OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

Fairwinds Credit Union

July, 2018

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

Info@glesec.com
www.glesec.com

Table of Contents

Table of Contents 2
About This Report 3
Confidentiality 3
Managed Breach Attack Simulation Service 4
Mail Attack Summary 5
WAF Attack Summary 12
Whole Compiled Recommendations 14

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.

The **"e-mail Security Exposure Level"** for your company for this simulation was classified as "medium" based on the "Risk Score" of 35%.

In the **e-mail simulation** shows that 58 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 has to 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.

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, worms and Ransomware right after dummies at numbers between 47% through 55% success rate. These exploits are present in outdated versions of Microsoft Office 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.

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 worms, and lastly ransomware 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 (you can see the description in Appendix A). All vectors, in a continuous cycle have to be considered to give an idea of the security state of all you infrastructure.

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

Risk Score:

35/100

Least vulnerable to:

links

*links to bad websites.

More vulnerable to:

dummy

*non malicious code execution.

Mail vector Attack Summary

1643 out of 3787 simulated attacks were successful attacks.

Risk Level	Sent	Penetrated	%
High	552	87	16%
Medium	839	169	20%
Low	2396	1387	58%

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

Assessment Result

Attack Type	Sent	Penetrated	%
Exploit	150	82	55%
Ransomware	479	227	47%
Malware	1269	497	39%
Worm	466	252	54%
Payload	464	219	47%
Dummy	583	366	63%
Links	376	0	0%

On the table above a list of the types of malware that were tested against your countermeasures followed by the results for every one of them.

Infected Simulated File types

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

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

Known Exploits

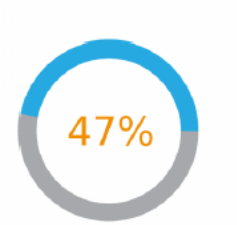
An exploit takes advantage of a bug or vulnerability in a software such as: Adobe, Word etc...

Executable Files

An executable file is a file that is used to perform various functions or operations on a computer that can be malicious.

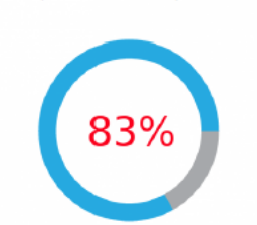
Office Files

Such as: Word, Excel, Power-point that may potentially contain malicious code execution.



Encrypted Files

Such as: Zip, Rar, 7z that may potentially contain malicious code execution and cannot be detected as



Files types detected as ALLOWED.

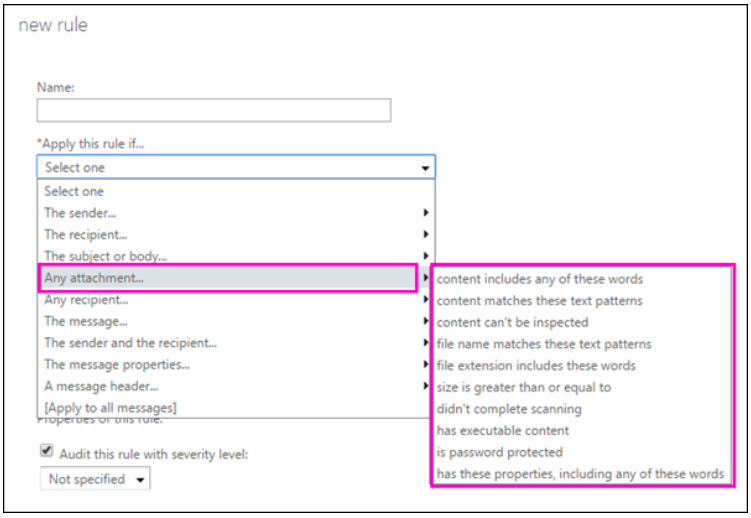
The chart above illustrates the file types that were used on the simulated attack and were able to access the network.

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 85 threats that have a higher level of impact as a High risk, which are Malware, Worm and Ransomware and dummy.

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: 31 files that await remote commands from a command and control server or try to obtain elevated privileges by disrupting the user activities with pop-ups.
- Ransomware: 26 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: 26 files disguised as Office Macros that attempt to spread through the network to infect other computers.
- Dummy: 2 file, dummy files are proof of concept of attacks, they are not real malware, but could be modified by malicious actors to carry out variations of existing attacks.

Successful Medium level simulated attacks

Email vector: 169 files within this severity indicator were able to penetrate the perimeter, these are the highlighted categories:

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

- RAR-PDF-ACCDB
- ZIP-ICS-XLL
- GZ-PDF-ACCDB
- VCS-ICS-XLM
- LZH-PDF-ACCDB
- MSG-VCS-XLT
- CAB-PDF-ACCDB
- TAR-PDF-ACCDB
- 7z-EML-PDF-ACCDB

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

- Exploit: The files that could enter the network target different vulnerabilities. For example, one aims to instigate a stack overflow attack MSCOMCTL.OCX, this attack targets Microsoft Office 2007 and 2010. Also, vulnerability makes uses of a Microsoft Word macro to gain access to a power shell command line. The third vulnerability allow remote code execution in older Firefox versions (50.0.1 or lower) (CVE-2016-9079, CVE-2017-5375). The fourth vulnerability uses an undocumented feature in Microsoft Word that allows malicious attackers to collect information about the OS and software versions remotely. The fifth exploit refers to a code injection in CSV files that allow remote code execution. The next vulnerability refers to an abuse in the Dynamic Data Exchange (DDE) protocol under Windows, that allows remote code execution from Office files without the use of macros.
- Worms: files under this category, are run automatically by the Office Macro scans ports and infects other computers in the network.
- Payloads: files under this category, periodically take screenshots of the user's desktop and attempts to read input from the user.

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

security countermeasures.

Successful Low level simulated attacks

1387 out of 2396 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.

WAF Attack Summary

For this POC, the risk score of your organization is considered **medium risk**. The risk score for this test is 66 %, which is considered a "medium" risk level.
Risk score:

66/100

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

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

Simulation summary: 1940/3309

Risk Level	Sent	Penetrated	%
High	640	333	52%
Medium	39	39	100%
Low	2630	1568	60%

Assessment Result

Attack Type	Sent	Penetrated	%
XSS	10520	6272	60%
File Injection	156	156	100%
SQL Injection	2000	996	50%
Command Injection	560	336	60%

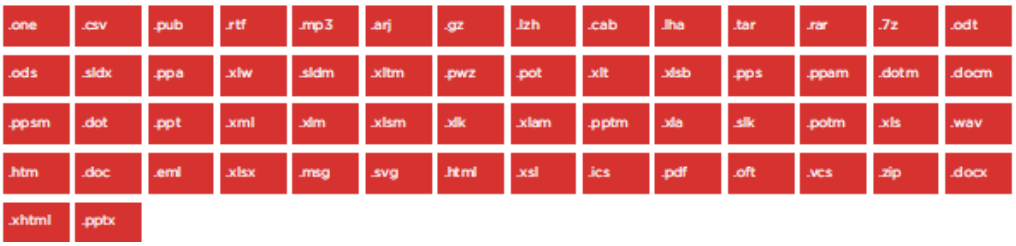
The samples used are classified in the categories showed above, along with their successful entries to their target. More than half of every attack type was able to successfully bypass the security measures in place. From the table above, the highest percentage of successful attack comes from File Injection, at 100%.
File injection refers to a vulnerability in web applications, in which the application executes a specific local or remote file due to a non-sanitized input by a malicious user. The next step, if this vulnerability is successfully exploited, is the remote code execution on the web server.

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

Complete 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 that is currently in place is no dropping or stopping many of the threats that are used in the simulations. Proper configuration of the WAF is necessary to ensure the web servers are not affected with SQL injection, XSS and other techniques.

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