MONTHLY OPERATIONS & INTELLIGENCE REPORT

TECHNICAL REPORT

Metrobank S.A.

May 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

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 range of addresses given by Metrobank S.A., we have found a total of 13 hosts, of which 11 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. In addition, you can observe the risk value score of your organization according to our metrics, there was as increase compared to last month, this is due to the fact that a critical host was found in their systems. This was reported to your organization.

Total IP's Scanned	IP's Vulnerable
13	11

Risk Distribution				
Critical	High	Medium	Low	Total
1	0	38	15	54

According to the metrics:

RV= 0.336894587

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

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

Category	Critical	High	Medium	Low	Total
General	0		30	7	37
Misc.	0		3	7	10
Service detection	0		3	0	3
Windows	1		2	0	3
Web Servers	0		0	1	1

- General (68.51%).
- Misc (18.51%).
- Services Detection (5.6%).

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

- Windows (68.5%).
- Web Server (1.8%).

Additional details about these vulnerabilities are presented in the Vulnerabilities found in METROBANK by severity section of the MSS-VM on page 7.

The total number of vulnerabilities for Metrobank in this period was 54. It was discovered that 11 of the 13 hosts analyzed have at least one problem of vulnerability, 1 critical risk, 38 with medium risk and 15 with low risk.

Most hosts are vulnerable support the use of SSL encryption that offers medium intensity encryption, other vulnerabilities were SSLv3 Padding Oracle in degraded inherited vulnerabilities (POODLE) and RC4 SSL encryption suites (Bar Mitzvah).

The 5 ports considered most vulnerable for this period were 443, 8089, 3389, 9443 and 25. This is due to the fact that many vulnerabilities were found that are related to them and are classified at a medium severity level.

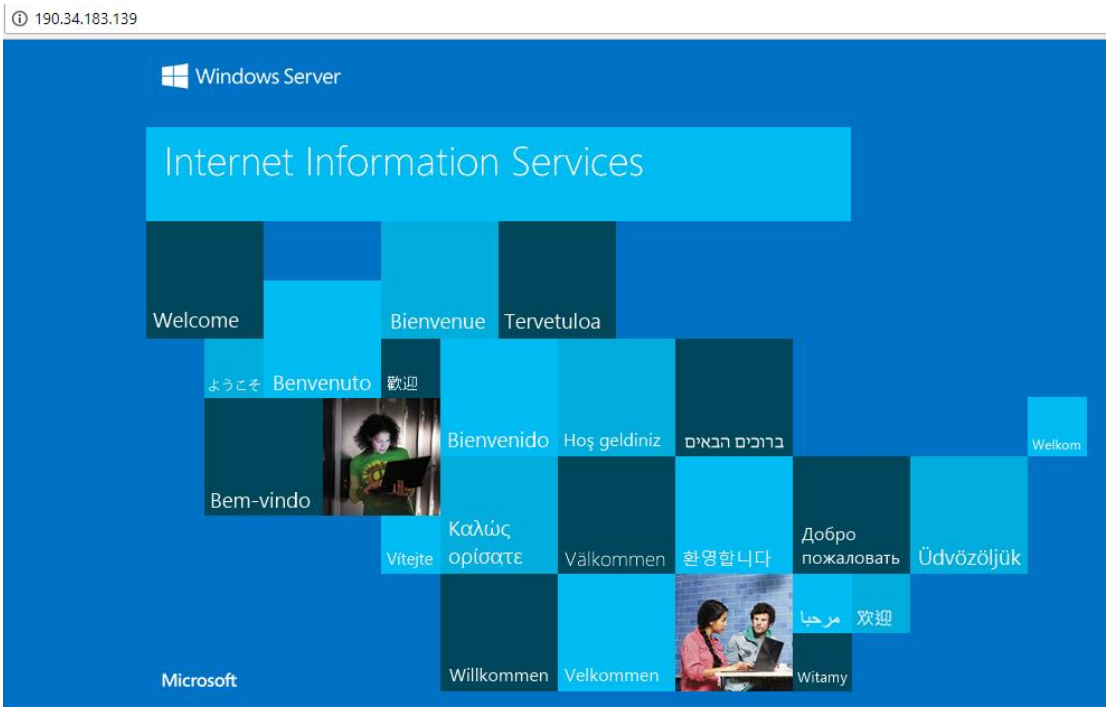
The hosts 190.34.183.139 (26.4%) and 190.34.183.142 (20.8%) have the greatest vulnerabilities between the categories (General, Misc and Windows).
These same vulnerabilities have been reported in previous periods.

Descriptions by Host

The remote host http://190.34.183.139/ is affected the action of Fingerprinting.
This vulnerability is known OS Fingerprinting is a technique that involves analyzing the footprints left by an operating system in its network connections. It is based on the response times to the different packages, to establish a connection in the TCP / IP protocol, which is used by the different operating systems. We recommend applying more security to your servers

We attach the image, showing the stated above.

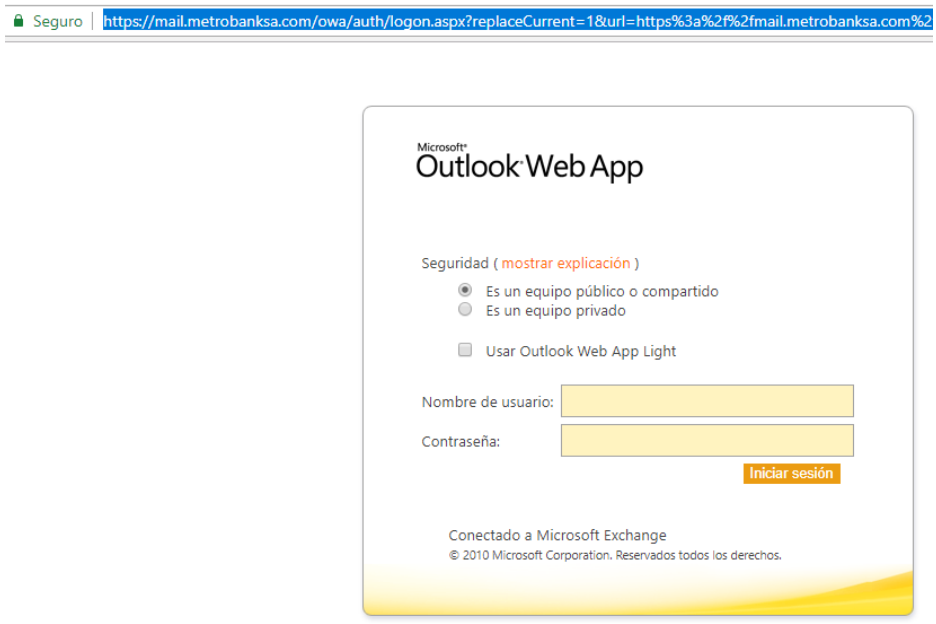
GLESEC
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



The remote host 190.34.183.131 is affected vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553), which affects Windows systems; we recommend applying all the security updates suggested by Windows, especially MS15-034 (KB 3042553), since all of these give solution to vulnerabilities found in this type of system.

Other vulnerabilities were SSLv3 Padding Oracle in degraded inherited vulnerability (POODLE) and RC4 SSL encryption suites (Bar Mitzvah) in 3 different servers:
https://mail.metrobanksa.com/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.metrobanksa.com%2fowa%2f(190.34.149),
https://www.metrobanksa.com/metrobank/es (190.34.184.152),
including the main web portal of Metrobank S.A and the Outlook web application.

We attach the image, showing the stated above



Vulnerabilities by severity

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

Critical Risk Level Vulnerabilities

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution

Description
The version of Windows running on the remote host is affected by an integer overflow condition in the HTTP protocol stack (HTTP.sys) due to improper parsing of crafted HTTP requests. An unauthenticated, remote attacker can exploit this to execute arbitrary code with System privileges.

Solution
Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2

Affected Systems
80 / tcp / possible_wls 190.34.183.131

443 / tcp / possible_wls 190.34.183.131

Output

```
HTTP response status: HTTP/1.1 301 Moved Permanently
```

```
HTTP response status: HTTP/1.1 200 OK
```

Medium Risk Level Vulnerabilities

SSL Medium Strength Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. GLESEC regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

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

Solution

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

Affected Systems

9443 / tcp / possible_wls 190.34.183.139
25 / tcp / smtp 190.34.183.148
8089 / tcp / possible_wls 190.34.183.139
443 / tcp / possible_wls 190.34.183.90,190.34.183.91,190.34.183.132, 190.34.183.139, 190.34.183.142, 190.34.183.149, 190.34.183.152

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)

    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}
```

SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

1. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

2. Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

3. Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

4. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Affected Systems

25 / tcp / smtp 190.34.183.148

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=PA/ST=Panama/L=Panama/OU=Metrobank/O=Metrobank, S.A./CN=correo.metrobanksa.com
|-Issuer  : C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - SHA256 - G2
```

Affected Systems

443 / tcp / possible_wls 190.34.183.154

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : 2.5.4.15=Private
Organization/2.5.4.5=1991/1.3.6.1.4.1.311.60.2.1.3=PA/C=PA/ST=Panama/L=Panama/2.5.4.9=Ground
Floor, Metrobank Tower/OU=Metrobank/O=Metrobank, S.A./CN=metronet.metrobanksa.com
|-Issuer  : C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3
```

Affected Systems

443 / tcp / possible_wls 190.34.183.142

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=PA/CN=190.34.183.142/O=Glesec Panama, S.A./OU=Radware Web Management
|-Issuer  : C=PA/CN=190.34.183.142/O=Glesec Panama, S.A./OU=Radware Web Management
```

Affected Systems

443 / tcp / possible_wls 190.34.183.90190.34.183.91190.34.183.132

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=fwmetro..5afb7i
|-Issuer  : O=fwmetro..5afb7i
```

Affected Systems

3389 / tcp / msrdp 190.34.183.139

8443 / tcp / possible_wls 190.34.183.139

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=AppServer.metrobank.local
|-Issuer  : CN=AppServer.metrobank.local
```

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=PA/ST=Panama/L=Panama/OU=Metrobank/O=Metrobank, S.A./CN=appserver.metrobanksa.com
|-Issuer  : C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - SHA256 - G2
```

SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

1. An insecure padding scheme with CBC ciphers.

2. Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support

nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Affected Systems

9443 / tcp / possible_wls	190.34.183.139
8089 / tcp / possible_wls	190.34.183.139
443 / tcp / possible_wls	190.34.183.139190.34.183.142190.34.183.149

Output

```
- SSLv3 is enabled and the server supports at least one cipher.
```

Transport Layer Security (TLS) Protocol CRIME Vulnerability

Description
The remote service has one of two configurations that are known to be required for the CRIME attack :

- SSL / TLS compression is enabled.

- TLS advertises the SPDY protocol earlier than version 4.

Solution
Disable compression and / or the SPDY service.

Affected Systems

8089 / tcp / possible_wls	190.34.183.139

Output

```
The following configuration indicates that the remote service
may be vulnerable to the CRIME attack :

  - SSL / TLS compression is enabled.
```

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Note: Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Solution

Disable SSLv3.

Affected Systems

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

9443 / tcp / possible_wls 190.34.183.139
443 / tcp / possible_wls 190.34.183.139,190.34.183.142,190.34.183.149

Output

```
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

Microsoft Exchange Client Access Server Information Disclosure

Description

The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.

Affected Systems

443 / tcp / possible_wls 190.34.183.149

Output

```
GET /autodiscover/autodiscover.xml HTTP/1.0
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which returned the following IP address :

10.1.1.235
```

Low Risk Level Vulnerabilities

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Affected Systems

9443 / tcp / possible_wls	190.34.183.139
443 / tcp / possible_wls	190.34.183.139,190.34.183.142,190.34.183.149

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

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

SSH Server CBC Mode Ciphers Enabled

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Affected Systems

22 / tcp / ssh 190.34.183.129, 190.34.183.142

Output

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
```

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  blowfish-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  blowfish-cbc
```


SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Affected Systems

9443 / tcp / possible_wls 190.34.183.139

443 / tcp / possible_wls 190.34.183.139, 190.34.183.154

Output

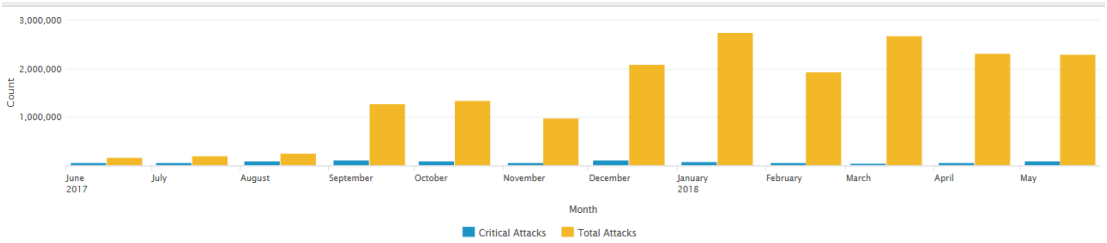
```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
```

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
less
```

THREATS

GLESEC uses its MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR and MSS-UTM to determine threat intelligence activity.

The threats reported by MSS-APS for this month are Anti-Scan, Access, DoS Behavior and Anomalies. All these threats were identified and discarded.



Based on the information collected from the security measures during this period, Metrobank S.A. received a total of: 2,299,931 attacks, of which 100,351 are critical, there was a decrease of 0.7% in the number of attacks received in this period in comparison with the previous month, with a response to critical attacks, there was a increase of 51%, all of these were stopped by the security countermeasures administered by GLESEC

Most attacks last less than a minute and are in the category Anti-scan and behavior-DoS, and attacks that last more than 1 hour include: access (violation of access to the blacklist), Anti-scanning (scanning TCP and horizontal scan TCP) and anomalies.

Most of the attacks are carried out from the following countries: Panama, Russian Federation, the United States, Chile and China; These are mainly aimed at ports: 8545 is intended for scans very frequently; if it is not necessary to leave it open, it would be advisable to close it or filter it from the traffic from the outside, the web access port (8080), 3389 (RDP) and SSH connection port (22).

Most attacks seem to be recognition (scanning). Approximately 91% of this month's attacks came from scanning, which can be considered recognition and is what you prefer for future attacks.

The attacks that consume the most amount of bandwidth are the attacks of B-DoS,

Anti-Exploration, Access, Anomalies and Intrusions.

For host 190.34.183.142, specific "flood IPv4 UDP" attacks of the category Behavioral DoS considered high risk, as well as attacks by Intrusions, Server Cracking (Wen Scan), HttpFlood (http page flood attack), have been launched. of the United States, Russian Federation, Canada.
The critical host discovered is 190.34.183.131 from its web portal Govimar https://190.34.183.131/fuerza-govimar/fuerza-govimar.html , which can be viewed from the Internet.

The DefensePro assisted in preventing attacks directed at network and server level which were directed at well-known port numbers: 8545 (),8080 (http-alt), 3389(RDP), 22 (ssh), 1433 (ms-sql), 5060 (sip), 80 (http), 445 (https), 443 (https), in order of frequency for this report period.

Top 5 Source IPs (Local or public).

- 190.34.192.34
- 190.34.192.31
- 195.43.95.90
- 77.72.82.24
- 77.72.83.235

The most frequent types of attacks were TCP Scan horizontal and vertical mode.
The first two IPs comes from Panama and the last two IPs comes from Russia.

Top 10 Destination IPs (Local or public) targeted
In this section we present the Destination IPs from denied or dropped connections that were most recurrent during this period.

- 190.34.183.135
- 190.34.183.158
- 190.34.183.137
- 190.34.183.132
- 190.34.183.149

The DefensePro system has operated properly with 100.00% up time and good performance.

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

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

Info@glesec.com
www.glesec.com