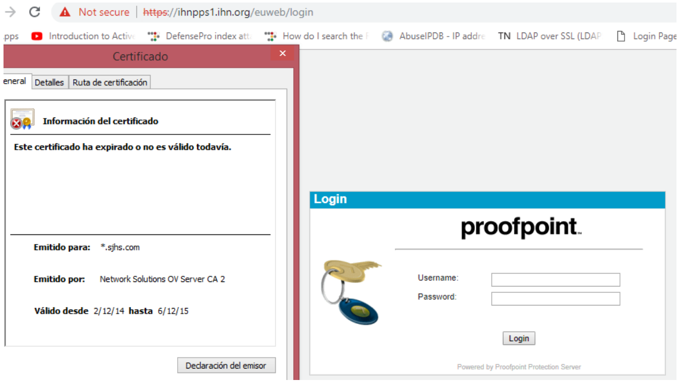
GLESEC INCIDENT REPORT

TLP-AMBER

Organization	Inspira Health Network.
Date	09/27/2018
Service	MSS-VM/MSS-APS
Severity Level	High
Impact Level	High
Vulnerability Level	High

INCIDENT DESCRIPTION

GLESEC Operation's Center discovered that host 170.75.33.4 has recently become the main destination of attacks for your systems, the most recurrent types of attack are L4 Source or Destination Port Zero (0) and Black List drops/blocks; this two comprise the 98% of the attacks targeting this system. This system appears to be a security and protection service for email and it is exposed to the internet with an invalid certificate, issued to "*.sjhs.com". this certificate issue was reported on the 29th of December 2017. This is event was detected as a correlation of services MSS-APS and MSS-VME.



Información del certificado

Este certificado ha expirado o no es válido todavía.

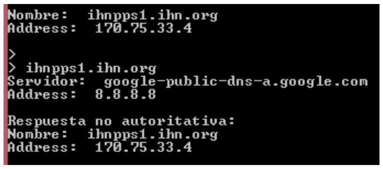
Emitido para: *.sjhs.com

Emitido por: Network Solutions OV Server CA 2

Válido desde 2/12/14 **hasta** 6/12/15

GLESEC INCIDENT REPORT

TLP-AMBER



```
Nombre:  ihnpps1.ihn.org
Address:  170.75.33.4

>
> ihnpps1.ihn.org
Servidor:  google-public-dns-a.google.com
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  ihnpps1.ihn.org
Address:  170.75.33.4
```

This IP address reverse resolves to ihnpps1.ihn.org and it is reachable from the internet.

ACTIONS TO BE TAKEN

Take a closer look of this event and verify what could have possibly changed that made this target more appealing for attackers, specially from the 20th of the current month. Issue and Install a valid certificate for this system.

COMMENTS AND RECOMMENDATIONS

GLESEC recommends keeping valid certificates installed on all system that are accessed through the internet through a secure protocol that requires it.

Malformed TCP/IP and UDP network traffic may have a source port of 0. TCP and UDP port 0 is a reserved port and should not normally be assigned. Traffic with this configuration may indicate malicious or abnormal activity.

GLESEC INFORMATION SHARING PROTOCOL

GLESEC CYBER SECURITY INCIDENTE REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, Restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/ Classified - Only Shared with US DHS).