OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

Metrobank S.A.

September, 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.

For this period and according to the range of addresses provided by Metrobank, the total number of hosts analyzed is 14, of which 7 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, it has decreased compared to last month. The critical vulnerability in host 190.34.183.131 continues to be reported to your organization.

Total IP's Scanned	IP's Vulnerable
15	10

Risk Distribution				
Critical	High	Medium	Low	Total
1	5	37	21	64

According to the metrics:
RV= 0.2640625

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	0	28	8	36
Misc.	0	0	7	9	16
Service detection	0	5	0	3	8
Windows	1	0	2	0	3
Web Servers	0	0	0	1	1

- General (56%).
- Misc (25%).
- Services Detection (12.5%).

Additional details about these vulnerabilities are presented in the Vulnerabilities found in Metrobank S.A by severity section of the MSS-VM on page 10.

Metrobank continues to present critical (2%), high (8%), medium (58%) and low (32%) vulnerabilities. For this month, the total number of vulnerabilities decreased to 37.

Main categories that have the most vulnerabilities:

- General (56%) presents mostly SSL-type vulnerabilities such as Medium Strength Cipher Suites Supported and SSL Certificate Cannot Be Trusted. These represent a medium level of severity.

- Misc. (16.2%) presents major vulnerabilities of type: SSH Server CBC Mode Ciphers Enabled, Logjam vulnerability represents a low level of severity and SSH Weak Algorithms Supported, SSL/TLS FREAK and DROWN vulnerabilities, Terminal Services doesn't use NLA and Encryption level is Medium or Low represents a medium severity level.

- Service Detection (8.10%) mainly presents the type vulnerability: SSL Version 2 and 3 Protocol Detection represent a high level of severity; and also presents SSL Anonymous Cipher Suites Supported which has a low level of severity.

- Windows (2.70%) its main vulnerability is MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check) represents a level of critical risk.

Of all the types of vulnerabilities mentioned above, the ones that are frequently presented are SSL Medium Strength Cipher Suites Supported (14%) and SSL Certificate Cannot Be Trusted (8%).

Among the vulnerabilities that present a level of critical and high severity we have:

- The HTTP.sys Vulnerability Allow Remote Code Execution (3042553) (uncredentialed check). There is a security update that is considered critical for all supported editions of Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1 and Windows Server 2012 R2. This vulnerability is still present on host 190.34.183.131.

- The SSL Version 2 and 3 Protocol Detection Vulnerability is considered to be of high severity and is presented on hosts 190.34.183.142, 190.34.183.139, 190.34.183.154 and 190.34.183.152.

The 4 ports considered most vulnerable for this period were 443 (HTTPS), 3389(RDP) and 22 (SSH) and 80 (HTTP). This is due to the fact that many vulnerabilities related to them were found and the majority is classified at a medium severity level, except port 80 that has a critical severity level.

Below are the most vulnerable hosts for these ports:

- 443 (HTTPS) Most of the hosts are vulnerable by this port, among them we have: 190.34.183.139, 190.34.183.142, 190.34.183.152, 190.34.183.154.

- 22 (SSH) vulnerabilities presented by this port are: SSH Weak Algorithms Supported, SSH Server CBC Mode Ciphers Enabled and SSH Weak MAC Algorithms Enabled. The host affected is 190.34.183.142.

- 3389 (RDP) vulnerabilities presented by this port are: Microsoft Windows Remote Desktop Protocol Server Man-in-the-middle Weakness, Terminal Services doesn't user NLA Only, Terminal Services Encryption Level is Medium or Low. The affected host is 190.34.183.139.

- 80 (HTTP) the host that presents vulnerability by this port is 190.34.183.131 and it's a critical vulnerability as mentioned before "HTTP.sys Vulnerability Allow Remote Code Execution (3042553) (uncredentialed check)".

The port that appears most frequently as vulnerable is 443.

There is a low percentage of vulnerability between the categories of Port Scanners

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

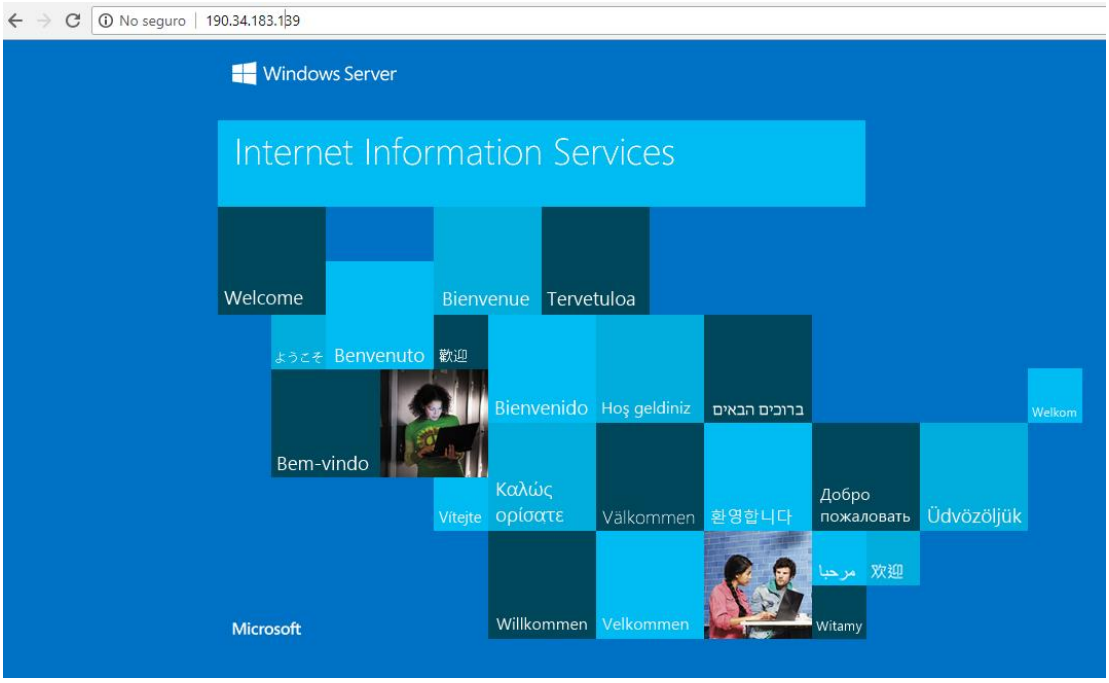
and Firewalls (Chek Point) that present an " informational" level of severity, at ports 18264, 264 and 500 (hosts: 190.34.183.132, 190.34.183.91 and 190.34.183.90).

The most vulnerable hosts are: 190.34.183.139, 190.34.183.142, 190.34.183.152 and 190.34.183.154; most are of medium and low severity.

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.
Another vulnerability that it presents is: Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness. This is based on the fact that a remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle attack (MiTM). The RDP client does not endeavor to validate the identity of the server when configuring the encryption. An attacker with the ability to intercept RDP server traffic can establish encryption with the client and the server without being detected.

We attach the image, showing the stated above.



The remote host 190.34.183.131 (https://www.govimar.com.pa/) is affected vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553), which affects Windows systems (ports 80/443); We recommend to apply all the security updates suggested by Windows, especially MS15-034 (KB 3042553), since they all solve the vulnerabilities found in this type of system. The previous month this vulnerability was presented.

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
```

High Risk Level Vulnerabilities

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
443 / tcp / possible_wls 190.34.183.139, 190.34.183.149, 190.34.183.154, 190.34.183.152, 190.34.183.142
Output

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

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
8089 / tcp / possible_wls 190.34.183.139
443 / tcp / possible_wls 190.34.183.132, 190.34.183.139, 190.34.183.142, 190.34.183.149, 190.34.183.152, 190.34.183.154, 190.34.183.90, 190.34.183.91

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 190.34.183.142

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 190.34.183.90, 190.34.183.91, 190.34.183.132

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
```

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 / possible_wls 190.34.183.132, 190.34.183.142, 190.34.183.90, 190.34.183.91

SSL Self-Signed Certificate

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Affected hosts:

- 190.34.183.142
- 190.34.183.132

- 190.34.183.91
- 190.34.193.90

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

443 / tcp / possible_wls 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.
```

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Affected systems

- 190.34.183.154
- 190.34.183.152
- 190.34.183.139

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

443 / tcp / possible_wls190.34.183.139,190.34.183.142,190.34.183.149, 190.34.183.152, 190.34.183.154

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

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
```

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

443 / tcp / possible_wls190.34.183.154, 190.34.183.152, 190.34.183.139

Output

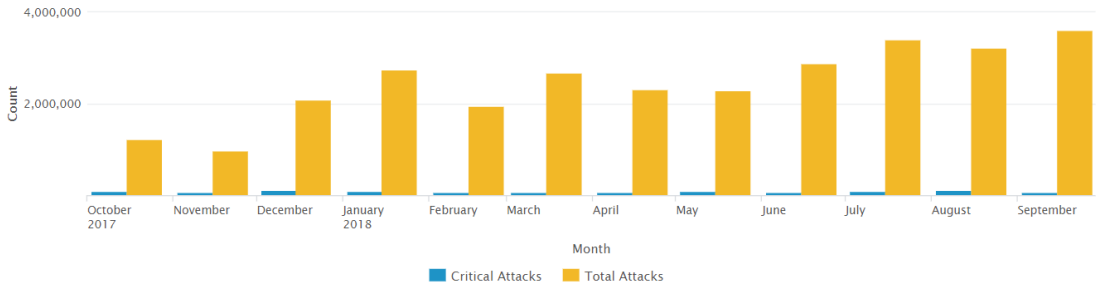
```
Vulnerable connection combinations :

  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)
```


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

THREATS

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

The Threats as reported by the MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR, MSS-UTM for this month are mostly anti-scan attacks. 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: 3,596,487 attacks, of which 51,427 are critical, there was an increase of 11% in the number of attacks received in this period compared to the month of August (Total attacks: 3,233,186), and a 58% decrease in critical attacks for this month compared to August (121,500 critical attacks). The critical attack that occurs most frequently for this month was Network Flood IPv4 UDP (67%) and belongs to the Behavorial-DoS category.

Here are some of the blocked attacks and the level of severity they represent:

- Network flood IPv4 UDP, Pattern flood Detected, SIP-Scanner-SIPVicious and Access denied due to malicious request are considered with a high level of severity.

- TCP Scan (horizontal), TCP Scan, UDP Scan (horizontal), UDP Scan, Ping Sweep and TCP Scan (vertical), are considered with a medium severity level.

- Threat List, handshake violation, first packet not SYN and Invalid IP Header or Total Length, they are considered with a low level of severity.

It has an "Informational" severity of type Anomaly-SSL-renegotiation-Cli that belongs to the Intrusions category on host 190.34.183.154 through port 443.

Between frequent and blocked attacks per week we have: TCP Scan (horizontal), TCP Scan, Threat List, Network flood IPv4 UDP, UDP Scan (horizontal), UDP Scan, SIP-Scanner-SIPVicious, Ping Sweep, TCP handshake violation, first packet not syn and Invalid IP Header or Total Length.
All this was stopped by the security countermeasures managed by GLESEC.

The duration that presents the most attacks are:

- Less than one minute are generated from the categories of Anti-Scanning, Behavioral-DoS and HttpFlood.
- More than one hour are generated from the Access, Anomalies and Anti-Scanning categories.

Among the 5 countries that frequent the highest number of attacks we can mention: Russian Federation (61%), Panama (11%), United States (11%), China (5.5%) and Germany (2.7%); These are mainly destined to the ports: 8545 is destined to explorations with a lot of frequency; if it is not necessary to leave it open, it would be advisable to close it or filter it from traffic from outside, 3389 (RDP: Microsoft Terminal Server) and the web access port (8080).

Most attacks seem to be recognition (scanning) lasting less than a minute and up to more than an hour. Approximately 95% of the attacks are scanning, which can be considered recognition and is utilized as setup for future attacks. The attacks that consume the most amount of bandwidth are the attacks of Behavorial-DoS, Anti-Scanning, Access, Anomalies and Intrusions.

In this period there was a low percentage of attacks in the categories:

- Cracking Protection (Web Scan) to the IP addresses 190.34.183.139, 190.34.183.149 and 190.34.183.153; (SMTP Scan) to the IP address 190.34.183.148.
- HttpFlood (Http Page Flood Attack) to the IP addresses 190.34.183.154 and

190.34.183.149.

- Intrusions (SQL-Inj-select3, SQL-Inj-select and SQL-Injection-All-Select) to the IP address 190.34.183.131, has already been reported to your organization.

DefensePro helped prevent attacks directed to the network and at the server level directed to known port numbers: 3389 (RDP), 23 (Telnet), 8080 and 81 (HTTP-Alternative), 5060 (SIP), 8545 (JSON-RPC), 443 (HTTPS), in order of frequency for this period.

Top 5 Source IPs (Local or public).

- 190.34.192.31
- 77.72.85.25
- 195.43.95.90
- 5.188.40.100
- 5.1822.40.99

The most frequent types of attacks were TCP Scan and TCP Scan (Horizontal).
The first IP address remains as the main attacker as in the previous month and comes from Panama, the second IP address comes from Bulgaria, and the three remaining IP addresses come from Russia.

Correlation between the MSS-APS and MSS-VME

In the following table we will describe which hosts are the most frequent targets if these attacks target specific vulnerabilities on these hosts.

Attack destination (MSS-APS/APFW)	Number of attacks	Vulnerabilities that are present (MSS-VME)
190.34.183.135	18,418	None
190.34.183.153	9,291	None
190.34.183.137	7,678	None

190.34.183.132	5,069	• SSL Certificate cannot be trusted • SSL Certificate Signed Using Weak Hashing Algorithm • SSL Medium Strength Cipher Suites supported
190.34.183.149	3,943	• SSL version 2 and 3 Protocol Detection • Microsoft Exchange Information Disclosure • SSL DROWN Attack • SSL POODLE Vulnerability • SSL Bar Mitzvah Vulnerability • SSL Medium Strength Cipher Suites supported

Analysis:

- Most of the attacks on host 190.34.183.132 were network Flood using UDP protocol, these attacks don't target any specific vulnerability however the rest of the attacks targeted multiple ports, among them port 80 (HTTP) and 443 (HTTPS), the vulnerabilities in this host can be exploited through port 443 causing the communications to be intercepted or decrypted by a malicious actor.

- Most of the attacks to host 190.34.183.149 are split between Web Scan, TCP handshake violation and TCP Scan (vertical).
  Web Scan refer to a tactic used to gather information about the server, automated tools are used to send different types of HTTP requests and analyzing the answers it obtains. These attacks target port 80 and 443 and many of the vulnerabilities present in this host can be exploited through these ports.
  TCP handshakes refer to traffic dropped due to a match with an ACL.
  TCP Scan (Vertical) refers to the practice of scanning multiple ports in a single host, this practice is used as a reconnaissance tactic to identify weak spots in hosts.

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