www.glesec.com

GLESEC

OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

BANVIVIENDA

JULY,2018

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

Info@glesec.com
www.glesec.com

Table of Contents

CONFIDENTIAL

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.

CONFIDENTIAL

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 10 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	4	25	9	38

According to the metrics:

$RV = 0.287719298$

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	23	8	31
Service detection		4	0	0	4
Misc.		0	1	1	2
Windows		0	1	0	1

- General
- Services detection
- Misc
- Windows

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

The 6 most vulnerable hosts during this period have medium severity vulnerabilities.
• 200.90.137.87 (21%) and 200.90.137.89 (21%) have vulnerability in port 25 and with risks of low, medium and high level.

• 200.90.137.83, 200.46.227.230 and 200.46.19.100; port 443 vulnerable in these host and low, mediun and high severity risks.

• 200.90.137.91, with port 443, 25 and 10000 vulnerable in these hosts and has medium level risks.

• Ports 443 and 25 are of high severity.

Additional details about these vulnerabilities are presented in the Vulnerabilities found in BANVIVIENDA by severity section of the MSS-VM **on page 11.**

15 hosts were discovered, of which 10 are vulnerable, BANVIVIENDA has 38 vulnerabilities in total this month, the vast majority have been medium risk vulnerabilities 25 (66%), high 4 (10%) and low risks 9 (23 %) and No vulnerabilities of critical severity have been found during the course of the month.
The number of medium and low vulnerabilities has remained the same throughout the month. The category of Vulnerabilities presented is: General (81), Service Detection (11%), Misc (5%) and Windows (3%).

The vulnerabilities found of high consideration for this period are:
- SSL Version 2 and 3 Protocol Detection on hosts: 200.90.137.87, 200.90.137.89, 200.90.137.83 and 200.46.19.100.

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.

Las vulnerabilidades de consideración media encontradas para este periodo son las siguientes:
- SSL Medium Strength Cipher Suites Supported
- SSL Certificate Cannot Be Trusted
- SSL Certificate Signed Using Weak Hashing Algorithm
- SSL Self-Signed Certificate
- SSL Weak Cipher Suites Supported

CONFIDENTIAL

- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE).

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.
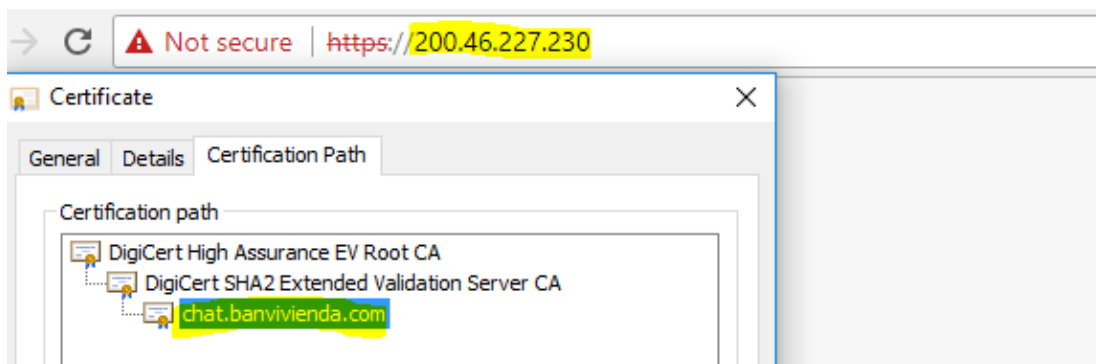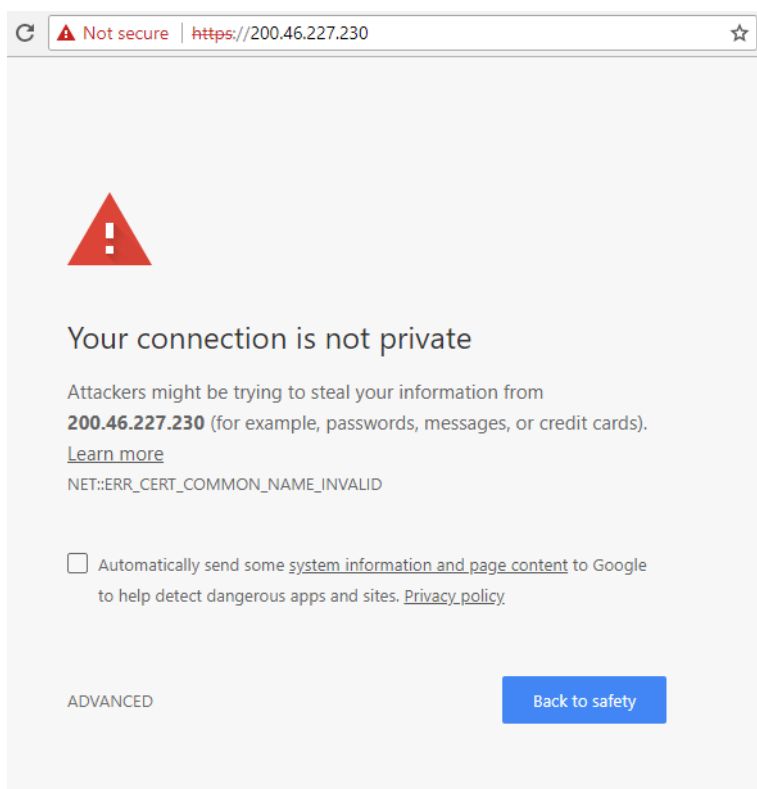
200.46.227.230
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Medium Strength Cipher Suites Supported, SSL Weak Cipher Suites Supported, SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK), SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.
https://www.banvivienda.com/es

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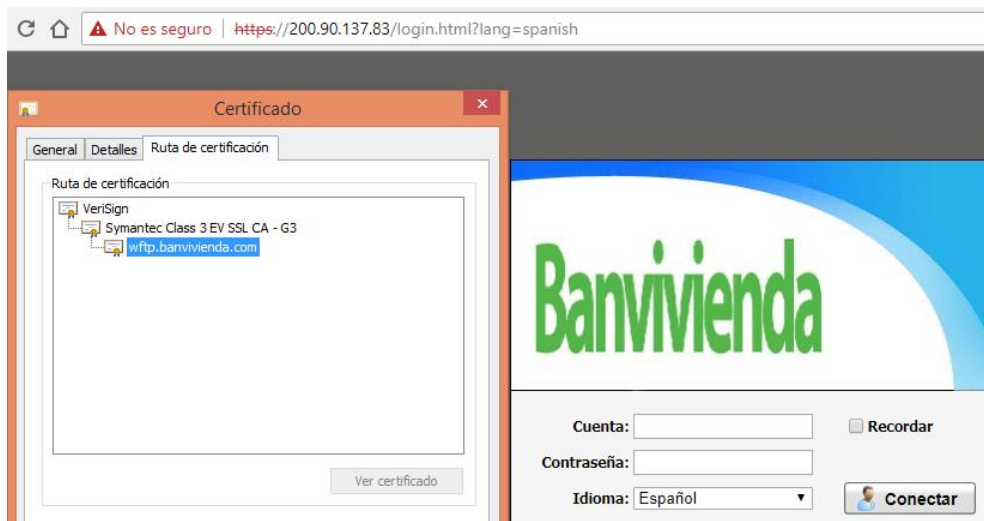Tel: +1 (609)-651-4246 / +(507)-836-5355

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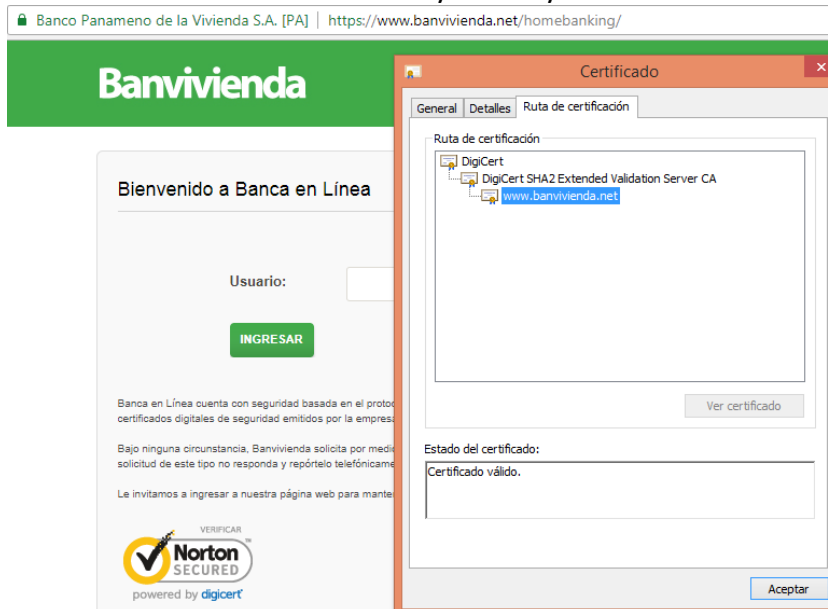
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
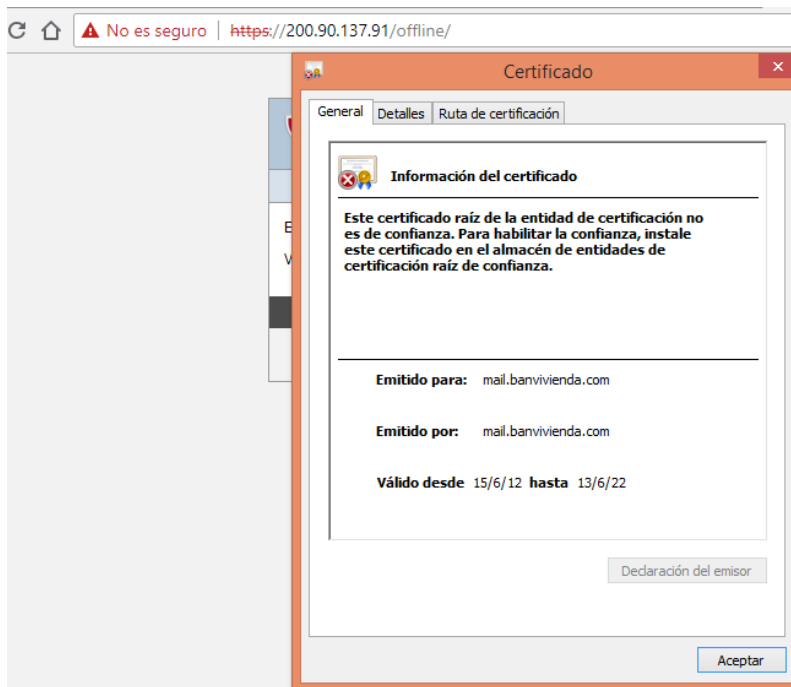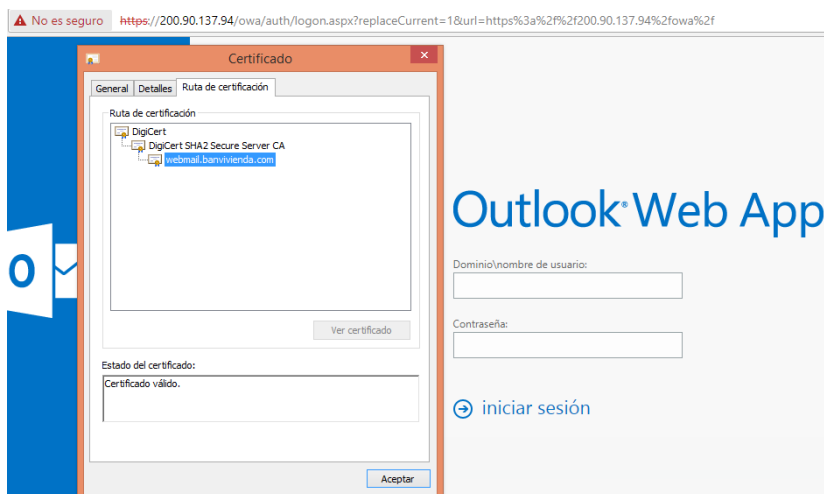Tel: +1 (609)-651-4246 / +(507)-836-5355

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.

CONFIDENTIAL
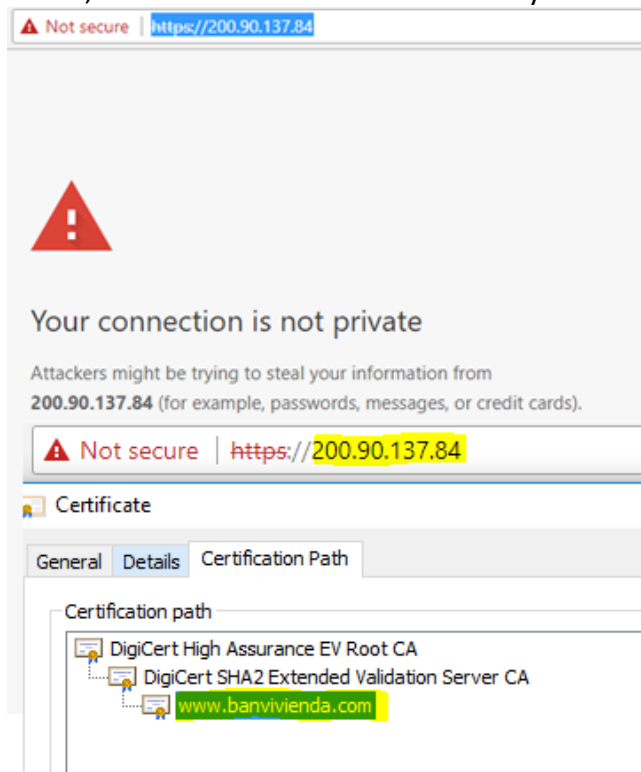
200.46.19.98
During this month, the GLESEC operations center, we rediscovered the same vulnerability called "Aggressive Internet key exchange (IKE) mode with pre-shared key". We recommend following the solution procedure for this problem, which is described in the Vulnerabilities by severity section of this document.
Of the attacks made to your organization, 42% are directed specifically to this host.

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.

57% of attacks are directed to this host.

Vulnerabilities by severity

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

High Risk Level Vulnerabilities

SSL Version 2 and 3 Protocol Detection
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:

- An insecure padding scheme with CBC ciphers.

- 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.

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 use 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

CONFIDENTIAL

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.

CONFIDENTIAL

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
```

CONFIDENTIAL

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.

CONFIDENTIAL

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

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 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

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

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)
```
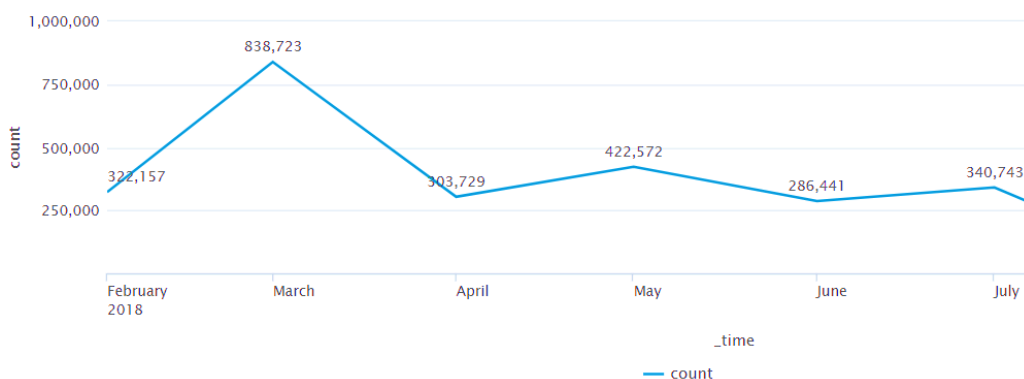
CONFIDENTIAL

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 340,743 attacks denied by the rules of the firewall.

We have noticed an increase in attack activity of 19% since last month. We recommend BANVIVIENDA to review the activity of the devices where these events are recorded.

All attacking addresses tried to access hosts 200.46.19.98 and 200.46.227.227, most attacks are directed to port 23 (Telnet), followed by port 80 (HTTP) and port 22 (SSH).

The type of attack mostly presented during this period was anti-spoof on the aforementioned hosts with a total of 70% (204,653 attacks of this type), TCPCheck 26% and UDPckeck 4%.
It has also had ICMP check attacks; all these attacks have been blocked.

The network activities are: Network access point, IKE and IPsec, User session, Access lists, IP Stack and NAT and PAT, which were noticed during the course of the month.

Los ataques son provenientes de países como China (29%), Rusia (26%), Estados Unidos (17%) y Brasil (8%). Most of these attack attempts were probing the services mentioned above.

CONFIDENTIAL

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

Types of attacks presented during this month for BANVIVIENDA:
- Anti-spoof
- TCPckeck
- UDPckeck
- Mgmtplane
- ICMPckeck
- DNS snoop
- L3 drop

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)
- 80 (HTTP)
- 22 (SSH)
- 443 (HTTPS)
- Snmp (25)

Top Five 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 is highlighted for quicker recognition.

- 209.97.180.124
- 103.99.2.120
- 62.32.81.84
- 200.46.73.116
- 200.46.239.19

Top Five 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.

- 200.46.227.227
- 200.46.19.98
- 172.16.230.196
- 150.150.1.147
- 10.100.202.204

CONFIDENTIAL

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, many false positive alerts, there were many alerts that show the regular operations of the applications installed on the hosts, some of them as repetitive as: updateservice.exe, patchagent.exe for the installation of security patches, nsclient ++. Exe, w3wp.exe using aspose.words.dll and other alerts generated by normal system processes.

During this period in our GOC, we have received fewer alerts compared to the previous month, a total of 282 alerts received from BANVIVIENDA.

The most notable behavior during this period is the following:
- Executable self-deletes, Executable dropped
- Executable dropped, Executable with abnormal extension created
- Executable dropped
- Executable dropped, File deleted in program files, File created in program files
- Service created, Service changed

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 following list of events presents details about the entities that generated the

alerts, the agents in which they were found, MD5 of the source file for validation, the user with whom it was executed, the source file execution path, the command line of the process used, and a brief description of each one These are considered the most relevant events during this month:

mscorsvw.exe
Behavior of this entity is the following:
- mscorsvw.exe->Executable dropped-> microsoft.windows.design.developer.wpf.ni.dll *
- mscorsvw.exe->File with double extension created-> microsoft.windows.design.developer.wpf.dll*
- mscorsvw.exe->Executable edited in system folder>microsoft.windows.design.developer.wpf.ni.dlll *

MD5: 7761fbd826c16a007d6386fbfb846241
Process directory: c:\windows\microsoft.net\framework\v4.0.30319\
The target entity changes from one alert to the other, but the behavior is the same. This process corresponds to the .NET Runtime Optimization Service; This behavior was identified repeatedly during certain days of the month of July.

wftptray.exe
It is one of the alerts we receive daily.
MD5: b97ea04bf5b3359e209bb0d73d78730f
Process directory: c:\program files (x86)\wing ftp server\
Severity: Medium
This is a process generated by an FTP server, we believe that it is part of the daily activities of the client.

Tiworker.exe
Behavior of this entity is the following:
- PMtiworker.exe-> Executable with abnormal extension created->Executables
- tiworker.exe-> Executable edited in system folder->Executables

MD5: 2b902ea3056aabf8eccb689d434ae2c9
Agent: BpvWebSvr
Process command line: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.18384_none_fa1d93c39b41b41a\TiWorker.exe –Embedding
Process directory: c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.18384_none_fa1d93c39b41b41a\

User: Local System
6/5/2018 8:58:53

This process is responsible for searching and installing updates in Windows; it is also used when adding or deleting a new feature in Windows systems, we can conclude that this is the reason why this process is executed repetitively in your systems.

lnsscomm.exe
MD5:ee4d8af19d68111fa1b1af39dcb4deca
Process directory: c: \ program files (x86) \ gfi \ languard 12 agent \
Agent: BpvUltimusWS
This is a process generated by languard agent 12

Teamviewer_.exe
It is one of the alerts we receive daily.
- Behavior of this entity is the following:
- teamviewer_.exe-> Executable dropped-> teamviewer_desktop.exe
- teamviewer_.exe-> Executable with abnormal extension created->tvmonitor.sy_
- teamviewer_.exe-> Executable path written to registry-> teamviewer_resource_en.dll
- teamviewer_.exe-> Executable self copy-> userinfo.dll
- teamviewer_.exe-> Executable self copy-> system.dll
- teamviewer_.exe-> Executable self copy-> tvgetversion.dll

MD5: 6f2d7f7e6b1b2af8c04b6ecbc8cb6aa5
Agent: BpvUltimusDB84
Severity: Medium
Process command line:
C:\Users\BPVSVR~1\AppData\Local\Temp\1\TeamViewer\TeamViewer_.exe /RUN
Process directory: c:\users\bpvsvr~1\appdata\local\temp\1\teamviewer\
User: bpvsvradm

This process is generated in another agent:
MD5: a889e7974a7b9a41af88b77e17627d26
Agent: BpvUltimusDB84
We have received in this period a total of 20 alerts related to this process.

csc.exe

Behavioral:
- csc.exe -> Executable Dropped -> app_web_acrnqef2.dll

MD5:eb70bf071ec54bf0c29408ffdb89e3bb
MD5:8d3c9fc98fe9770d6dc2caa289449db7
MD5:95e08f018b0eb4f76ef7368610ce49ce
Severity: Medium
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\utimus.persona\c1d3a94e\6f313c81\acrn qef2.cmdline"

w3wp.exe
Behavior of this entity is the following:
- w3wp.exe-> Executable edited in system folder->aspose.words.dll
- w3wp.exe-> Executable self copy->aspose.words.dll
- w3wp.exe-> Executable edited in system folder->interop.scripting.dll
- w3wp.exe-> Executable edited in system folder-> interop.msxml2.dll
- w3wp.exe-> Executable edited in system folder-> aspose.words.dll

Agent: BpvUltimusFE
Process command line: C:\Windows\SysWOW64\inetsrv\w3wp.exe -ap
"APP_Documentos" -v "v2.0" -l "webengine4.dll" -a \\.\pipe\iisipm6b497d70-af85-
480a-89de-199204135384 -h
"C:\inetpub\temp\apppools\APP_Documentos\APP_Documentos.config" -w "" -m 0
-t 20 -ta 0
Process directory: c:windows\syswow64\inetsrv\
User: ultimus

Aspose.Words for .NET is a cross-platform class library that enables your applications to perform a great range of document processing tasks. With Aspose.Words you can load, save and convert documents between the following formats: DOC, DOT, DOCX, DOCM, DOTX, DOTM, XML (including Word 2003 XML), RTF, HTML, MHTML, MOBI, ODT, OTT, TXT – also you can convert them to: PDF, XPS, SVG, EPUB, XAML, PS, PCL, TIFF, BMP, PNG, EMF, JPEG, GIF and other formats. With Aspose.Words you can generate, modify, convert, render and print documents without utilizing Microsoft Word®.

mrt.exe

- Behavior of this entity is the following:
- mrt.exe->Executable dropped -> mpgear.dll
- mrt.exe->Executable dropped-> mpengine.dll
- mrt.exe->Executable self delete-> mpgear.dll
- mrt.exe->Executable self delete-> mpengine.dll

Agent: BpvUltimusWS
Process command line: C:\Windows\system32\MRT.exe /EHB /Q
Process directory: c:\windows\system32\
User: Local system

This corresponds to a MRT.exe scan, this will happen as many times as it is configured to conduct threat scans.

updateservice.exe
- Behavior of this entity is the following:
- updateservice.exe-> Executable with abnormal extension created-> mpavdlta.vdm
- updateservice.exe-> Executable with abnormal extension created-> mpavbase.vdm
- updateservice.exe-> Executable dropped -> avemicrosoft.dll

MD5: ea88439e414813216532a4197c0e810c
Agent: BpvExch02
Process command line: "C:\Program Files\Microsoft\Exchange Server\V15\FIP-FS\Bin\updateservice.exe" -Embedding
Process   directory: c:\program   files\microsoft\exchange   server\v15\fip-fs\bin\

Microsoft Filtering Engine Update process, these 2 behaviors are related since every time the first 4 files are created, the other 2 are generated almost at the same time and from the same process, this process in particular has been up and running since 5/13/2018 6:22:39 PM, from that date, it has executed the same actions in a repetitive manner 175.

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

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

Info@glesec.com
www.glesec.com