MONTHLY OPERATIONS & INTELLIGENCE REPORT

TECHNICAL REPORT

BANVIVIENDA

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 address range given by BANVIVIENDA, we have found a total of 15 hosts, of which 9 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
15	10

Risk Distribution				
Critical	High	Medium	Low	Total
0	0	30	9	39

According to the metrics:

RV= 0.271794872

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			24	8	32
Service detection			4	0	4
Misc.			1	1	2
Windows			1	0	1

- General
- Services detection
- Misc
- Windows

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

Additional details about these vulnerabilities are presented in the Vulnerabilities found in BANVIVIENDA by severity section of the MSS-VM **on page 12.**

Overall the vulnerabilities for BANVIVIENDA this period have been 30 medium and 9 low risk. All Medium risk vulnerabilities have already been reported in previous months. Here are some examples of the most relevant ones: SSL Medium Strength Cipher Suites Supported, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSL RC4 Cipher Suites Supported (Bar Mitzvah), and SSL Certificate Signed Using Weak Hashing Algorithm. The ideal scenario would be for all of these to be hardened, more information about these can be found in the intelligence section for the MSS-VM.

Ports 443 and 25 are the most vulnerable ports for this period; this is because many vulnerabilities were found which are related to the services listening on them and categorized as medium and low risk.

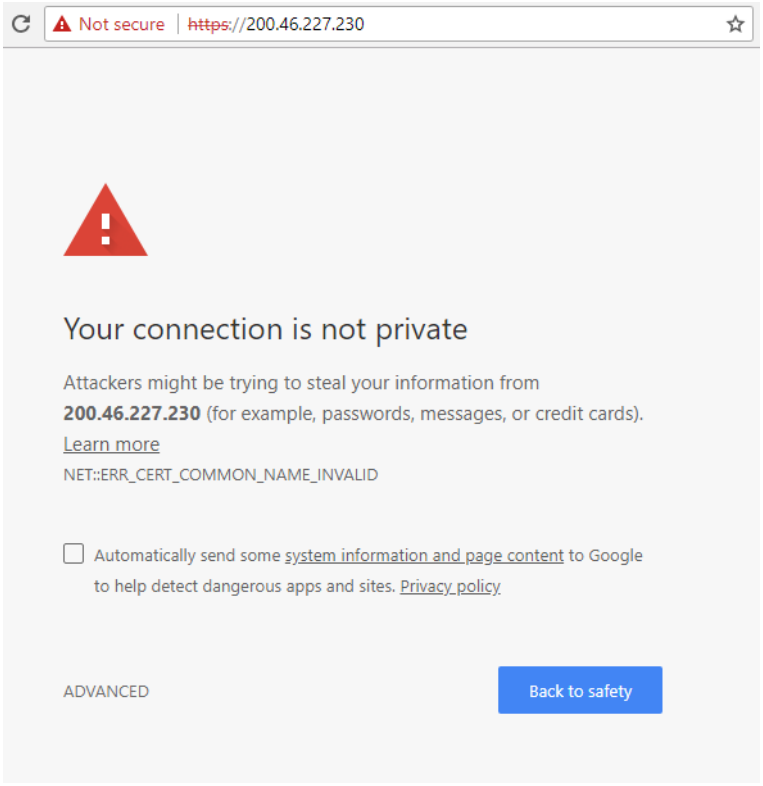
Description by Host

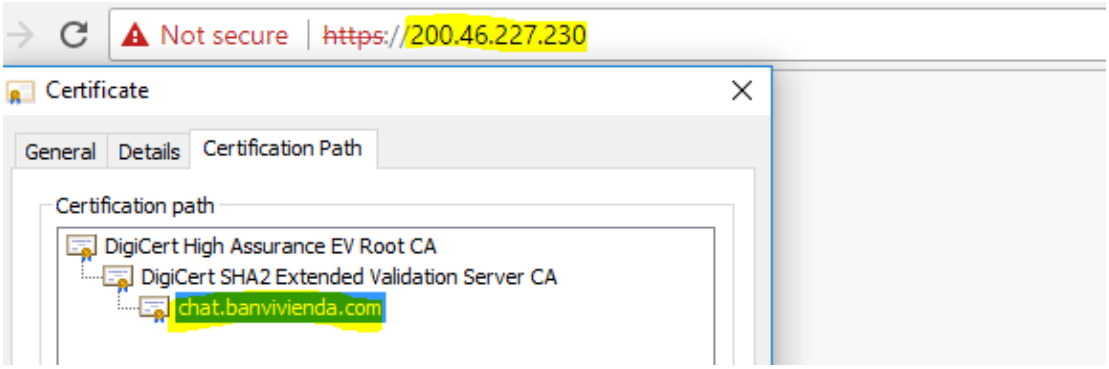
200.90.137.87
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSL Self-Signed Certificate, SSL Version 2 and 3 Protocol Detection, SSL Weak Cipher Suites Supported, OpenSSL AES-NI Padding Oracle MitM Information Disclosure, SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

200.90.137.89
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSL Self-Signed Certificate, SSL Version 2 and 3 Protocol Detection, SSL Weak Cipher Suites Supported, OpenSSL AES-NI Padding Oracle MitM Information Disclosure, SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

200.46.227.230

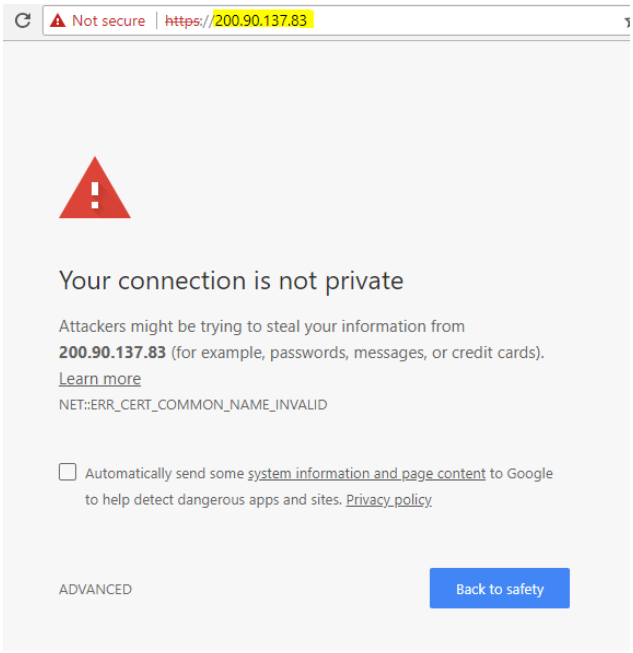
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Medium Strength Cipher Suites Supported, SSL Weak Cipher Suites Supported, SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK), SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

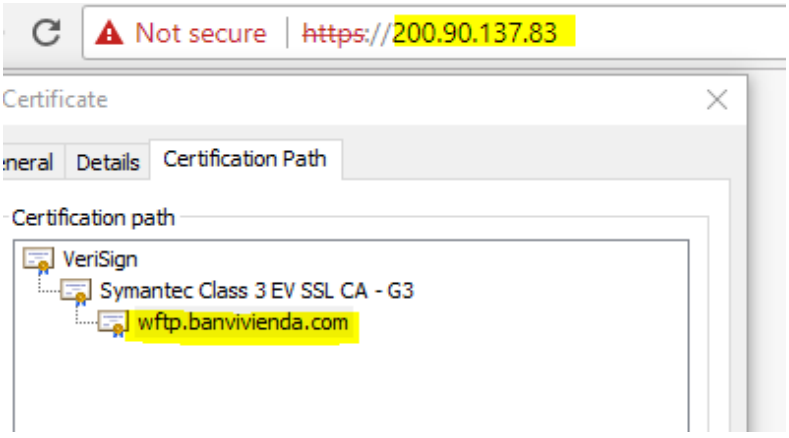




200.90.137.83

Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Medium Strength Cipher Suites Supported, SSL Version 2 and 3 Protocol Detection, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

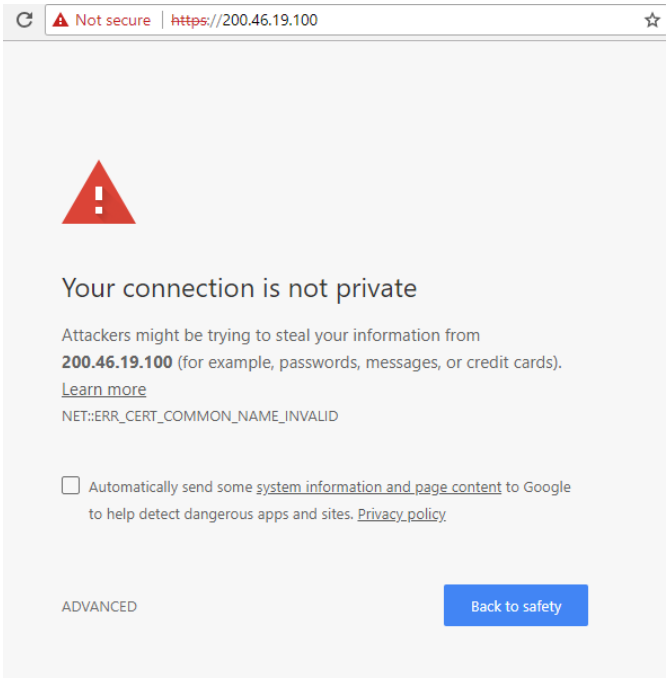


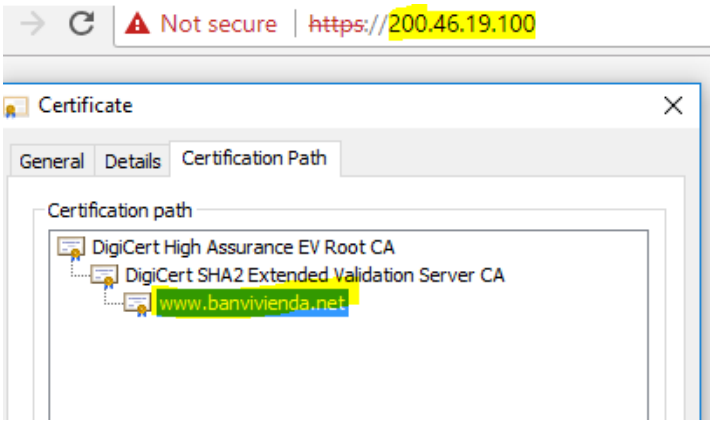


200.46.19.100

Several vulnerabilities found on this host are stated here:

SSL Version 2 and 3 Protocol Detection, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

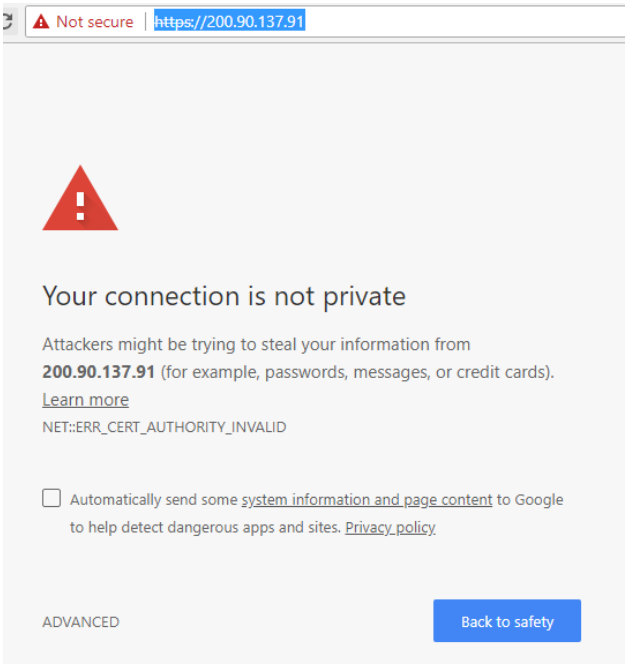


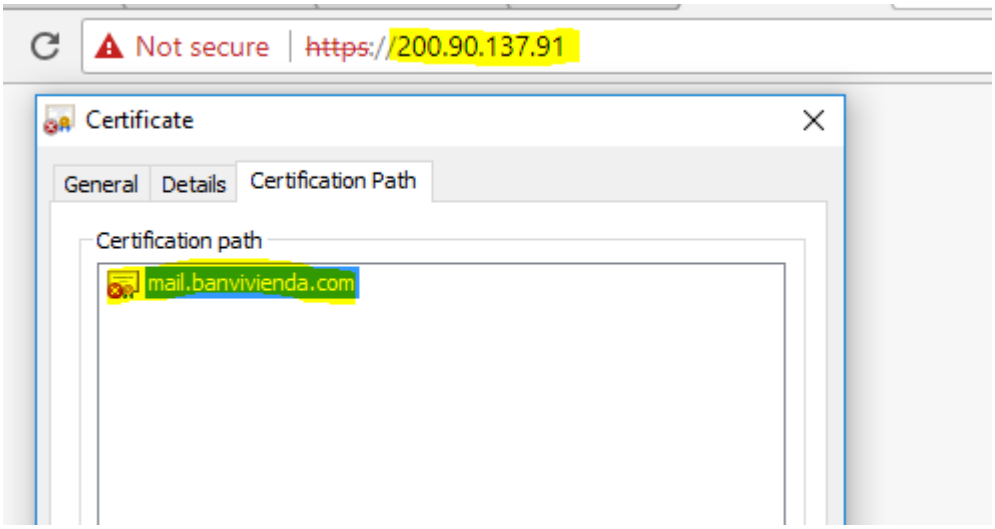


200.90.137.91

Several vulnerabilities found on this host are stated here:

SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Self-Signed Certificate. We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

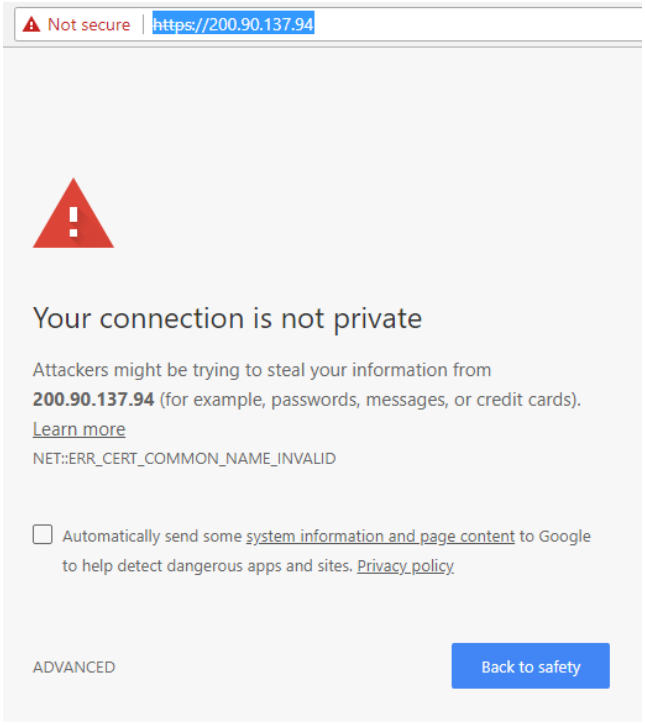


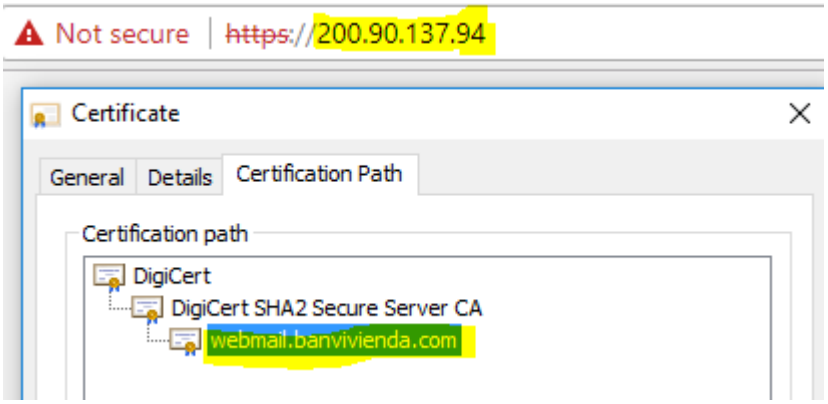


200.90.137.94

Several vulnerabilities found on this host are stated here:

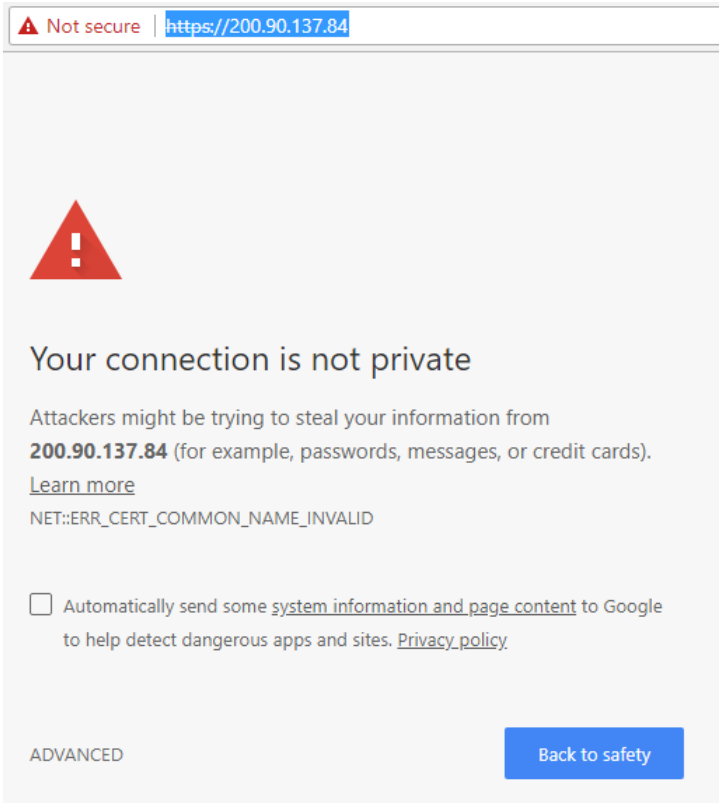
Microsoft Exchange Client Access Server Information Disclosure, SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

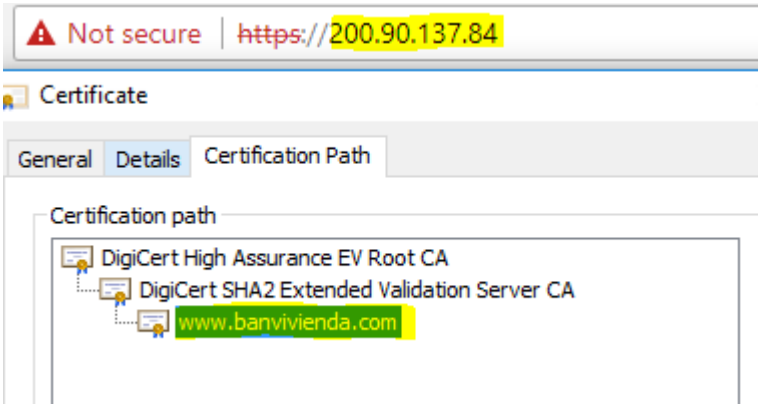




200.90.137.84

Several vulnerabilities found on this host are stated here:
SSL Medium Strength Cipher Suites Supported, SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.





200.46.19.98
During this month, GLESEC's operations center was able to discover only one vulnerability named "Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key". We recommend following the solution procedure for this issue, described in the Vulnerabilities by severity section of this document.

200.46.227.227
On this host, we were able to discover one vulnerability named "Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key". We recommend following the solution procedure for this issue, described in the Vulnerabilities by severity section of this document.

Vulnerabilities by severity

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

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
25 / tcp / smtp 200.90.137.87200.90.137.89
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
    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}
```

Affected Systems

443 / tcp / possible_wls 200.46.227.230, 200.46.227.230, 200.90.137.83, 200.90.137.83, 200.90.137.84, 200.90.137.84, 200.90.137.94, 200.90.137.94

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 200.90.137.87200.90.137.89

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=US/O=McAfee, Inc./OU=Email Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
|-Issuer  : C=US/O=McAfee, Inc./OU=Email Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
```

Affected Systems

443 / tcp / possible_wls 200.90.137.83,200.90.137.83

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 : 1.3.6.1.4.1.311.60.2.1.3=PA/2.5.4.15=Private
Organization/2.5.4.5=64474/C=PA/ST=Panama/L=Panama/O=Banco Panameno de la Vivienda
S.A./OU=IT/CN=wftp.banvivienda.com
|-Issuer  : C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA
- G3
```

Affected Systems

443 / tcp / possible_wls 200.46.227.230, 200.46.227.230

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/1.3.6.1.4.1.311.60.2.1.3=PA/2.5.4.5=64474/C=PA/ST=Panama/L=Panama City/O=Banco
Panameno de la Vivienda SA/OU=IT Department/CN=chat.banvivienda.com
|-Issuer  : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server
CA
```

Affected Systems

443 / tcp / possible_wls 200.90.137.91

10000 / tcp / possible_wls 200.90.137.91

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=mail.banvivienda.com/C=US/O=McAfee, Inc./OU=Email Gateway
|-Issuer  : CN=mail.banvivienda.com/C=US/O=McAfee, Inc./OU=Email Gateway
```

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
25 / tcp / smtp 200.90.137.87, 200.90.137.89
443 / tcp / possible_wls 200.46.19.100, 200.46.19.100,200.90.137.83, 200.90.137.83
Output

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

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
25 / tcp / smtp 200.90.137.87, 200.90.137.89
10000 / tcp / www 200.90.137.91

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/O=McAfee, Inc./OU=Email
Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Oct 10 22:51:42 2014 GMT
|-Valid To            : Oct 07 22:51:42 2024 GMT
```

Affected Systems

443 / tcp / possible_wls 200.90.137.91

10000 / tcp / possible_wls 200.90.137.91

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             : CN=mail.banvivienda.com/C=US/O=McAfee, Inc./OU=Email Gateway
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jun 15 18:52:06 2012 GMT
|-Valid To            : Jun 13 18:52:06 2022 GMT
```

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 / www 200.46.19.100, 200.46.19.100, 200.90.137.83
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 / www 200.90.137.94
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 :

10.100.201.119
```

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

443 / tcp / www 200.46.227.230, 200.46.227.230

Output

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

The fields above are :

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

Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

Description

The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.

Solution

1. Disable Aggressive Mode if supported.
2. Do not use Pre-Shared key for authentication if it's possible.
3. If using Pre-Shared key cannot be avoided, use very strong keys.
4. If possible, do not allow VPN connections from any IP addresses.

Note that this plugin does not run over IPv6.

Affected Systems

500 / udp / ikev1 200.46.227.227

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

25 / tcp / smtp 200.90.137.87, 200.90.137.89
443 / tcp / possible_wls 200.90.137.94

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}
```

Affected Systems

443 / tcp / possible_wls 200.46.19.100, 200.46.19.100,200.90.137.83, 200.90.137.83

Output

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

  Low Strength Ciphers (<= 64-bit key)

    EXP1024-RC4-SHA            Kx=RSA(1024)   Au=RSA      Enc=RC4(56)             Mac=SHA1
export
    EXP-RC4-MD5                Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

  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}
```

Affected Systems

443 / tcp / possible_wls 200.46.227.230

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

Output

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

  Low Strength Ciphers (<= 64-bit key)

    EXP1024-RC4-SHA             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)             Mac=SHA1
export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

  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}
```

OpenSSL AES-NI Padding Oracle MitM Information Disclosure

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256.

The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic.

Solution

Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.

Affected Systems

25 / tcp / smtp 200.90.137.87, 200.90.137.89

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_wls 200.90.137.84

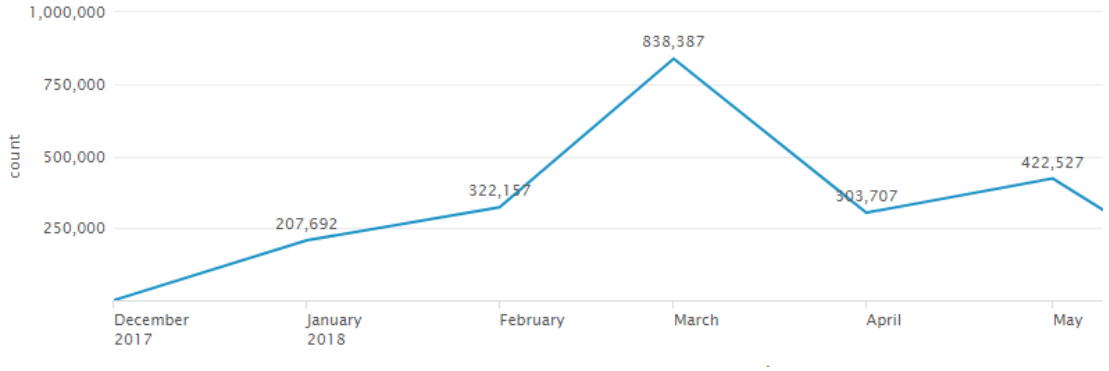
Output

```
Vulnerable connection combinations :

  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  : TLSv1.1
  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  : TLSv1.0
  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)

  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)
```

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 there are a total of 422,527 attacks denied by the rules of the firewall.



We have noticed an increase in attack activity of 39.12% from last month. We recommend BANVIVIENDA to review the activity of the devices where these events are registered.

Most of the attacks are targeting port 23(51,13%), followed by port 80(16,53%) and port 22(13.00%) these correspond to Telnet, HTTP and SSH respectively. About 51% of all attacks dropped are aiming the telnet port, something that slightly changed from the 62% in previous month. It is strongly advisable to, if opened, close this port (23) and switch all administration connections to SSHv2. The highest next count is HTTP with only a 16% of all attacked dropped, even if it does not seem like a big number it is very important to know it has been targeted.

The attacks are, for the most part, from the Russian Federation (19.4%), United States (21%) and the China (20.1%) as the three main sources. Most of these attack attempts were probing the services mentioned above.

Attack attempts blocked towards specific destination Port

In this section a list of ports that were targeted during the period, the first of the list was registered to receive the greatest number of attacks; it is sorted in a descending manner.

- 23 (Telnet)

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

- 80 (HTTP)
- 22 (SSH)
- 443 (HTTPS)
- 44046
- 12489
- 5666
- 445 (Microsoft-DS)
- 47545
- 1433(Ms-Sql-S)

Top 10 Source IPs (Local or public)

Private IP address appear in this section because the security countermeasures device has denied TCP connection to other Internal device, this can happen due to misconfigurations. The public IPs are highlighted for quicker recognition.

- 172.16.1.233
- 10.100.201.68
- **103.99.2.120**
- **200.46.161.233**
- **159.65.34.185**
- **222.73.254.215**
- 10.100.210.46
- **209.97.142.159**
- 10.100.210.31
- 10.100.201.107

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.

- 10.100.202.125
- **200.46.227.227**
- **200.46.19.98**
- 172.16.208.38
- 172.16.208.5
- 172.16.208.10
- 172.16.208.6
- 172.16.208.12
- 172.16.208.65
- 10.100.202.190

Managed End Point Incident Response Service (MSS-EIR)

The MSS-EIR is a preventive detection and response and a forensic service to identify without signatures and mitigate an attack to the end-points and servers of an organization. The service works by actively seeking malicious activity in the customer's network based on suspicious behaviors (not based on signatures). This technology allows our analysts to detect malicious software that may have evaded existing security countermeasures. At the same time we conduct investigations by responding to a security alert – this service is based on leveraging a powerful investigation platform to shorten the investigation time, respond to more incidents and get to the root cause of each incident.

During this month, our Operations Center was able to find several events that could be considered security events depending on whether or not BANVIVIENDA was aware they were happening. The agents that generated the greatest amount of alerts were BpvFtpSrvW12, BPVBLWB2 and BpvExch02. Within the most significant events found there were: Automatic updates, connections initiated from an application process to an external IP, Installation of several applications on agents, Executable dropped and self-delete, among others.

Three key concepts to take into consideration are entity, event and behavior; an entity is the most granular representation in the system. Entity types include: file, process, registry, IP address, socket and more. Event is an action that occurs between two entities. Event types: hooking, driver's changes, create file, read file, delete file, Windows service changes, New user, User Logon and more.
Behavior is an event or a collection of events that are more significant and identify a suspicious occurrence. In order to identify behaviors, the system analyzes the events collected over time using hybrid analytical methods that include expert-defined patterns and machine learning algorithms.

The next list of Events presents details about the agents they were found on, precise date of source process creation, MD5 of source file for validation, user it was executed with, execution path of the source file, process command line used and a brief description of every single one. These are considered the most relevant events during this month:

- **dbgview.exe**

MD5: baaca87fe5ac99e0f1442b54e03056f4
dbgview.exe->Driver added to registry->dbgv.sys
dbgview.exe->Executable path written to registry->dbgv.sys
Agent: BpvUltimusFE84
Date: 5/2/2018 3:32:38 PM
User: ultimus
Execution path: c:\software\debugview\
Process command line: "C:\SOFTWARE\DebugView\Dbgview.exe"
This process corresponds to Sysinternals Debug Output Viewer, it is an application that lets you monitor debug output on your local system, or any computer on the network that you can reach via TCP/IP. It is capable of displaying both kernel-mode and Win32 debug output, so you don't need a debugger to catch the debug output your applications or device drivers generate, nor do you need to modify your applications or drivers to use non-standard debug output APIs.

- **dopdf-full.exe**

MD5: 5852227cbc400a71f5b6a2fa252679be
dopdf-full.exe-> Network send-> 209.222.17.77 [tcp]:443
Agent: BpvExch01
Destino IP: 209.222.17.77
User: jorge.jarpa
Date: 5/7/2018 9:42:19 AM
Execution path: c:\users\jorge.jarpa\appdata\local\temp\
Process command line: "C:\Users\jorge.jarpa\AppData\Local\Temp\dopdf-full.exe"
Dopdf.exe is a type of EXE file associated with NovaPDF Printer developed by Softland for the Windows Operating System.

- **dopdf-full.exe**

MD5: ea0a8f2b9ac182e9e49028de14c345a1
dopdf-full.exe-> executable self delete-> dopdf-full.exe
dopdf-full.exe->executable dropped-> dopdf-full.exe
Agent: BpvExch01
User: jorge.jarpa
Date: 5/7/2018 9:43:04 AM
Execution path: c:\users\jorge.jarpa\appdata\local\temp\{b50a2d42-d55a-49ad-a7f0-8f90acb93e6d}\.be\
Process command line: "C:\Users\JORGE~1.JAR\AppData\Local\Temp\{B50A2D42-

D55A-49AD-A7F0-8F90ACB93E6D}\.be\novapdf.exe" -q -burn.elevated BurnPipe.{06AE090A-74D7-487A-9F07-FCC3D9DB5AD2} {C349421D-3AD2-4579-94D4-CE25A9EDAE49} 29076
doPDF is the simplified version of Softland's commercial NovaPDF, which offers additional features including Advanced Encryption Standard, password protection, digital signing, URL links support, text/images watermark, the ability to choose PDF version, etc. This executable does not cause any damage.

- **msmpeng.exe**

MD5: b9ad53d60da72c194f0aa2c89136fa35
msmpeng.exe -> Executable dropped -> mpengine.dll
msmpeng.exe -> Executable self delete -> mpengine.dll
msmpeng.exe -> Executable with abnormal extension-> mpasdlta.vdm
Date: 5/9/2018 9:16:02 PM
Execution path: c:\programdata\microsoft\windows defender\platform\4.14.17639.18041-0\
Process command line: "C:\ProgramData\Microsoft\Windows Defender\platform\4.14.17639.18041-0\MsMpEng.exe"
User: Local System
Msmpeng.exe is create by Windows Defender as Antimalware Engine Service. This is most likely to be seen while an antimalware scan is being run and at boot time. If Windows Defender is enabled, then this process will appear and most likely have this behavior as part of its regular function. This service is not Mandatory in any case so it can be disabled if the system counts with other malware protection tools.

- **ultimusstudio.exe**

MD5: b2ea22a272d82a12d1d8cf0265e39fca
ultimusstudio.exe-> Executable file written to registry-> ultimusstudio.exe
Agent: BpvUltimusFE
Date: 5/10/2018 5:45:06 PM
Execution path: c:\program files (x86)\ultimus bpm suite 7.3\
Process command line: "C:\Program Files (x86)\Ultimus BPM Suite 7.3\UltimusStudio.exe" ""
User: bpvsvradm
Registry Data: c:\progra~2\ultimu~1.3\ultimu~4.exe
Registry Key: hklm\software\classes\wow6432node\clsid\{7e1219f4-b760-422c-8db0-db494026530f}\localserver32
Registry Value type: REG_SZ

- **ssms.exe**

MD5: 6c91137b6f1dc87ada3871902005f430
ssms.exe -> Executable file written to registry-> notepad.exe
Agent: BpvUltimusDB84
Date: 5/10/2018 5:21:47 PM
Execution path: d:\program files (x86)\microsoft sql server\110\tools\binn\managementstudio\
Process command line: "D:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\Ssms.exe"
User: bpvsvradm
Registry Data: c:\windows\system32\notepad.exe
Registry Key: hku\s-1-5-21-1715171594-2963467581-4185796964-1001\software\microsoft\sql server management studio\11.0_config\toolsoptionsdefaults\webbrowser
Registry Value type: REG_SZ
SQL Server Management Studio (ssms.exe) is a Windows GUI for SQL Server. This event was initiated by Microsoft SQL SERVER Management Studio using user "bpvsvradm", it added notepad.exe as a key to toolsoptionsdefaults\webbrowser for sql server management studio. This event seems like notepad was added as an external tool to SQ server Management Studio.

- **ultimus.xvsobjectservice.exe**

MD5: 46fa740fe67377cd6c67362261dbe60f
ultimus.xvsobjectservice.exe -> Network – New protocol –> 10.100.210.55, 0.0.0.0
Execution path: c:\program files (x86)\ultimus adaptive bpm suite 8.4\
Process command line: "C:\Program Files (x86)\Ultimus Adaptive BPM Suite 8.4\Ultimus.XVSObjectService.exe"
User: ultimus
Agent: BPVULTIMUSFE84
Date: 5/11/2018 7:44:50 PM
This is considered part of regular function of the ULTIMUS solution. This application connects to the same IP configured on NIC.

- **msdtc.exe**

MD5: 915747e010a9414b069173284a9b93f4
msdtc.exe->Network – New protocol -> 10.100.201.38 [tcp]:58562
msdtc.exe->Network – New protocol -> 10.100.210.55 [tcp]:52424
Agent: BpvUltimusDB84

Process ID: 1564
Date: 5/11/2018 7:40:51 PM
Execution path: c:\windows\system32\
Process command line: C:\Windows\system32\msdtc.exe
MSDTC is a Windows service providing transaction infrastructure for distributed systems. In this case, a transaction means a general way of structuring the interactions between autonomous agents in a distributed system. Each transaction is a state transformation with four key properties - the ACID properties: Atomic (all or nothing), Consistent (legal), Isolated (independent of concurrent transactions) and Durable (once it happens, it cannot be abrogated). This Process started a connection to Agent BpvUltimusFE and BpvUltimusFE84 (itself).

- **mrt-kb890830.exe**

MD5: 2fa4579ba7472b438c99ad74e3ed8829

Origin Entity	Behavior name	Destination entity
mrt-kb890830.exe	Executable self-delete	mpengine.dll, mpgear.dll, offreg.2564.dll
	Executable dropped	mpengine.dll, mpgear.dll, offreg.2564.dll
	Executable edited in system folder	offreg.2564.dll

Agent: Bpvblwb1
Date: 5/13/2018 1:58:15 AM
User: Local System
Execution path: c:\windows\system32\
Process command line: "C:\Windows\system32\MRT-KB890830.exe" /Q /W
Microsoft Windows Malicious Software Removal Tool.

- **lsass.exe**

MD5: 382100e75b6f4668aeaef228c6ceffad
Agent: Bpvexch01
Date: 5/13/2018 6:22:14 PM
Execution path: c:\windows\system32\
Process command line: C:\Windows\system32\lsass.exe
User: Local System
Isass.exe is the Local Security Authority Service of Microsoft, Inc., which is responsible for the security policy and other Windows security mechanisms.

Lsass.exe also verifies the identification of the user when he is logging into his computer and generates the responsible processes for this authentication when using Winlogon service. The lsass.exe operates mainly in the system due to its ability to create access tokens.

- **lnsscomm.exe**

MD5: ee4d8af19d68111fa1b1af39dcb4deca
lnsscomm.exe ->Executable self delete -> heartbleed.py
lnsscomm.exe ->Executable self delete ->conficker.py
lnsscomm.exe ->Executable dropped -> freak.py
lnsscomm.exe ->Executable dropped -> avast4_pro_isrunning.py
Agent: BpvUltimusWS
Date: 5/13/2018 9:24:09 PM
User: Local System
Execution path: c:\program files (x86)\gfi\languard 12 agent\
Process command line: "C:\Program Files (x86)\GFI\LanGuard 12 Agent\lnsscomm.exe" -Embedding
lnsscomm.exe is a legitimate process file popularly known as LNSS Communicator module. It is associated with GFI LanGuard software, developed by GFI Software Development. Is required by third-party software or hardware and should not disabled.
This executable is the LNSS Communicator module for the GFI LANguard 2011 application - network security application for companies, which provides patch management, vulnerability assessment, network auditing and many other functions;

- **msexchangefrontendtransport.exe**

MD5: 509acf2e843f65311da92361f51b8163
msexchangefrontendtransport.exe-> network send-> 10.100.201.113 [tcp]:46324
msexchangefrontendtransport.exe-> network send-> 10.100.201.113 [tcp]:46268
Agent: BpvExch02
Date: 5/13/2018 1:01:39 AM
User: Local System
Execution path: c:\program files\microsoft\exchange server\v15\bin\
Process command line: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe"
This files most often belongs to product Microsoft® Exchange. and were most often developed by company Microsoft Corporation.

- **edgetransport.exe**

MD5: c1a7402f239b06f8fdce367691ddc30b
edgetransport.exe->Network - new protocol-> 10.100.201.118 [tcp]:57687
edgetransport.exe->Network - new protocol-> 10.100.201.119 [tcp]:40043
Agent: BpvExch01
Date: 5/13/2018 6:24:44 PM
User: undefined
Source port: 2525
Execution path: c:\program files\microsoft\exchange server\v15\bin\
Process command line: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\edgetransport.exe" -pipe:1704 -stopkey:Global\ExchangeStopKey-edf56ba9-09f8-4f45-aa11-316efb50cf25 -resetkey:Global\ExchangeResetKey-c074cf44-8fd8-40dd-9a75-8a8022057dba -readykey:Global\ExchangeReadyKey-92f1cb63-29fd-42e6-8f61-2a8d64bbfb6c -hangkey:Global\ExchangeHangKey-ff9e526f-cb2d-4a78-9e55-e96e589990ed -workerListening
EdgeTransport.exe and MSExchangeTransport.exe are the executable files used by the Microsoft Exchange transport service. This service runs on all Hub Transport servers or on all Edge Transport servers. Changes that are saved in the EdgeTransport.exe.config file are applied after the Microsoft Exchange Transport service is restarted.

- **mscorsvw.exe**

MD5: 7761fbd826c16a007d6386fbfb846241
mscorsvw.exe->Executable edited in system folder-> System.web.routing.ni.dll, System.web.routing.dll
mscorsvw.exe->Executable Dropped->system.web.routing.ni.dll
Execution path: c:\windows\microsoft.net\framework\v4.0.30319\
Process command line: C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe -StartupEvent 500 -InterruptEvent 0 -NGENProcess 7e4 -Pipe 5d8 -Comment "NGen Worker Process"
Date: 5/14/2018 5:09:46 AM (Most recent)
Agent: BpvExch01
User: Local System
This is a runtime optimization service for the .net framework, it's a worker process for NGEN which helps optimization. Precompiles assemblies. This shows an alert but should not, since on client's environment there are many .NET apps.

- **csc.exe**

MD5: eb70bf071ec54bf0c29408ffdb89e3bb
csc.exe -> Executable edited in user's folder-> app_web_5ztmqqbp.dll
Execution path: c:\windows\microsoft.net\framework\v4.0.30319\
Process command line: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\ultimus.banvivi.prestamoauto\9133a72b\27311f75\5ztmqqbp.cmdline"
Agent: BpvUltimusFE84
Date: 5/14/2018 10:27:35 AM
Visual C# Command Line Compiler. Used by .NET framework apps.

- **svchost.exe**

MD5: c78655bc80301d76ed4fef1c1ea40a7d
svchost.exe -> Network - new protocol -> 10.100.210.210 [tcp]:51395
*It has more destination entities.
Execution path: c:\windows\system32\
Process command line: C:\Windows\system32\svchost.exe -k netsvcs
User: Local System
Agent: bpvblwb2
Date: 5/14/18 3:50:24 PM
svchost.exe is a process that hosts other Windows services that perform various system functions. There can be multiple instances of svchost.exe

- **w3wp.exe**

MD5: 18f2a1df70b5fa7f547d391d73b1ddb5
w3wp.exe-> Executable Self Copy->seguros.dll
Agent: BpvUltimusFE
Date: 5/15/2018 9:09:21 AM
Execution path: c:\windows\syswow64\inetsrv\
Process command line: C:\Windows\SysWOW64\inetsrv\w3wp.exe -ap "AppWAPPFram2" -v "v2.0" -l "webengine4.dll" -a \\.\pipe\iisipm800eb189-d28a-46f0-86ce-8517f0ce643f -h "C:\inetpub\temp\apppools\AppWAPPFram2\AppWAPPFram2.config" -w "" -m 0 -t 20 -ta 0
An Internet Information Services (IIS) worker process is a windows process (w3wp.exe) which runs Web applications, and is responsible for handling requests sent to a Web Server for a specific application pool. This is part of the regular

functioning of the IIS.

- **wmiprvse.exe**

MD5: dcc48f1bdc0e239776ba05a7239991f7
wmiprvse.exe-> Process execution from a suspicious path-> dismhost.exe
wmiprvse.exe-> Executable Self Delete -> dismhost.exe
*It has more destination entities.
Agent: BpvFtpSrvW12
Date: 5/15/2018 4:15:54 AM
Execution path: c:\windows\system32\wbem\
Process command line: C:\Windows\system32\wbem\msexchangefrontendtransport.exe -Embedding
WMI Provider Host (WmiPrvSE.exe) stands for Windows Management Instrumentation Provider Service. It's an important service that applications cannot run without. If this process stops, many of the features in your PC will become useless. On top of all, you might not even receive error notifications.

- **iexplore.exe**

MD5: 947bf3d2c108c7bda86d3e7c57713f11
iexplore.exe -> Executable dropped -> analytics[1].js
*It has more destination entities.
Agent: BpvUltimusFE84
Date: 5/15/2018 1:30:38 PM
User: jorge.gaitan
Execution path: c:\program files (x86)\internet explorer\
Process command line: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:60332 CREDAT:275457 /prefetch:2
The iexplore.exe file is referred to as the executable file of Microsoft Internet Explorer. The graphical user interface of the iexplore.exe file is composed of graphical Internet pages viewed. Iexplore.exe is the Web browser that connects to the Internet when a user enters a URL in the address bar found on its GUI.

- **sqlservr.exe**

MD5: 857af0e5875315ec2aeb176b715a65df
sqlservr.exe -> Network – new protocol -> 10.100.201.68 [tcp]:39772
* Generates other target entities with the same address with different ports
Agent: BpvUltimusDB84
Date: 5/16/2018 4:20:32 PM

Execution path: d:\program files\microsoft sql server\mssql11.mssqlserver\mssql\binn\
Process command line: "D:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\sqlservr.exe" -sMSSQLSERVER
The main executable for Microsoft SQL Database Server.

- **dbgview.exe**

MD5: baaca87fe5ac99e0f1442b54e03056f4
dbgview.exe -> Executable file written to registry -> imagepath
Agent: BpvUltimusFE84
Date: 5/16/2018 4:55:18 PM
User: ultimus
Execution path: c:\software\debugview\
Process command line: "C:\SOFTWARE\DebugView\Dbgview.exe"
DebugView is an application that lets you monitor debug output on your local system, or any computer on the network that you can reach via TCP/IP.

- **setup.exe**

MD5: e77bcaeaff3b21372265d612f6bca98c
setup.exe -> Executable self-delete -> setup.exe
Agent: BpvUltimusWS
Date: 5/17/2018 3:35:23 AM
User: Local System
Execution path: c:\program files (x86)\google\chrome\application\65.0.3325.181\installer\
Process command line: "C:\Program Files (x86)\Google\Chrome\Application\65.0.3325.181\Installer\setup.exe" --update-setup-exe="C:\Windows\TEMP\CR_DC6B1.tmp\SETUP_PATCH.PACKED.7Z" --new-setup-exe="C:\Windows\TEMP\CR_DC6B1.tmp\setup.exe" --verbose-logging --do-not-launch-chrome --system-level
Setup.exe is a software file that is used by software programs for installations. In this case, a recent version of the Chrome browser was installed.

- **dllhost.exe**

MD5: cc05c14eeff5e7813a49718ba88e59b0
dllhost.exe -> Network – New protocol -> 10.100.210.55 [tcp]:56294
dllhost.exe-> Executable dropped->prestamoautosfideicomiso.dll
dllhost.exe->Executable self copy -> prestamoautosfideicomiso.dll

Agent: BpvUltimusFE84
Date: 5/16/2018 4:07:16 PM
User: ultimus
Execution path: c:\windows\syswow64\
Process command line: C:\Windows\SysWOW64\dllhost.exe /Processid:{E1F42722-E135-4777-84C4-A0225E5F4E92}
"dllhost.exe" is a Microsoft Windows standard process, it manages the configuration and tracking of Component Object Model (COM)+-based components. It is used for launching other applications and services. It should be left running as it is critical to several system resources. The behaviors found correspond to regular ultimus functioning.

- **msdtc.exe**

msdtc.exe -> Network – new protocol -> 10.100.210.62 [tcp]:51423
MD5: 915747e010a9414b069173284a9b93f4
smsvchost.exe -> network – new protocol -> 0.0.0.0 [tcp]:42708
Agent: BpvUltimusFE84
Date: 5/18/2018 6:10:25 PM
Execution path: c:\windows\system32\
Process command line: C:\Windows\System32\msdtc.exe
Msdtc.exe is an integral component of the Microsoft Distribution Transaction Coordinator (MSDTC) program. The purpose of this program is to allow multiple client applications to have more than one source of data, for any one transaction. The msdtc.exe process is then tasked with coordinating the distribution across the various servers of the transaction.

- **dism.exe**

MD5: b1b97114d180b5b1b05eb84f50441091
dism.exe-> Executable file created-> transmogprovider.dll
Agent: BPVBLBE2
Date: 5/19/2018 12:09:11 AM
Execution path: c:\windows\system32\
Process command line: C:\Windows\TEMP\03CCDF2E-B9AE-4C60-9B91-473BEC180DDF\dismhost.exe {BD6514E5-0E82-495A-A334-056B9A00D484}

User: Local System
This is a Portable Executable file, more specifically, it is a Win32 EXE file for the Window command-line subsystem that addresses 64-bit architectures.

- **macmnsvc.exe**

macmnsvc.exe -> Network – new Protocol -> 10.100.210.133 [tcp]:58600
macmnsvc.exe -> Network – new Protocol -> 10.100.210.143 [tcp]:64370
macmnsvc.exe -> Network – new Protocol -> 10.100.210.136 [tcp]:56000
macmnsvc.exe -> Network – new Protocol -> 10.100.210.84 [tcp]:62956
MD5: 94fec1b803f743470306fabfa18cf711
Agent: BpvUltimusDB84
Date: 5/21/2018 11:25:22 AM
Execution path: c:\program files (x86)\mcafee\common framework\
Process command line: "C:\Program Files (x86)\McAfee\Common Framework\macmnsvc.exe" /ServiceStart
McAfee Agent Common Service.

- **msexchangehmhost.exe**

msexchangehmhost.exe -> Network – new protocol -> 10.100.201.118 [tcp]:25615
*It has more destination entities.
MD5: 38891e157d7d95aeed90afad77997830
Agent: BpvExch02
Date: 5/21/2018 12:10:45 PM
User: Local System
Execution path: c:\program files\microsoft\exchange server\v15\bin\
Process command line: "C:\Program Files\Microsoft\Exchange Server\V15\Bin\MSExchangeHMHost.exe"
Exchange Health Manager Service.

- **ultimusorganizationcharts.exe**

ultimusorganizationcharts.exe -> Network - new protocol -> 0.0.0.0 [tcp]:80
ultimusorganizationcharts.exe -> Network - new protocol -> 172.16.1.202 [tcp]:389
MD5: feeb305189f601bd2fe4678134f928f7
Agent: BpvUltimusFE84
User: jorge.gaitan
Date: 5/22/2018 6:25:20 PM
Execution path: c:\program files (x86)\ultimus adaptive bpm suite 8.4\
Process command line: "C:\Program Files (x86)\Ultimus Adaptive BPM Suite 8.4\UltimusOrganizationCharts.exe"
Ultimus Organizational Charts App is trying to fetch information from host IP 172.16.1.202 on port 389(LDAP), This host is not part of the group of hosts with agents installed even though it is accessed or probed to a private IP address.

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

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

Info@glesec.com
www.glesec.com