Servicio Andaluz de Salud
CONSEJERÍA DE SALUD

INFORME DE INVESTIGACIÓN OSINT

Junio 2024

ÍNDICE

1. INTRODUCCIÓN

Debido a la solicitud del “Servicio Andaluz de Salud” para el desarrollo de un análisis técnico de investigación OSINT así como la detección de vulnerabilidades que alberga la compañía, se procede a la evaluación y al planteamiento de medidas preventivas frente a posibles ciberataques.

Los objetivos de esta investigación, son, la detección de vulnerabilidades críticas, las cuales posteriormente, permitan acceder a la red interna de la compañía y llevar a cabo un ciberataque. A raíz de esto, se procederá a la búsqueda de soluciones frente a las vulnerabilidades encontradas.

2. ALCANCE

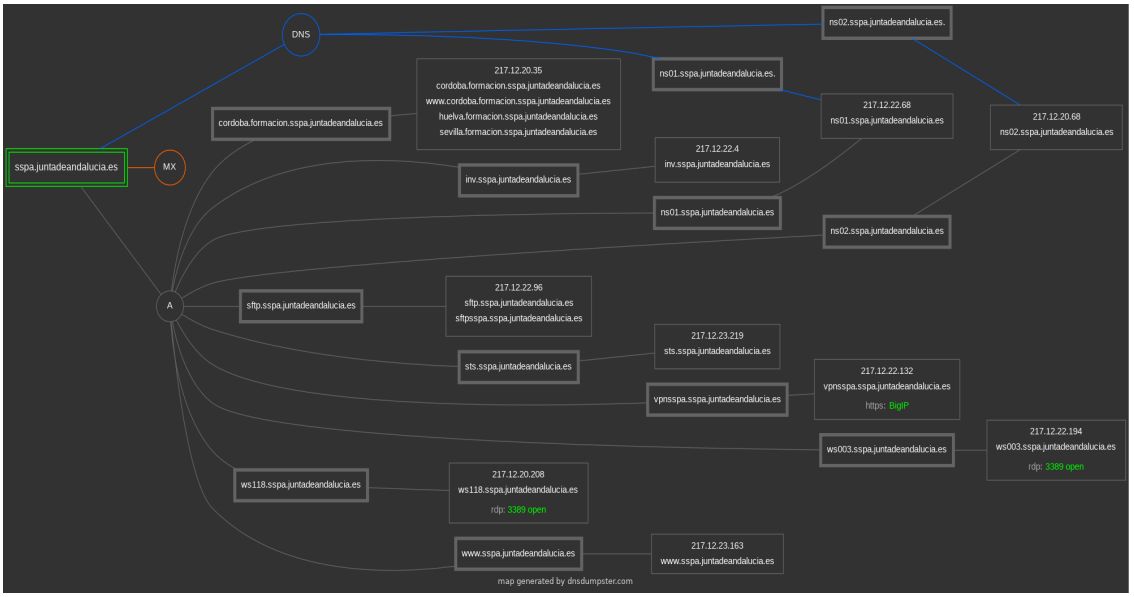
La información obtenida mediante herramientas como Shodan, Google Dorks, FOCA, Maltego y Spider Foot entre otros, revela varios puntos críticos en la infraestructura del SAS que podrían poner en riesgo la seguridad de la organización. Este análisis cubre aspectos relacionados con certificados SSL, redirecciones HTTP, correos electrónicos expuestos y la presencia de direcciones IP y correos electrónicos comprometedores.

3. PERFILADO DE LA ORGANIZACIÓN

El SAS Sistema Andaluz de Salud es un organismo autónomo adscrito al SSPA que se organiza bajo la Junta de Andalucía, gestionando una red extensa de servicios de salud donde SSPA se refiere al Sistema Sanitario Público de Andalucía.

Utilizando diversas herramientas de análisis, hemos podido realizar el perfilado de la organización así como se identificaron elementos clave de su infraestructura tecnológica.

A continuación, se presenta un gráfico organizacional basado en la información obtenida en Dnsdumpster así como un registro *txt* descubierto por la misma herramienta:



Como se evidencia en la imagen adjunta, durante el primer mapeo de sus dominios se identificó que la infraestructura del SAS integra dos sistemas de Servicio de Nombres de Dominio (DNS), proporcionados por la Sociedad Andaluza para el Desarrollo de las Telecomunicaciones (SANDETEL), con las siguientes IPs asociadas: 217.12.22.68 (ns01.sspa.juntadeandalucia.es) y 217.12.20.68 (ns02.sspa.juntadeandalucia.es), también destaca las principales direcciones IP, servicios, y asociaciones de dominios bajo el dominio principal sspa.juntadeandalucia.es.

Información relevante encontrada a partir del gráfico:

- Dominio Principal: sspa.juntadeandalucia.es
  - Asociado con la dirección IP principal: 217.12.23.163
  - Puertos Abiertos:
    - 80 (HTTP): Servicio web no cifrado.
    - 443 (HTTPS): Servicio web cifrado.

En la siguiente imagen, podemos observar una visión más detallada de las direcciones IP's vinculadas al dominio y subdominios web, así como el owner.

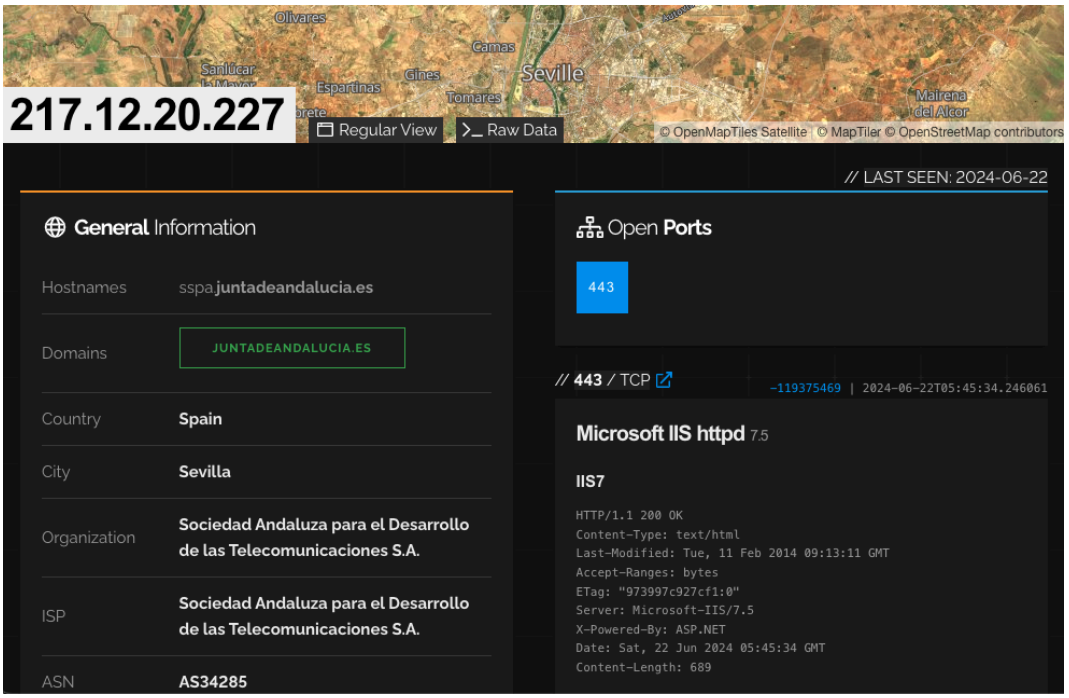
Hostname	IP Address	Type	Netblock Owner	Country
cordoba.formacion.sspa.juntadeandalucia.es	217.12.20.35	A	JJAA-AS	Spain
www.cordoba.formacion.sspa.juntadeandalucia.es	217.12.20.35	A	JJAA-AS	Spain
huelva.formacion.sspa.juntadeandalucia.es	217.12.20.35	A	JJAA-AS	Spain
sevilla.formacion.sspa.juntadeandalucia.es	217.12.20.35	A	JJAA-AS	Spain
inv.sspa.juntadeandalucia.es	217.12.22.4	A	JJAA-AS	Spain
ns01.sspa.juntadeandalucia.es	217.12.22.68	A	JJAA-AS	Spain
ns02.sspa.juntadeandalucia.es	217.12.20.68	A	JJAA-AS	Spain
sftp.sspa.juntadeandalucia.es	217.12.22.96	A	JJAA-AS	Spain
sftpsspa.sspa.juntadeandalucia.es	217.12.22.96	A	JJAA-AS	Spain
sts.sspa.juntadeandalucia.es	217.12.23.219	A	JJAA-AS	Spain
vpnsspa.sspa.juntadeandalucia.es	217.12.22.132	A	JJAA-AS	Spain
ws003.sspa.juntadeandalucia.es	217.12.22.194	A	JJAA-AS	Spain
ws118.sspa.juntadeandalucia.es	217.12.20.208	A	JJAA-AS	Spain
www.sspa.juntadeandalucia.es	217.12.23.163	A	JJAA-AS	Spain
ns02.sspa.juntadeandalucia.es.	217.12.20.68	NS	JJAA-AS	Spain
ns01.sspa.juntadeandalucia.es.	217.12.22.68	NS	JJAA-AS	Spain

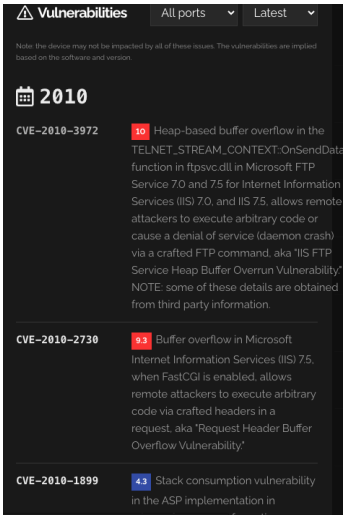
4. VULNERABILIDADES

Buscando en Shodan por SO Windows, encontramos otro servidor en este caso Microsoft II S httpd 7.5. (217.12.20.227 y 217.12.22.227)

Microsoft Internet Information Services (IIS) es un software de servidor web utilizado para alojar sitios web y aplicaciones web.

Tener un servidor con las siguientes vulnerabilidades encontradas, presenta varios riesgos para la organización, poniendo en compromiso la integridad, confidencialidad y disponibilidad de los datos.





CVE-2023-44487:

· Puntuación CVSS: 7.5

· El protocolo HTTP/2 permite una denegación de servicio (consumo de recursos del servidor) porque la cancelación de solicitudes puede restablecer muchas transmisiones rápidamente, como se explotó en la naturaleza entre agosto y octubre de 2023.

CVE-2010-2730:

· Puntuación CVSS: 9.3

· Descripción: Permite a atacantes remotos ejecutar código arbitrario a través de encabezados manipulados en una solicitud, también conocida como "Request Header Buffer Overflow Vulnerability".

CVE-2010-1899:

· Puntuación CVSS: 4.3

· Descripción: Permite a atacantes remotos causar una denegación de servicio (caída del a través de una solicitud manipulada, relacionada con asp.dll, también conocida como

"IIS Repeated Parameter Request Denial of Service Vulnerability".

CVE-2010-3972:

· Puntuación CVSS: 10.0

· Descripción: Permite a atacantes remotos ejecutar código arbitrario o causar una denegación de servicio a través de un comando FTP manipulado, también conocida como "IIS FTP Service Heap Buffer Overrun Vulnerability".

de seguridad periódicas para identificar y abordar nuevas vulnerabilidades.

CVE-2022-41742:

· Puntuación CVSS: 6.5

· Una vulnerabilidad clasificada como crítica fue encontrada en Nginx Open Source, Open Source Subscription y Plus (Web Server). Una función desconocida del componente ngx_http_mp4_module es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Los efectos exactos de un ataque exitoso no son conocidos. El resumen de CVE es:

La vulnerabilidad fue publicada el 2022-10-20 con identificación K28112382 (confirmado). El advisory puede ser descargado de support.f5.com. La vulnerabilidad es identificada como CVE-2022-41742. No se conocen los detalles técnicos ni hay ningún exploit disponible.

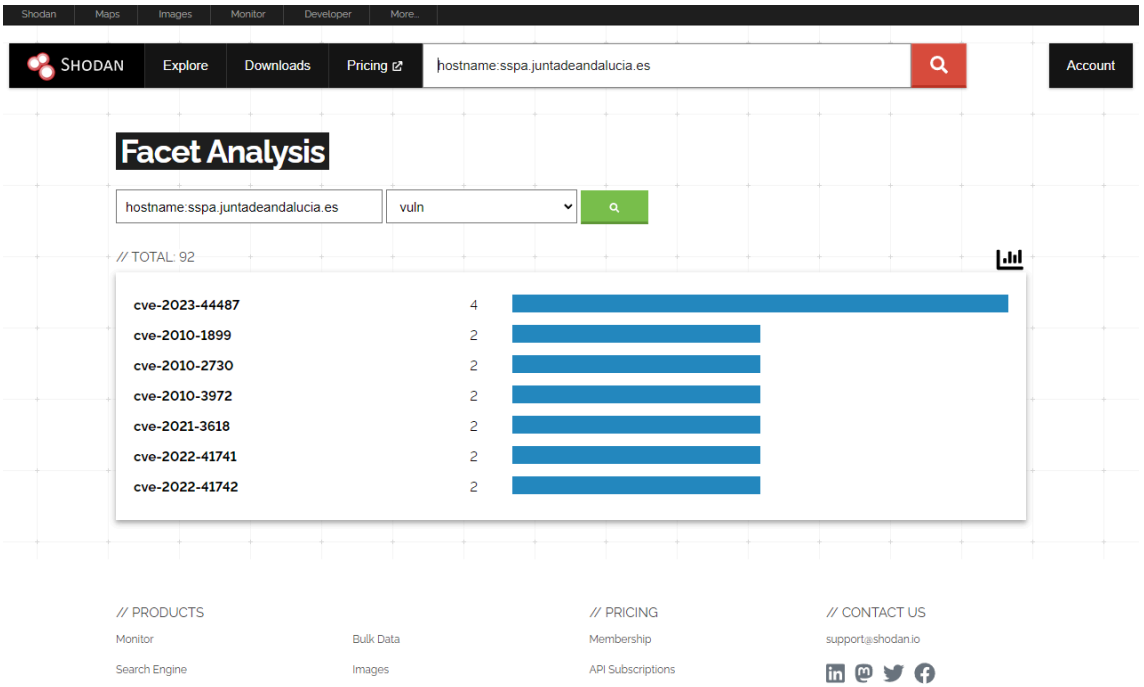
Una actualización elimina esta vulnerabilidad.

CVE-2022-41741:

· Puntuación CVSS: 7.3

Una vulnerabilidad clasificada como crítica fue encontrada en Nginx Open Source, Open Source Subscription y Plus (Web Server). Una función desconocida del componente ngx_http_mp4_module es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Los efectos exactos de un ataque exitoso no son conocidos. El resumen de CVE es:

La vulnerabilidad fue publicada el 2022-10-20 con identificación K81926432 (confirmado). El advisory puede ser descargado de support.f5.com. La vulnerabilidad es identificada como CVE-2022-41741. No se conoce los detalles técnicos ni hay ningún exploit disponible.

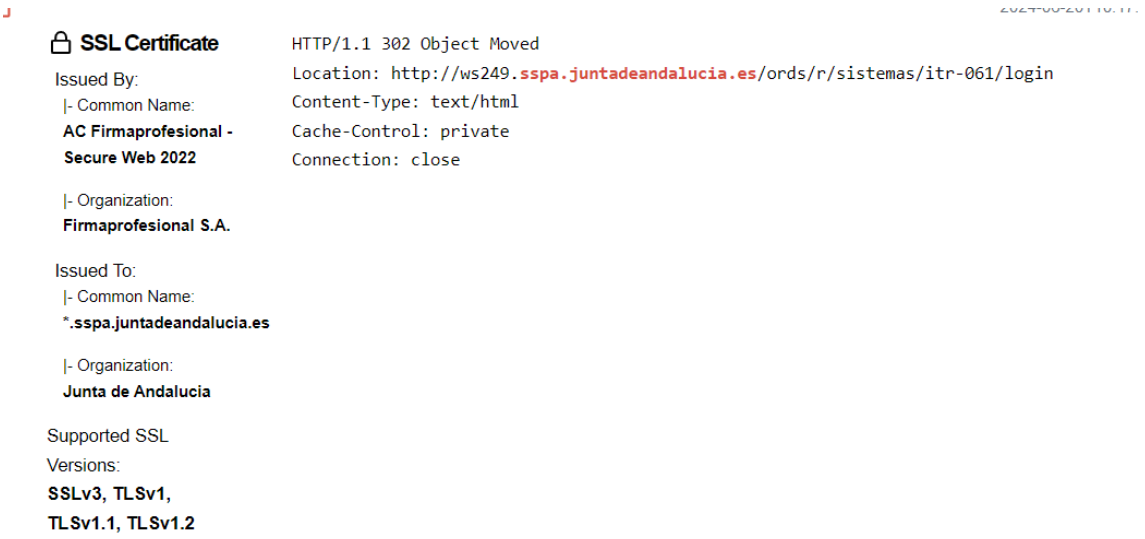


Certificados SSL y Redirecciones HTTP :

- **Certificado SSL:** Emitido por Firmaprofesional S.A. para el dominio *.sspa.juntadeandalucia.es. Soporta SSLv3, TLSv1, TLSv1.1 y TLSv1.2.

- **Redirección HTTP:** Código 302 indicando movimiento temporal de recursos, lo que puede ser una potencial vulnerabilidad para ataques de phishing.

Esta información fue obtenida a partir de la herramienta Shodan como se muestra continuación:



Esta información fue obtenida a partir de la herramienta FOCA como se muestra continuación:

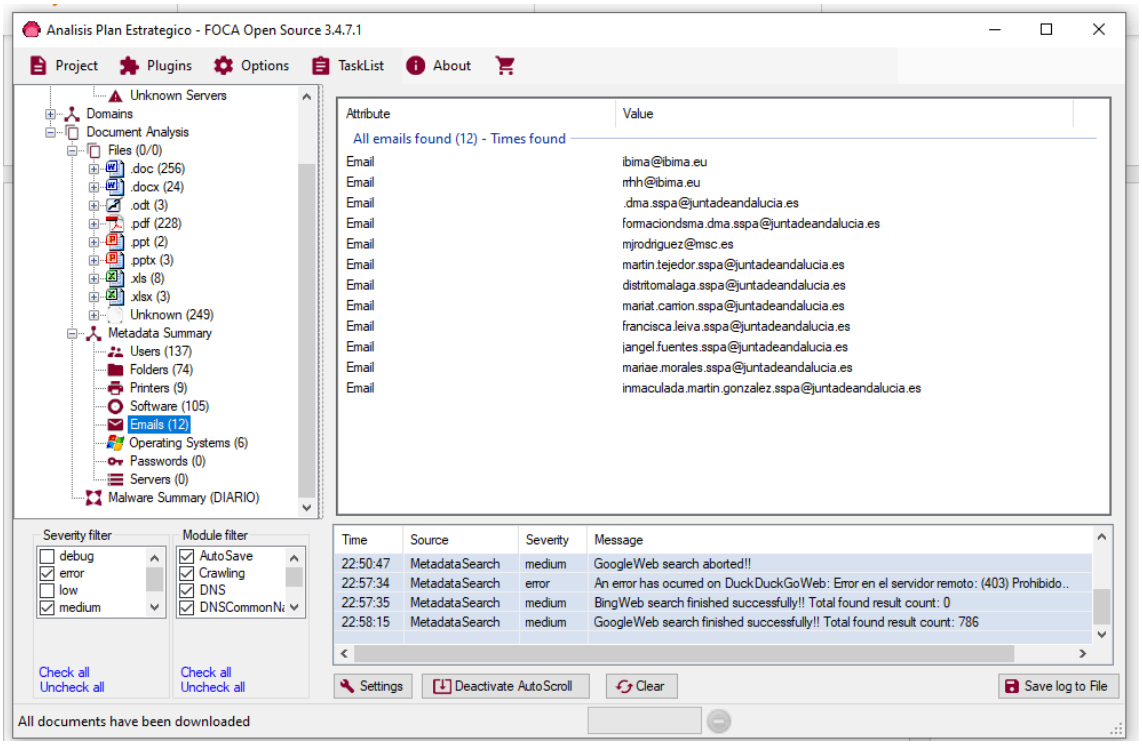
Correos Electrónicos y Direcciones IP Comprometidos:

- Se identificaron correos electrónicos maliciosos comprometidos pertenecientes al dominio del SAS.

Correos Electrónicos Encontrados:

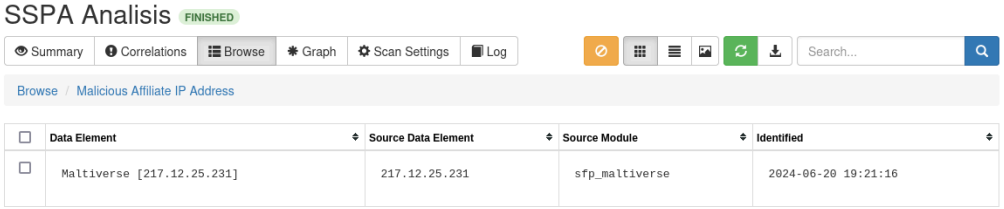
1. **ibima@ibima.eu**
2. **rtnh@ibima.eu**
3. **dma.sspa@juntadeandalucia.es**
4. **formaciondma.dma.sspa@juntadeandalucia.es**

5. **mjrodriguez@msc.es**
6. **martin.tejedor.sspa@juntadeandalucia.es**
7. **distritomalaga.sspa@juntadeandalucia.es**
8. **marit.carrion.sspa@juntadeandalucia.es**
9. **francisca.leiva.sspa@juntadeandalucia.es**
10. **jangel.fuentes.sspa@juntadeandalucia.es**
11. **mariae.morales.sspa@juntadeandalucia.es**
12. **inmaculada.martin.gonzalez.sspa@juntadeandalucia.es**

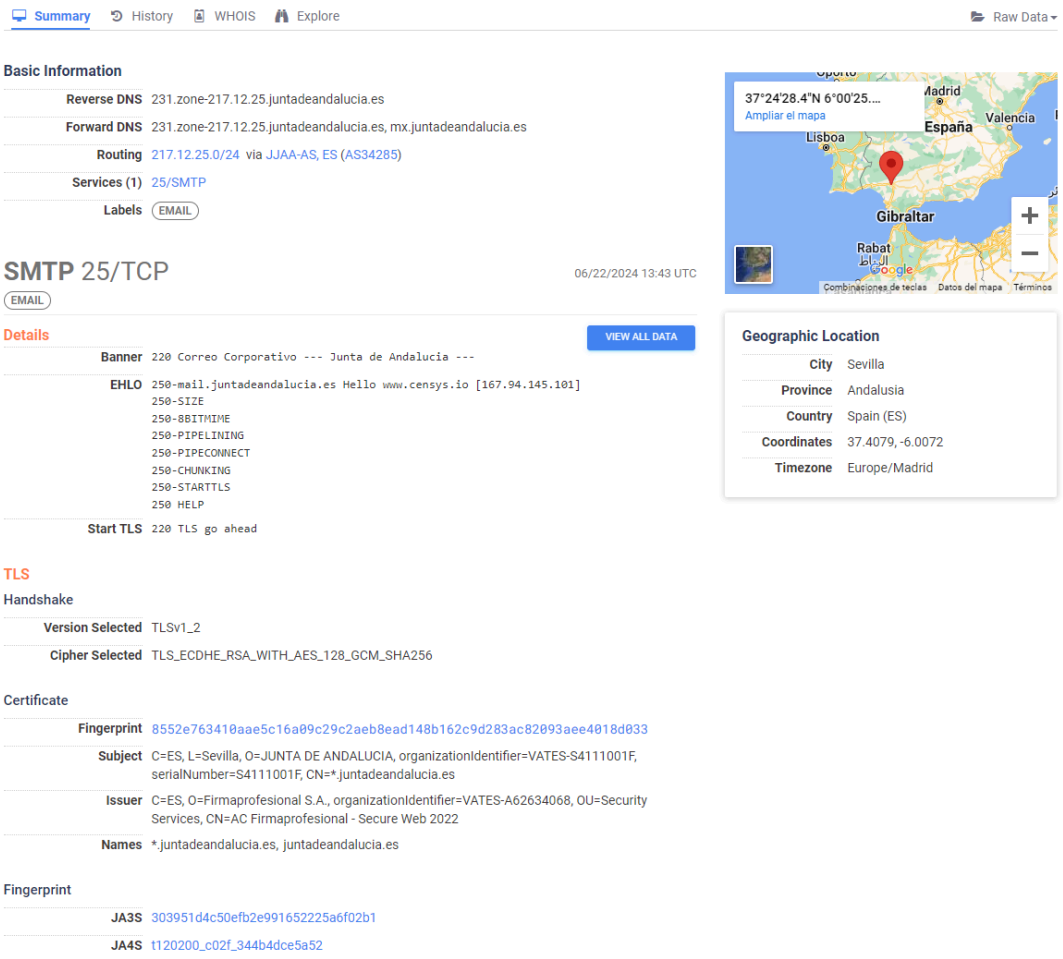


La dirección IP 217.12.25.231 está asociada con actividades maliciosas.

Esta información fue obtenida a partir de la herramienta SpiderFoot como se muestra continuación:



Tras revisar la IP en Censys, podemos ver que se trata de SMTP (Protocolo para transferencia simple de correo) de un servicio de correo corporativo de la Junta de Andalucía.

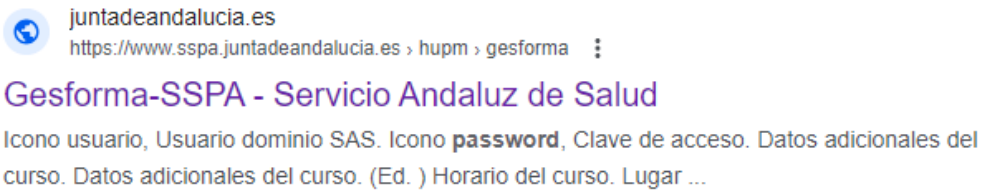


Puntos de acceso donde se manejan contraseñas y credenciales de usuario:

- **Páginas de Restablecimiento de contraseñas**: Permite a los usuarios del sistema reiniciar sus contraseñas a través de un enlace enviado por correo electrónico.

  Esta información fue obtenida mediante el Google Dork site:sspa.juntadeandalucia.es "password" para identificar páginas relacionadas con contraseñas.

- **Plataforma de Gestión de Formación**: Utilizada por los empleados del SAS. La página también utiliza HTTPS para proteger las credenciales de acceso (usuario y contraseña).



Análisis de Vulnerabilidades:

- La infraestructura del SAS presenta los siguientes puertos abiertos (**80, 443, 22, 53, 1443, 8442, 9443, 8443**).

Updated	Module	Source	Data
2024-06-20 12:52:33	sfp_censys	217.12.20.193	217.12.20.193:443
2024-06-20 12:52:33	sfp_censys	217.12.20.193	217.12.20.193:80
2024-06-20 12:56:09	sfp_censys	217.12.20.208	217.12.20.208:22
2024-06-20 12:54:03	sfp_censys	217.12.20.68	217.12.20.68:53
2024-06-20 12:55:39	sfp_censys	217.12.22.194	217.12.22.194:1443
2024-06-20 12:55:15	sfp_censys	217.12.22.222	217.12.22.222:8442
2024-06-20 12:55:15	sfp_censys	217.12.22.222	217.12.22.222:9443
2024-06-20 12:55:27	sfp_censys	217.12.22.223	217.12.22.223:8443

- Las páginas de restablecimiento de contraseñas y gestión de formación pueden sufrir ataques, por lo que es crucial que tenga medidas adecuadas para proteger los datos de los usuarios.
- Aunque las páginas utilizan HTTPS para proteger la información de los usuarios pueden sufrir ataques donde un atacante puede descubrir si un nombre de usuario o correo electrónico está registrado en el sistema.

5. SOLUCIONES O RECOMENDACIONES

El análisis realizado al Servicio Andaluz de Salud (SAS) ha revelado una serie de vulnerabilidades críticas y áreas de mejora que deben ser abordadas con urgencia para asegurar la integridad y seguridad del sistema. Las recomendaciones principales serían:

Actualización de SSL/TLS:

- Deshabilitar SSLv3 y TLSv1.0 debido a vulnerabilidades conocidas.

Revisión de Redirecciones:

- Analizar y asegurar las URL de redirección para protegerlas contra ataques de phishing.

Monitoreo y Auditoría de Infraestructura:

- Implementar un monitoreo continuo de la infraestructura IP y DNS.
- Realizar auditorías de seguridad periódicas para identificar y mitigar vulnerabilidades.

Protección de Información Personal:

- Revisar y eliminar información personal y correos electrónicos antes de publicar documentos.

Medidas de Seguridad Adicionales:

- Utilizar autenticación multifactor (MFA) como por ejemplo doble verificación a través de SMS, para proteger cuentas de correo y otros servicios
- Implementar políticas de control de acceso y gestión de identidades robustas.
- Asegurar configuraciones seguras en servidores y servicios expuestos.

- Sustitución del servicio web basado en la arquitectura Microsoft IIS HTTPD V7.5. a otra con soporte actual, ya que esta está obsoleta y no consta de actualizaciones de seguridad.

- Para los puertos abiertos “80, 443, 22, 53, 1443, 8442, 9443, 8443” , se recomienda revisar la necesidad de que permanezcan todos ellos abiertos.

- Se recomienda aplicar parches y actualizaciones de seguridad (CVE) para así poder eliminar dichas vulnerabilidades.

Educación y Concienciación:

- Se encontraron direcciones de correo electrónico expuestas públicamente, lo que puede conducir a ataques de phishing y otros tipos de ingeniería social. Es crucial implementar prácticas de protección de la información y sensibilizar a los empleados sobre los riesgos de compartir información sensible públicamente.
- **Vulnerabilidades en Actualizaciones**: Se detectaron varias vulnerabilidades relacionadas con actualizaciones de software, conocidas como CVEs (Common Vulnerabilities and Exposures). Estas vulnerabilidades, si no se abordan, pueden ser explotadas por atacantes para obtener acceso no autorizado y comprometer el sistema. Es imperativo mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- **Sistemas Obsoletos**: La presencia de sistemas y software obsoletos representa un riesgo significativo. Estos sistemas no solo carecen de las últimas mejoras de seguridad, sino que también pueden no recibir soporte técnico, lo que aumenta su vulnerabilidad a ataques. La migración a versiones más recientes y soportadas es esencial para reducir estos riesgos.
- **Subdominios**: La detección de subdominios mal configurados o innecesarios puede ser una puerta de entrada para atacantes. La gestión y monitoreo adecuado de subdominios es fundamental para asegurar que no existan puntos débiles en la infraestructura web.