media, gambling and other sites.

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

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

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

Info@glesec.com
www.glesec.com