MONTHLY OPERATIONS & INTELLIGENCE REPORT

TECHNICAL REPORT

Institute of Electrical and Electronics Engineers

May 2018

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

Info@glesec.com

www.glesec.com

Table of Contents

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

About This Report

This report is a companion to the Monthly Operations & Intelligence Executive Report. The purpose of this document is to provide Technical and Tactical level information, detail and recommendations to the extent that can be summarized. GLESEC processes significant amount of data and not all can be presented in a detail report format. For more information you can review the dashboards of the GMP or if necessary contact us at the GLESEC Operation Centers (GOC).

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 Vulnerability Service (MSS-VM)

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.

In the address range given by the Institute of Electrical and Electronics Engineers, we have found a total of 348 hosts, of which 101 are vulnerable. These vulnerabilities are divided in the following severities as shown in the following table. Additionally you can notice the Risk Value score of your organization according to our metrics.

Total IP's Scanned				IP's Vulnerable
348				101
Risk Distribution				
Critical	**High**	**Medium**	**Low**	**Total**
20	27	149	22	218

According to the metrics:

RV= 0.155699014

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

In general, Institute of Electrical and Electronics Engineers vulnerabilities in this period have been Critical (20), High (27), medium (149), low (22); it was discovered that 101 of the 348 hosts analyzed have at least one problem of vulnerability

This month the number of discovered hosts increased and due to the fact that several of these hosts have some vulnerability, the number of vulnerable hosts was also increased.

The port considered most vulnerable for this period were 443(HTTPS), this is due to the fact that many vulnerabilities were found that are related to them and are classified at a medium severity level.

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

For all the IP we found with vulnerabilities, we did a connectivity check using the PING utility. The following addresses were unreachable. Additional tests showed that many ports were also filtered; no further information could be gathered.

- 140.98.194.12
- 140.98.194.14
- 140.98.194.15
- 140.98.194.17
- 140.98.200.17
- 14.98.200.27
- 140.98.200.30
- 140.98.200.34
- 140.98.200.35
- 140.98.200.36
- 140.98.200.37
- 208.99.166.229
- 208.99.166.251

All the vulnerabilities found in your organization belong to the following categories:

Category	Critical	High	Medium	Low	Total
General	0	0	96	13	109
Web Servers	13	14	37	4	68
CGI abuses	7	12	6	0	25
FTP	0	1	5	0	6
Misc.	0	0	1	5	6
Service detection	0	0	4	0	4

Description of the most frequent vulnerabilities by name, present in hosts

Of the 348 scanned hosts, there is a large amount of critical (20) and high (27) vulnerabilities. Many of the vulnerabilities correspond to outdated versions of ISS, Apache and PHP that reached the end of life state, this means that these versions no longer receive patches to correct or fix vulnerabilities present in the software. The recommendation for the hosts that have the mentioned outdated versions is to upgrade to a recent version, in order to receive security updates.

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

In total, there are 36 critical and 14 high vulnerabilities

Hosts with ISS 6.0:
140.98.194.90,140.98.194.88,140.98.194.86,140.98.194.85,140.98.194.61-64,140.98.194.59,140.98.194.55-56,140.98.194.52.53,140.98.194.218,140.98.194.206,140.98.194.202-203,140.98.194.197,140.98.194.192,140.98.194.189,140.98.194.176-179,140.98.194.170,140.98.194.168,140.98.194.165,140.98.194.160-161

Hosts with outdated versions of PHP (v5.4x o lower)
140.98.200.30, 140.98.200.102-103.

Host that presents an outdated version of Apaches (v2.2 o lower)
140.98.202.36

SSL Medium Strength Cipher Suites Supported

This vulnerability refers to the use of cipher suites that are no longer considered secure and are easy to crack by attackers. The solution for this vulnerability is the reconfiguration of the hosts or applications that use the weak cipher suites, to make use of more robust ones. Specifically, disable all the ciphers that use less than 256 bits, such as DES, 3DES, RC4 and AES 128/128.

The commands or tools that are used to remedy this vulnerability depend on the operating system running in the affected host.

For ISS servers, the best choice is to use the freeware tool ISS Crypto developed by Nartac Software. The tool is a graphic UI for configuring Schannel.dll, which is the Windows component responsible for the implementation of SSL/TLS, the tool follows the recommendations suggested by Microsoft in the following article:

https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc.

The configurations for Apache servers, must be done in the https.conf and ssl.conf files.

Looking at the names of some of these hosts (test.comsoc.org, beta.qa.staging.spectrum.ieee.org), we can conclude some of the servers could be used for tests or experimentations and this could be the reason that they are not

properly configured, this is reported nevertheless, since the recommendations are done with all the information available to our GOC. 19 hosts affected with this vulnerability

SSL Certificate Cannot Be Trusted

The scans performed in these hosts are done using the IP addresses, since the name defined in the certificates does not match with the IP address. This does not represent vulnerability itself, this is due the way the vulnerability scans are conducted. The hosts affected are the same hosts that present medium cipher suites. 19 hosts affected with this vulnerability.

F5 BIG-IP Cookie Remote Information Disclosure

The results of this vulnerability test, indicate the possibility that the affected hosts are F5 BIG-IP load balancers. This vulnerability exposes the IP addresses and real name of the servers that use the load balancer, because the cookies that store the information do so in plain text. The manufacturer created an article with the procedure to remedy this vulnerability by encrypting the content of the cookies:

https://support.f5.com/csp/article/K14784?sr=45997495

13 hosts affected by this vulnerability.

SSL Certificate Expiry

This vulnerability is present in hosts which have an expired digital certificate or if the certificate expires in 60 days or less. The remediation for this vulnerability is to renew the certificates for new valid ones.

Among the 12 affected hosts, there are some hosts that are also part of the hosts that present the other SSL vulnerabilities.

HTTP TRACE/TRACK Methods Allowed

This vulnerability shows that the debug configurations in the Web servers are enabled, allowing the possibility of unauthorized third parties to manipulate or reconfigure the servers. The remediation for this vulnerability is to disable the debug options, the following article explains two methods for disabling the options:

http://www.techstacks.com/howto/disable-tracetrack-in-apache-httpd.html

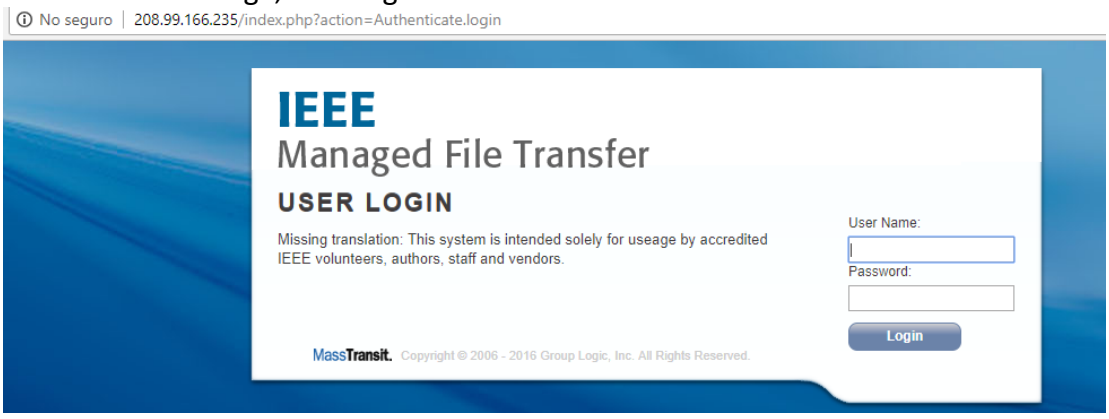
This vulnerability is present in the group of suspected test servers, as indicated by the hostname “test.comsoc.org” in the ip 140.98.202.151. There are 11 hosts affected by this vulnerability

One of the recommendations for a vulnerability found by our MSS-VME service, called **Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure** (in which a malicious user can gain information about the handshake method used during a communication with a client and could allow the malicious user to impersonate the server or decrypt communications that should be encrypted), GLESEC recommend to verify with your devices vendor if there is a patch available for the TLS implementation. In case there is no patch available, it is recommended to disable RSA key exchange and enable instead ECC (Elliptic Curve Diffie Hellman).

TheIPs,208.99.166.236,208.99.166.240,208.99.166.237,208.99.166.249,208.99.166.228,208.99.166.234,208.99.166.243,208.99.166.247,208.99.166.251,208.99.166.229,208.99.166.233,208.99.166.23547 present the ROBOT vulnerability.

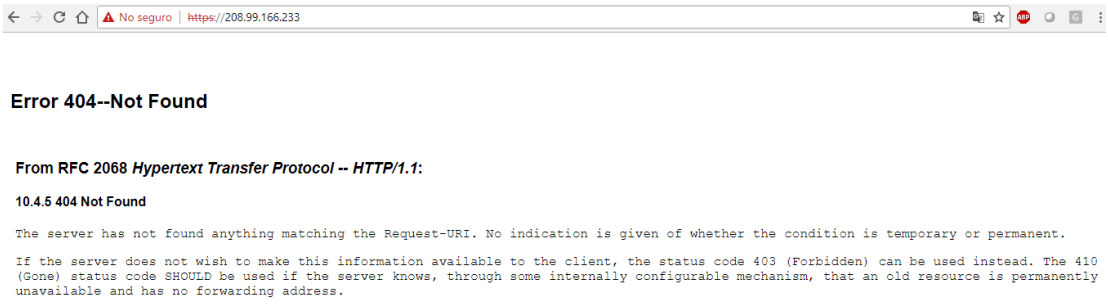
Vulnerability found correspond to SSL certificates that cannot be trusted. In these particular cases, since the tests were done using the IP address of the hosts, the name that comes in the certificate do not match with the IP. This in itself does not represent a vulnerability. To remove the message, define the IP address of the hosts as Subject Alternative Name field in the certificate.

We attach the image, showing the stated above.



The host at https://208.99.166.233/ hosts an HTTP webpage, it then tries to redirect to the HTTPS protocol and returns the error 404, as seen in the screenshot taken

below. Following the least privilege principle, if this host does not requires the use of HTTP or HTTPS protocols to perform its function, those protocols should be disabled.



Vulnerabilities by severity

The following section will describe in detail each vulnerability found according to their severity.

Critical Risk Level Vulnerability

Microsoft Windows Server 2003 Unsupported Installation Detection

Description
The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.
Solution
Upgrade to a version of Windows that is currently supported.
Affected Systems
140.98.194.52,140.98.194.56,140.98.194.64,140.98.194.85,140.98.194.88,140.98.194.90,140.98.194.160,140.98.194.161,140.98.194.165,140.98.194.192,140.98.194.202,140.98.194.203

Microsoft IIS 6.0 Unsupported Version Detection

Description
According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a version of Microsoft IIS that is currently supported.

Affected Systems
80 / tcp / possible_wls,
140.98.194.52,140.98.194.56,140.98.194.64,140.98.194.88,140.98.194.90140.98.194.160,140.98.194.161,140.98.194.165,140.98.194.192,140.98.194.202,140.98.194.203

Output

```
Installed version  : 6.0
Supported versions : 7.0 or later
EOL date           : 2015/07/14
```

PHP 5.4.x < 5.4.45 Multiple Vulnerabilities

Description
According to its banner, the version of PHP running on the remote web server is 5.4.x prior to 5.4.45. It is, therefore, affected by the following vulnerabilities :

- Multiple use-after-free memory errors exist related to the unserialize() function. A remote attacker can exploit these errors to execute arbitrary code.
(CVE-2015-6834)

- A use-after-free memory error exists related to the php_var_unserialize() function. A remote attacker, using a crafted serialize string, can exploit this to execute arbitrary code. (CVE-2015-6835)

- A type confusion error exists related to the serialize_function_call() function due to improper validation of the headers field. A remote attacker can exploit this to have

unspecified impact. (CVE-2015-6836)

- Multiple flaws exist in the XSLTProcessor class due to improper validation of input from the libxslt library. A remote attacker can exploit thse flaws to have an unspecified impact. (CVE-2015-6837, CVE-2015-6838)

- A flaw exists in the php_zip_extract_file() function in file php_zip.c due to improper sanitization of user-supplied input. An unauthenticated, remote attacker can exploit this to create arbitrary directories outside of the restricted path. (VulnDB 127122)

Solution
Upgrade to PHP version 5.4.45 or later.

Affected Systems

80 / tcp / possible_wls	140.98.200.103
443 / tcp / possible_wls	140.98.200.17,140.98.200.103, 140.98.200.30

Output

```
  Version source    : X-Powered-By: PHP/5.4.37
  Installed version : 5.4.37
  Fixed version     : 5.4.45


Version source    : X-Powered-By: PHP/5.4.40
Installed version : 5.4.40
Fixed version     : 5.4.45
```

Oracle GlassFish Server 3.1.2.x < 3.1.2.15 Multiple Vulnerabilities

Description
A ccording to its self-reported version number, the Oracle GlassFish Server running on the remote host is 3.1.2.x prior to 3.1.2.15. It is, therefore, affected by multiple vulnerabilities :

- An information disclosure vulnerability exists in the bundled version of libcurl in the smb_request_state() function due to using values that are assumed valid without properly checking boundaries. An unauthenticated, remote attacker can exploit this, via a malicious SMB server, to disclose arbitrary memory contents. (CVE-2015-3237)

- An unspecified flaw exists in the Web Container subcomponent that allows an unauthenticated, remote attacker to execute arbitrary code. (CVE-2016-3607)

Solution
Upgrade to Oracle GlassFish Server version 3.1.2.15 or later as referenced in the July 2016 Oracle Critical Patch Update advisory.

Affected Systems

80 / tcp / possible_wls	140.98.196.190
443 / tcp / possible_wls	140.98.196.190, 140.98.196.36

Output

```
Version source    : GlassFish Server Open Source Edition 3.1.2.2
Installed version : 3.1.2.2
Fixed version     : 3.1.2.15
```

High Risk Level Vulnerability

Within the High severity vulnerabilities the vast majority can be cataloged as old versions of PHP, we recommend to upgrade to the latest version of this service. Among others, there was also found a High vulnerability related to Oracle Glass fish Server which we also recommend to update to the latest version.

FTP Privileged Port Bounce Scan

Description
It is possible to force the remote FTP server to connect to third parties using the PORT command.

The problem allows intruders to use your network resources to scan other hosts, making them think the attack comes from your network.

Solution
See the CERT advisory in the references for solutions and workarounds.

Affected Systems
21 / tcp / ftp 140.98.196.80

Output

```
The following command, telling the server to connect to 169.254.237.122 on port 10794:
PORT 169,254,237,122,42,42
produced the following output:
200 PORT command successful.
```

Affected Systems
990 / tcp / ftp 140.98.196.80

Output

```
The following command, telling the server to connect to 169.254.87.122 on port 10794:
PORT 169,254,87,122,42,42
produced the following output:
200 PORT command successful.
```

Medium Risk Level Vulnerability

Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure

Description
The remote host is affected by information disclosure vulnerability. The SSL/TLS service supports RSA key exchanges, and incorrectly leaks whether or not the RSA key exchange sent by a client was correctly formatted. This information can allow an attacker to decrypt previous SSL/TLS sessions or impersonate the server.

Note that this plugin does not attempt to recover an RSA ciphertext, however it sends a number of correct and malformed RSA ciphertexts as part of an SSL handshake and observes how the server responds.

This plugin attempts to discover the vulnerability in multiple ways, by not completing the handshake and by completing it incorrectly, as well as using a variety of cipher suites. Only the first method that finds the service to be vulnerable is reported.

Solution

Upgrade to a patched version of the software. Alternatively, disable RSA key exchanges and enable ECC instead (Eliptic Curve Diffie Hellman).

Affected Systems

443 / tcp / http_proxy 208.99.166.236, 208.99.166.240
443 / tcp 208.99.166.237, 208.99.166.249
443 / tcp / possible_wls 208.99.166.228, 208.99.166.234, 208.99.166.247, 208.99.166.251

Output

```
The test sent a crafted RSA ciphertext and then sent a TLS Finished message with incorrect
padding.
The following differences in behaviour were seen by Nessus :
  - As a baseline with correct formatting : server sent TLS alert 40, server sent TLS alert 40,
server sent TCP FIN
  - With incorrect leading bytes          : server sent TLS alert 40, server sent TCP FIN
  - With the 0x00 byte in incorrect place : server sent TLS alert 40, server sent TLS alert 40,
server sent TCP FIN
  - With the 0x00 byte missing            : server sent TLS alert 40, server sent TCP FIN
  - With an incorrect version number      : server sent TLS alert 40, server sent TLS alert 40,
server sent TCP FIN
```

Affected Systems

443 / tcp / possible_wls 208.99.166.229,208.99.166.235

Output

```
The test sent a crafted RSA ciphertext and then waited, without sending a TLS Finished message.
The following differences in behaviour were seen by Nessus :
  - As a baseline with correct formatting : server waited
  - With incorrect leading bytes          : server sent TLS alert 40, server sent TCP FIN
  - With the 0x00 byte in incorrect place : server sent TLS alert 40, server sent TCP FIN
  - With the 0x00 byte missing            : server sent TLS alert 40, server sent TCP FIN
  - With an incorrect version number      : server sent TLS alert 40, server sent TCP FIN
```

SSL Medium Strength Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Affected Systems

7002 / tcp 140.98.200.22
443 / tcp 208.99.166.249
5061 / tcp / sip 140.98.200.22
443 / tcp / possible_wls
140.98.194.12,140.98.194.15,140.98.194.17,140.98.196.36,140.98.196.190,140.98.200.11,140.98.200.17,140.98.200.27,140.98.200.30,140.98.200.34,140.98.200.35,140.98.200.36,140.98.200.37,140.98.200.73,140.98.200.75,140.98.200.77,140.98.200.83,140.98.200.85,140.98.200.91,140.98.200.93,140.98.200.94,140.98.200.95,140.98.200.96,140.98.200.97,140.98.200.98,140.98.200.103,140.98.200.144,140.98.200.181,140.98.200.215,140.98.202.252,208.99.166.229,208.99.166.234,208.99.166.235

Output

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

The solution for this vulnerability involves disabling all encryption ciphers that use less than 256bit, such as DES, 3DES, RC4 and AES 128/128.

For ISS servers, the best approach is to use the freeware tool ISS Crypto by Nartac Software, which is a GUI for enabling/disabling certain cryptographic algorithms and protocols in Schannel.dll (The Windows component responsible for implementing SSL/TLS) and follows the recommendations of Microsoft according to the article https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc.

For Apache servers, the httpd.conf or ssl.conf file must be edited with the following lines:

```
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-
CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-
AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-
RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-
CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-
SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-
SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-
SHA:!DSS
SSLHonorCipherOrder on
```

The aforementioned lines can be customized to the needs of your organization, the lines provided are a general guideline for disabling all medium strength cipher suites in SSL.

SSL Certificate Signed Using Weak Hashing Algorithm

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Solution

Contact the Certificate Authority to have the certificate reissued.

Affected Systems

443 / tcp 140.98.202.240,140.98.202.189,140.98.202.13,140.98.202.4, 140.98.202.244, 140.98.202.16, 140.98.202.40, 140.98.202.173, 140.98.202.197

Output

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             :
C=US/ST=WA/L=Seattle/O=MyCompany/OU=IT/CN=localhost.localdomain/E=root@localhost.localdomain
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 11 02:44:12 2014 GMT
|-Valid To            : Sep 08 02:44:12 2024 GMT
```

The root CA must be configured to sign certificates with SHA-2 or higher, then re-issue the certificates. In case the certificate is provided by a 3rd party, the configuration process needs to be done by the provider, and they must re-issue the certificates to the organization.

Low Risk Level Vulnerability

The low level vulnerabilities are related to the weak cipher suites such as RC4, RSA and also related to errors in SSL certificates.

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 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 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 "Low" based on the "Risk Score" of 19%.

In the **email simulation** 44 of the different file types, holding a malicious-payload within, were able to penetrate your security measures (See "Files detected as ALLOWED"). 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.

A very important detail that can be observed in the Summary shown above is that the highest percentage penetration for the **email vector** this month comes from links at 77%. Links refers to links contained in emails, used in phishing and spear-phishing attacks, modern phishing, called spear-phishing attacks, are targeted at a particular organization after gathering information of said organization to make it look as valid as possible or spoofing the sender domain to make them look they come from a real company. This medium risk factor indicates that your organization is very vulnerable via e-mail to these types of attacks. It is difficult to completely remove this threat vector, but some techniques that help reduce the number of attacks received through this vector are anti-spam filters, anti-phishing solutions with the capability of checking for domain spoofing and implementing DMARC framework to be able to stop any suspicious email from reaching the mail server; personnel training is also advised, there are platforms both free and paid that allow the organization to forge phishing campaigns for internal simulations and tests.

Mail Attack Summary

Within the set of threats that can penetrate via email, exists a high percentage of penetration in critical threats mainly Exploits, followed by Ransomware. For our analysts the Risk Score for your organization is of level Low. It has to be clear that only the e-mail vector was used for this proof of concept, but 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 you infrastructure.

Risk conditions based in test MSS-BAS e-mail vector. May 2018
E-mail Security Exposure Level: Low
Risk Score: 19%

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

Least Vulnerable To:

ransomware

*i.e: WannaCry, Petya.

Most Vulnerable To:

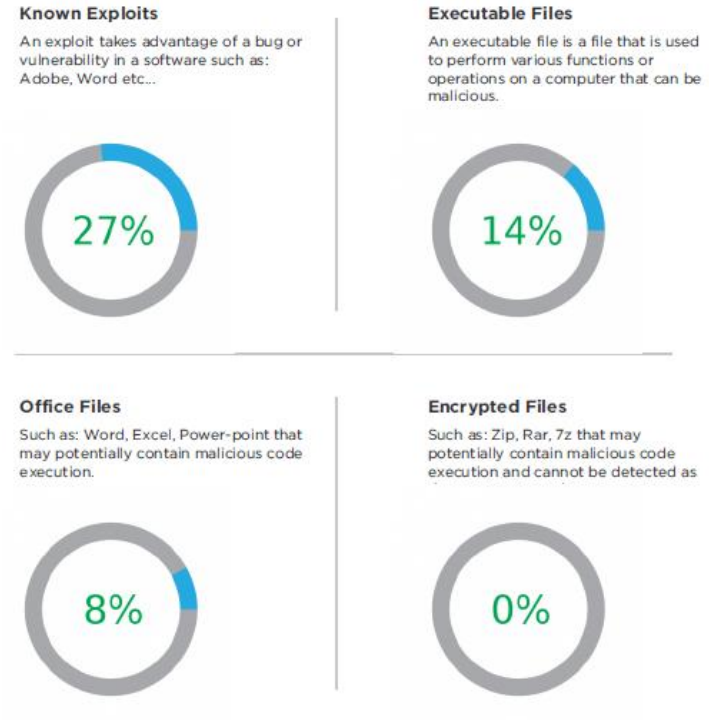
links

MSS-BAS e-mail vector Simulation Summary 918/4272

Risk Level	*Sent*	*Penetrated*
High	555	28
Medium	1324	713
Low	2396	177

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

.mp3	.gz	.tar	.one	.csv	.pub	.7z	.rar	.rtf	.mcl	.lha	.arj	.lzh	.dot
.accdb	.pptx	.pwz	.sldx	.ppam	.dotm	.ics	.pptm	.htm	.mdb	.doc	.xlm	.ppt	.xlsb
.xls	.xlam	.slk	.msg	.wav	.xlsx	.pdf	.svg	.vcs	.oft	.docx	.xsl	.zip	.eml
.html	.xhtml												

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

File types detected by GLESEC as BLOCKED

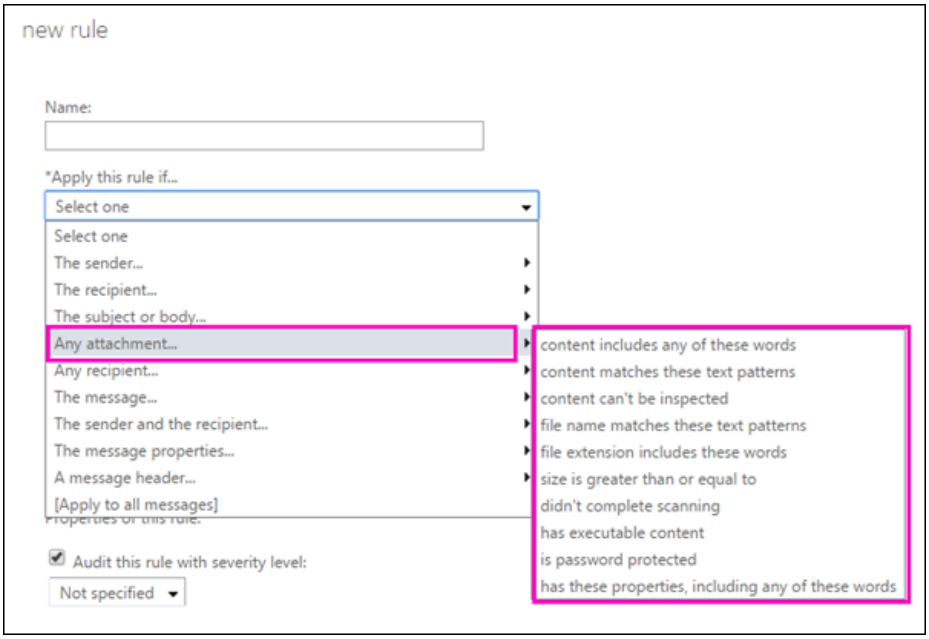
.jar	.msi	.chm	.UUE	.cab	.odt	.ods	.wbk	.pps	.docm	.xltm	.ppa	.sldm	.xml
.pot	.xlk	.xlsm	.xlw	.xlt	.xll	.potm	.ppsm	.xla	.vbs	.scr	.jse	.pif	.hta
.bat	.wsf	.vbe	.js	.exe	.com	.cmd	.lnk						

Remediation 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.

The following recommendations are valid for on-premise email servers. Hosted email servers configurations must be done by provider.

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 matches 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, based in rules, 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 depends on the OS that is running the mail server.

The integration of SpamAssassin and ClamAV into Postfix vary depending on the Linux distro.

For ClamAV in Ubuntu:

1. Open a terminal

2. Write the following command: *sudo apt-get install clamav clamav-freshclam clamsmtp.*

3. Accept the installation of any dependency requested.
After the installation is complete, the daemon will be already running and there are some additional configurations that must be done.

- Change the ports defined in /etc/clamsmtpf.conf to the ports used by Postfix.
- In postfix, add the following lines to the /etc/main.cf:

content_filter = scan:127.0.0.1:10025
receive_override_options = no_address_mappings

In the /etc/postfix/master.cf file add the following lines at the end of the file:

AV scan filter (used by content_filter)
scan unix - - n - 16 smtp
smtp_send_xforward_command=yes
# For injecting mail back into postfix from the filter
127.0.0.1:10026 inet n - n - 16 smtpd

- content_filter=
- receive_override_options=no_unknown_recipient_checks,no_header_body_checks
- smtpd_helo_restrictions=
- smtpd_client_restrictions=
- smtpd_sender_restrictions=
- smtpd_recipient_restrictions=permit_mynetworks,reject

- mynetworks_style=host
- smtpd_authorized_xforward_hosts=127.0.0.0/8

To configure automatic updates:

- Open a terminal, write the command sudo crontab -e
- Add the following line 00 1 * * * /usr/bin/freshclam –quiet. (Adjust the hour to an hour that is adequate to the needs of the organization).

For SpamAssassin in Ubuntu:

- Open a terminal, execute apt-get install spamassassin spamc
- Create a user for Spamassasin with adduser spamd --disabled-login
- In Postfix you have to define the content filter to use, this can be done in /etc/postfix/master.cf adding the following lines:

```
smtp      inet  n       -       -       -       -       smtpd
 content_filter=spamassassin
spamassassin unix -     n       n       -       -       pipe
 user=spamd argv=/usr/bin/spamc -f -e
/usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

For this change to take effect, Postfix has to be restarted with:

```
systemctl restart postfix.service
systemctl enable spamassassin.service
systemctl start spamassassin.service
```

Additional configurations regarding Spam filters can be requested to GLESEC Personnel.

Additional countermeasures that minimize malware penetration

For file extensions that are part of the permitted list there are two approaches to take:

- A restrictive approach that could greatly reduce the malware penetrations in the mail vector is a Content Disarm and Reconstruction (CDR) solution to examine the mails before delivering it to their destination.
  This type of solution usually correctly identify the file type without relying on the file extension, deconstruct the file in several components to then remove any unneeded data and rebuild the file again without any loss in functionality and keeps the original final in quarantine, delivering the sanitized file to its

destination.

- A less restrictive approach is the use of a software with the capability to detect and analyze the behaviors and actions taken by the files in a detailed fashion allowing to identify from which file or process the action was originated with timestamp, actions taken, directories affected then report the events, allowing further analysis to be done before taking action, but with the capability to take immediate action if necessary.

Successful High level simulated attacks

High risk files able to penetrate the perimeter were Worm, Ransomware. This specific type of ransomware was categorized as a high risk, because the number of clicks required to execute it are considerably low.
Malicious code can be hidden within different other file types so that it is not recognized and stopped by regular security countermeasures. The malicious Ransomware was hidden within different file types:

•HTM: An HTM file is an HTML web page used by web browsers. It contains markup code that is stored a plain text format and is used to display and format text and images in a web browser.
•ACCDB: An ACCDB file is a database created with Microsoft Access 2007 or later. It typically contains data organized into tables and fields.
•MDB: An MDB file is a database file created by Microsoft Access. It contains the database structure (tables and fields) and database entries (table rows).
•ICS: this extension refers to calendar application files, most common apps that use this type of files are: Microsoft Outlook, IBM Lotus Notes, Apple Calendar, Yahoo! Calendar, among others.
•XLS: An XLS file is a spreadsheet file created by Microsoft Excel. An XLS spreadsheet may contain one or more worksheets, which store and display data in a table format.
•XLM: Contains macros used for automating processes in Microsoft Excel.
•DOTM: A DOTM file is a document template created by Microsoft Word. It contains the default layout, settings, and macros for a document.
•PDF: A PDF file is a multi-platform document created PDF application. The PDF format is commonly used for saving documents and publications in a standard format that can be viewed on multiple platforms.
•XLAM: File used by Microsoft Excel, contains a macro-enabled add-in, which

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

provides extra functionality and tools that may execute macros.
•XLSM: An XLSM file is a macro-enabled spreadsheet created by Microsoft Excel. It contains worksheets of cells arranged by rows and columns as well as embedded macros programmed in the VBA language.
•VCS: Contains information about an event or appointment, saved in the vCalendar format; includes the event date and time and other information about the event.
•XLK: Backup file created by Microsoft Excel; contains a backup copy of an .XLS file.
•XLT: An XLT file is a template created by Microsoft Excel. It contains default formatting and data for a spreadsheet and is used as a basis for creating new .XLS files.
•HTML: This is the standard web page file type on the internet. The content of this type of files is accessible through any web browser.
•XLTM: Template file created by Microsoft Excel, contains default settings and layout properties for a macro-enabled spreadsheet; used to create a new macro-Enabled workbook .XLSM file.
•7z: A 7Z file is a compressed archive created with Igor Pavlov's 7-Zip file compression utility.
•EML: An EML file is an email message saved by Microsoft Outlook or other e-mail programs. It may also contain an e-mail attachment, which is a file sent with the message.
•XLL: A special type of file similar to the DLL libraries but exclusively used by Excel.
•SVG: An SVG file is a graphics file that uses a two-dimensional vector graphic format. It describes images using a text format that is based on XML.

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

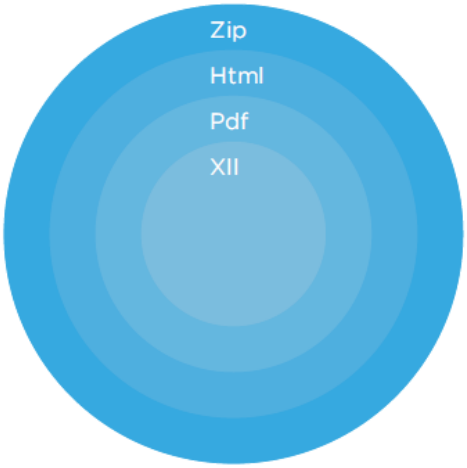
Even though all the other tested threats: Payload, Worms, Links, Malware, Exploits and Dummy were able to penetrate the perimeter, we consider Ransomware alone as the highest risk due to its probability of occurrence and possible negative impact.
Successful Low level simulated attacks.

Comments

Malware that uses Office documents as infection method commonly use macro files to execute the payload. Another method that is becoming more common, as seen by the malware that exploits CVE-2017-0199, consists in making winword.exe, or

any program of the Office suite, issue an HTTP request to a remote server to retrieve a file that contains the malware script; in this method the user is presented with a decoy document instead of a macro file to trick the end-user that is a legitimate document.

This method of leveraging documents to retrieve the payload itself instead of directly embedding in the document makes standard AV protection unable to detect anything malicious in the email attachment, until the payload is being downloaded in the victim's computer.
A graphical representation for demonstration of how the malware interacts with multiple file types is showed in the example below, the payload itself is contained in the XLL file, that is requested by a hyperlink in the PDF file, which in turn is hosted in a webpage, the user receives in his email a zip file with a link pointing to said webpage:



Web Gateway Attack Summary

During this month, the BAS-Browser vector has not been executed, this has been notified to personnel of your organization, for us is very important to run the simulated attacks because this can help to improve the security posture of your organization and prevent incidents.

WAF Attack Summary

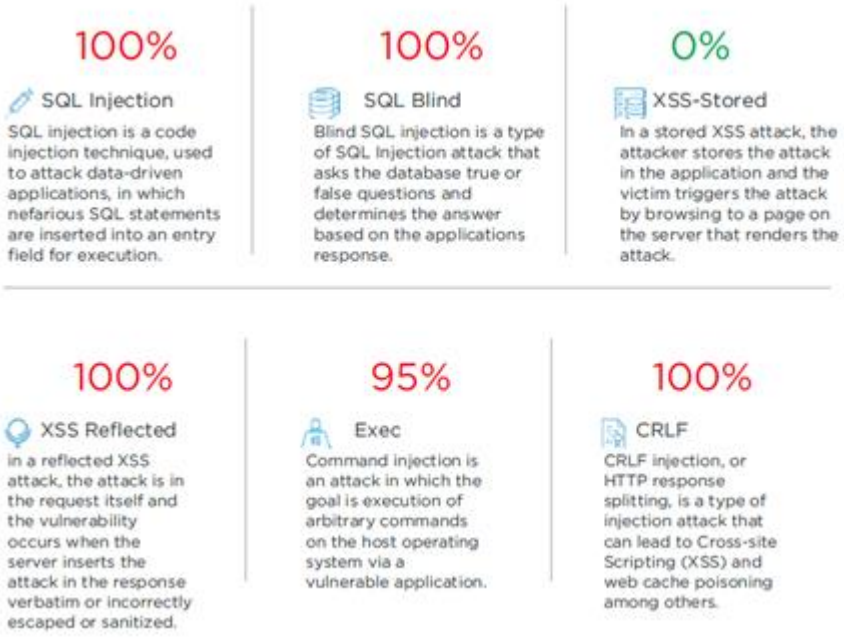
For this month's simulations, the risk score of your organization is considered **high risk**. This situation is of concern and should be addressed as soon as possible; however the fact that the successful simulations percentage was very close to 100%, and with the information we have, could point that there is no countermeasure in place to defend against this vector. The risk score for this month is 99 %, which is considered a high-risk level.

The following table summarizes the successful penetrations by risk level, the table shows clearly that all but two high risk level payloads were able to bypass the security measures in place (see down below, first row) and all others, medium and low risk payloads bypassed the WAF security policies.

Simulation Summary: 332/334

Risk Level	Sent	Penetrated
High	54	52
Medium	112	112
Low	168	168

Assessment Result



The samples used are classified in the categories showed above, along with their successful entries to their target. It is worth noting that there is a 0% percent in the XSS-Stored category, this means that at the very least, the countermeasures tested, scans for fragments of code when a user enters data through the input boxes or forms and sanitize the input data if it finds anything anomalous.

Observations

This report made to an URL of your organization determined that 99% 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: ieee.org is being protected with the Web Application Firewall, WAF.

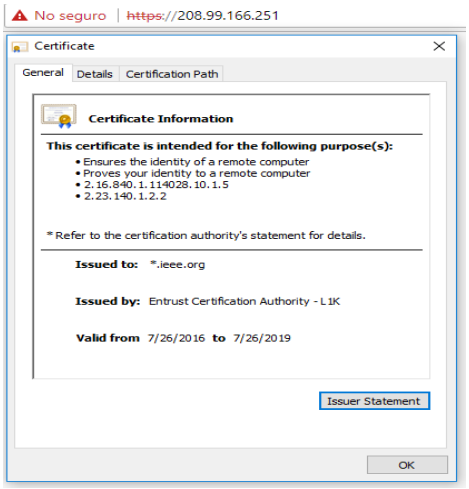
Whole Compiled Recommendations

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.

1. Many of the critical vulnerabilities found in your system are present in outdated versions of Apache, PHP, Oracle, and can be remedied by updating the software to the latest version, and to continue to receive security updates.

2. For the vulnerability named Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure, Upgrade to a patched version of the software. Alternatively, disable RSA key exchanges and enable ECC instead (Elliptic Curve Diffie Hellman).

3. For the vulnerability related to SSL certificates that cannot be trusted. In these particular cases, since the tests were done using the IP address of the hosts, the name that comes in the certificate do not match with the IP. This in itself does not represent vulnerability. To remove the message, define the IP address of the hosts as Subject Alternative Name field in the certificate.



Further investigations on this IP 208.99.166.247 that also presented the SSL certificate error, redirected to the following webpage: https://webservices.ieee.org/bms/services_update.html

4. The service MSS-BAS 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:

.mp3	.gz	.tar	.one	.csv	.pub	.7z	.rar	.rtf	.mcl	.lha	.arj	.lzh	.dot
.accdb	.pptx	.pwz	.sldx	.ppam	.dotm	.ics	.pptm	.htm	.mdb	.doc	.xlm	.ppt	.xlsb
.xls	.xlam	.slk	.msg	.wav	.xlsx	.pdf	.svg	.vcs	.oft	.docx	.xsl	.zip	.eml
.html	.xhtml												

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.

5. For the MSS-BAS WAF vector, we suggest if you could provide us with additional details about how your organization protects their websites, since the tests we ran, show different non-conclusive scenarios.

Appendix A

There is extensive amount of more detail that can be provided upon request.

GLESEC
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