MONTHLY OPERATIONS & INTELLIGENCE REPORT

TECHNICAL REPORT

BANVIVIENDA

March 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 is a for the MSS-BAS service.

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				9
Risk Distribution				
Critical	High	Medium	Low	Total
0	0	28	9	37

According to the metrics:

RV= 0.241621622

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:

plugin_family	low	medium
General	8	22
Service detection	0	4
Misc.	1	1
Windows	0	1

- General
- Services detection
- Misc
- Windows

Additional details about these vulnerabilities are presented in the Vulnerabilities found in BANVIVIENDA by severity section of the MSS-VM on page 5.

Overall the vulnerabilities for BANVIVIENDA this period have been 28 medium and 9 low-risk. Please refer to MSS-VM intelligence section for more detail about specific vulnerabilities. Medium risk vulnerabilities found were classified as SSL Medium Strength Cipher Suites Supported, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah), and SSL Certificate Signed Using Weak Hashing Algorithm. This means that attackers could take advantage of any of those and attempt to cause and negative impact to your Organization.

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

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. Nessus 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 that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

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

Affected Systems

25 / tcp / smtp 200.90.137.87200.90.137.89

443 / tcp / www 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

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	200.90.137.87, 200.90.137.89
443 / tcp / www	200.90.137.83, 200.90.137.83, 200.90.137.91
10000 / tcp / www	200.90.137.91

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 / www	200.46.19.100, 200.46.19.100, 200.90.137.83, 200.90.137.83

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
443 / tcp / www	200.90.137.91
10000 / tcp / www	200.90.137.91

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, 200.90.137.83

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, 200.90.137.94

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

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 / www 200.90.137.94, 200.46.19.100, 200.90.137.83, 200.46.227.230

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

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.

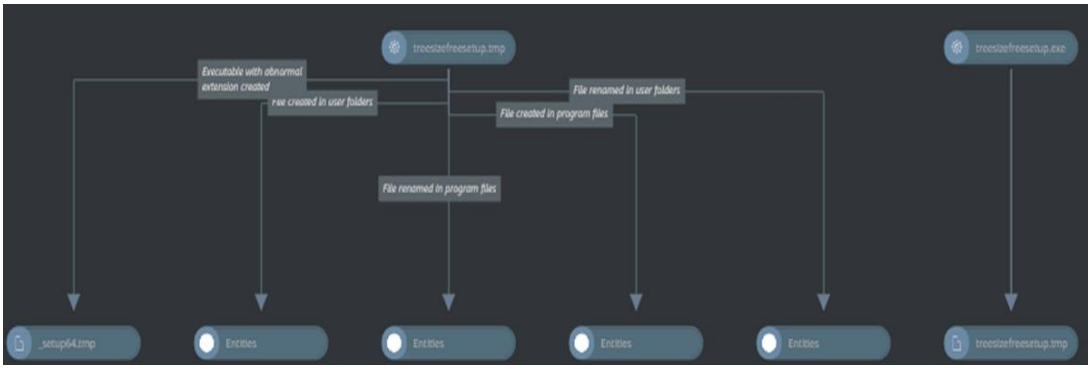
Top Events Registered By High Severity Level

Wireshark
Our Operation Center found that on agent BPVBLBE1, installed on your computer, user gmadm00 on the 29th of march,2018 at 12:14 PM performed Wireshark uninstallation from file in "D:\Program Files\Wireshark\uninstall.exe". As part of Wireshark uninstallation process also WinPcap was uninstalled from file in "C:\Program Files (x86)\WinPcap\uninstall.exe". GLESEC considers this event as high priority since installs/uninstalls/upgrades on production servers can cause high impact if it was not intended to happen. If this is part of regular procedures or you were aware of this, please let us know.

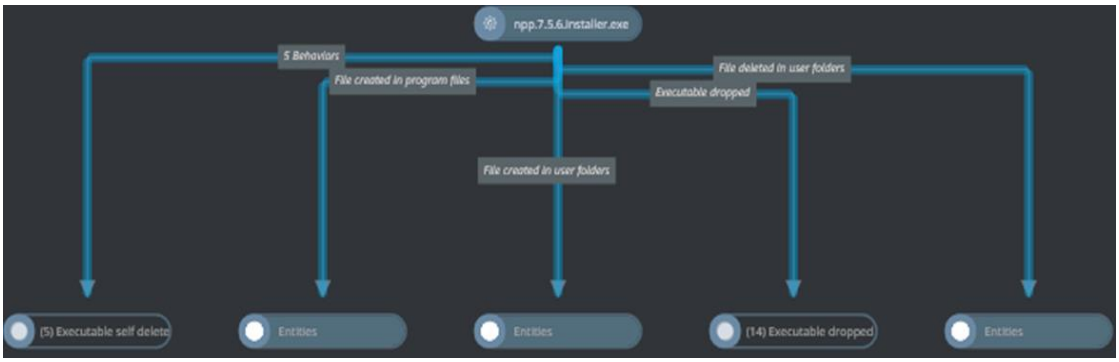
Note: WinPcap is very common traffic capturing tool regularly installed/uninstalled along with Wireshark.

Wireshark, TreeSizeFree
Our Operation Center found that agent BPVBLBE1, installed on your computer, at approximately 12:20 of the 29th of march 2018, user gmadm00 performed installation/uninstallation on this server of the following applications: Wireshark, TreeSizeFree, npp++ and 7-Zip. GLESEC considers this event as high priority since installs/uninstalls/upgrades on production servers can cause high impact if it was not intended to happen. If this is part of regular procedures or you were aware of this, please let us know.
TreeSizeFree uninstallation from file in "c:\program files\jam software\TreeSize Free\unins000.exe" with MD5 2d3665b200d4b8983e0114bedab1d4a7

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



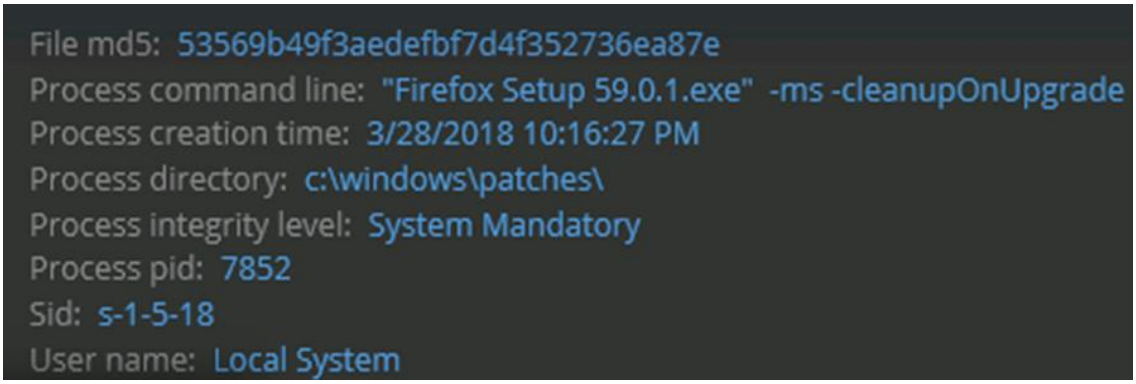
npp++ uninstallation from file in “d:\Program Files (x86)\Notepad++\uninstall.exe with MD5ed65b3ea722d605b1016bea3d06db491



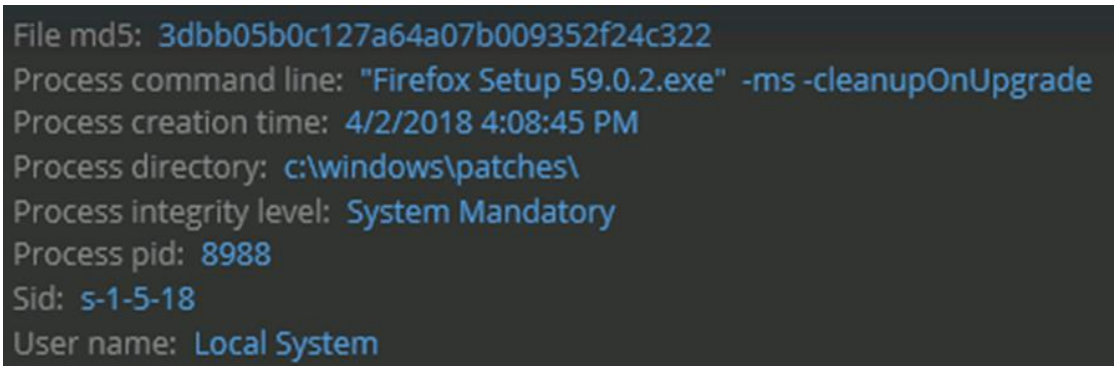
Mozilla Firefox

It was found that on agent bpvblbbe1, installed on your computer, there was an automatic upgrade by Local System user for Mozilla Firefox web browser on two different dates as follows:

•28/03/2018 at 10:16 pm: Upgrade to Firefox v 59.0.1 from file in “c:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice_tmp.exe”→ “c:\windows\patches\Firefox Setup 59.0.1.exe”



•02/04/2018 at 4:10 pm: Upgrade to Firefox v 59.0.2 from file in ":\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice_tmp.exe" → "c:\windows\patches\Firefox Setup 59.0.2.exe"



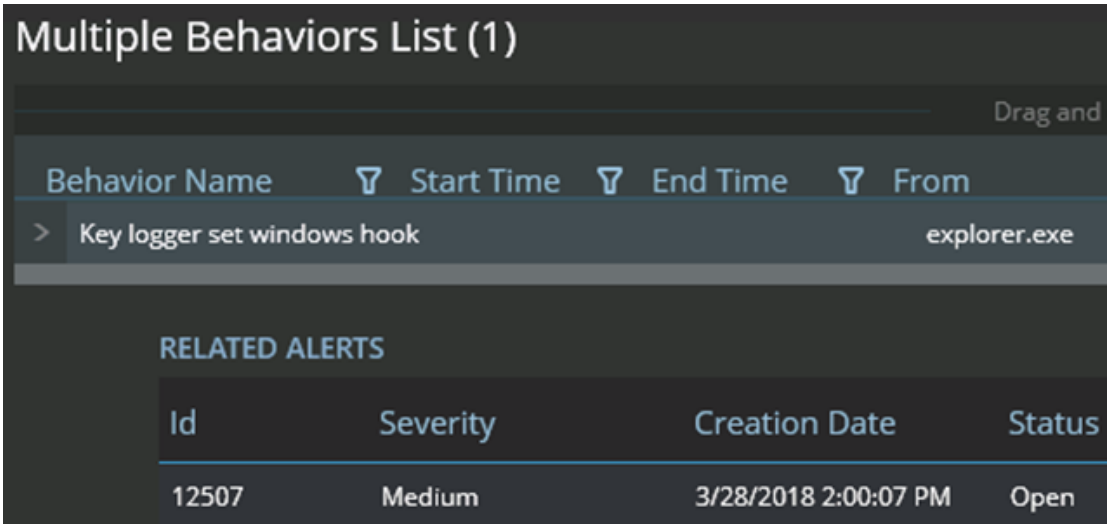
If this is part of regular procedures or you were aware of this, please let us know.

Top Events Registered By Medium Severity Level

key logger

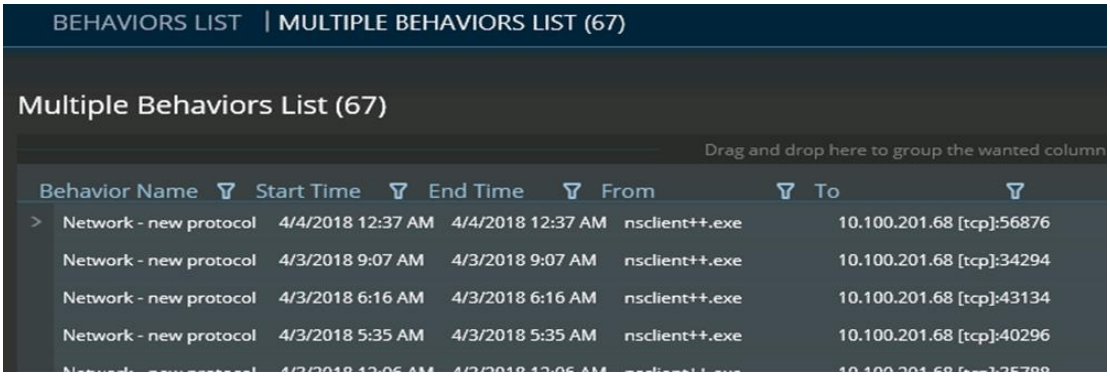
Our Operation Center found that agent BPVBLBE1, installed on your computer, at 09:59 PM of the 26th of march 2018, using user gmadm00, key logger set a Windows hook from "exploerer.exe". After follow up investigation on this event we found that it was part of a regular windows process.

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



nsclient++.exe

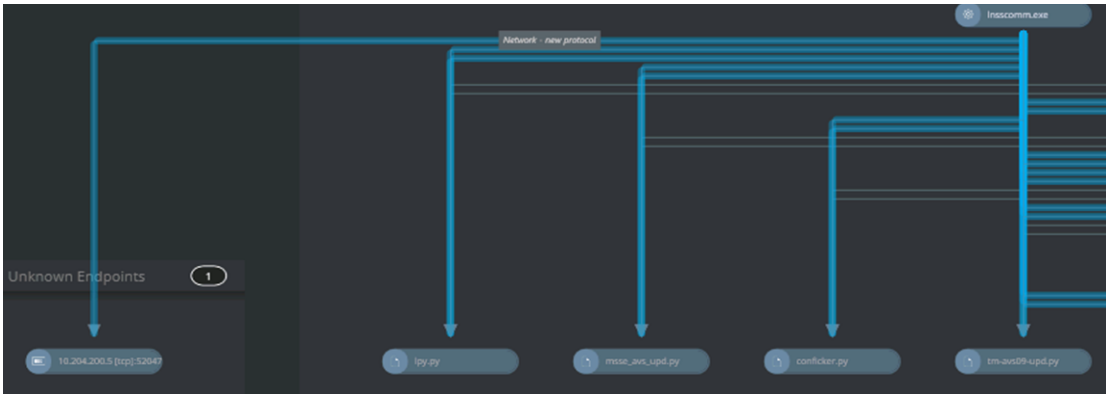
It was found that on agent BPVBLBE2, installed on your computer, from 31/03/2018 until Current time, a new connection is established to local address 10.100.201.68, this occurs many times a day. This connection is not initiated by a regular user but by "nsclient++.exe". This behavior is suspicious unless this is a monitoring agent configured to send data to previous mentioned address which should be the official collector of that information. If this is the regular monitoring agent for this server or you were aware of this, please let us know.



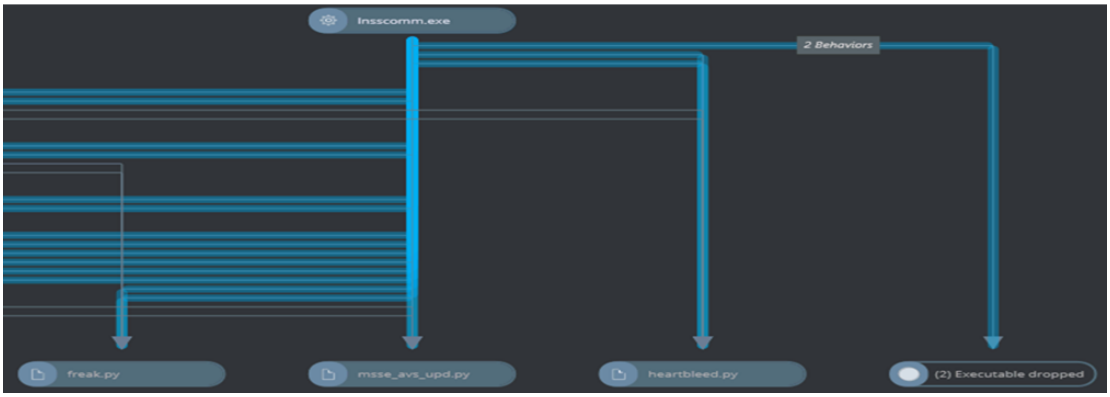
LanGuard 12 Agent

Our Operations Center was able to recognize that on computer BPVBLBE2, on 29/03/2018, from Local System user, a connection to host 10.204.200.5:52047 from 10.204.200.5:61301 was initiated from process command line "C:\Program Files(x86)\LanGuard 12 Agent\lnsscomm.exe" also, many python files were

executed as a result of this action as can be seen below. If this agent is installed officially and under network administrator's awareness, please let us know.



On 02/04/2018 Same event was repeated with the only difference that this time it did not start a connection to other entity, only executed many python files.



We noticed that 2 of the files executed by lnsscomm.exe are named "heartbleed.py" and "freak.py" as shown above. We strongly recommend to inspect the content of these files for better awareness.

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

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

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

Info@glesec.com
www.glesec.com