Campaña de ransomware en entidades sanitarias: Vigilancia y Recomendaciones.

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el Centro Criptológico Nacional, CCN-CERT, informa de un **incidente de *ransomware*** que está afectando especialmente a **entidades del sector sanitario.**

Se trata del ***ransomware* Hive** involucrado en numerosos incidentes desde mediados de este año. Su modus operandi es similar al empleado hoy en día por otros grupos de atacantes que hacen uso de *ransomware*: una vez comprometida la organización exfiltran datos personales y proceden con el cifrado de los mismos para, posteriormente, presionar a sus víctimas mediante la, cada vez más común, doble extorsión.

El **vector de entrada** utilizado por los atacantes **es el correo electrónico**, generalmente, mediante el uso de ***spear phishing* con adjuntos maliciosos**. Para la ejecución de sus TTPs (Tácticas Técnicas y Procedimientos) los atacantes suelen orquestar sus acciones desde herramientas de control remoto tales como el archiconocido CobaltStrike así como el software comercial Connectwise/ScreenConnect, herramienta legítima utilizada en los últimos años por diversos grupos de atacantes.

Debido a los ataques que diversas entidades del sector sanitario están recibiendo mediante este código dañino, la Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones ruega encarecidamente **extremar la vigilancia y las precauciones** ante la posibilidad de ser abordados por este *ransomware*. Llamamos vuestra atención sobre la necesidad de aplicar las siguientes recomendaciones.

Recomendaciones

A nivel usuario:

Preste atención a los correos electrónicos que recibe:

- Compruebe el dominio del correo remitente y que su nombre coincide con su cuenta de correo electrónico (nombre y dominio).
- Desconfíe de los correos electrónicos cuyo texto esté mal redactado o con faltas de ortografía.
- Evite abrir archivos adjuntos si se desconoce al remitente o no se espera el documento.
- Preste atención a la sintaxis de los enlaces a páginas web que le lleguen por correo electrónico. Una letra puede marcar la diferencia.
- Si observa alguna anomalía en un correo electrónico, contacte con el remitente a través de otro canal (ej. Teléfono) para comprobar la autenticidad del mensaje.

Sea especialmente cuidadoso con la navegación web.

- Navegue solo por sitios web fiables y necesarios para el desempeño de su trabajo

A nivel técnico:

Paso 1. Mantener los dispositivos y aplicaciones actualizados: Contar con la última versión del navegador, sistema operativo, software o aplicación que utilicemos contribuirá a reforzar nuestra seguridad

---

Paso 2. Se debe **verificar** que el equipo está protegido con el **antivirus corporativo *Symantec Endpoint Protection***, dispone de las **últimas firmas publicadas y** tiene el **módulo IPS instalado y habilitado**.

Paso 3. Es **altamente recomendable verificar que está instalado** el **Agente EDR de Crowdstrike**. En caso contrario, puede obtener el procedimiento de instalación **aquí**.

Paso 4. Incluir IOCs (Indicadores de Compromiso) en proxies y firewalls provinciales

Actualmente desde la USTIC estamos trabajando en un sistema de implementación automática de IOC para el ámbito de la seguridad corporativa en distintas líneas de servicios de seguridad (proxies, firewalls, EDR...)

Los proxies **SQUID** son los primeros elementos de seguridad en los que se están pilotando esta solución, mediante una servicio de descarga diaria de los IOC del repositorio de Andalucia-CERT e integración en listas de denegación de Ip y dominios.

Este repositorio de Andalucia-CERT, a su vez, proviene de los análisis de la cibertinteligencia de la herramienta **REYES** (CC N-CERT).

Los **IOC que recomienda CCN-CERT**, que corresponden a indicadores de explotación de la vulnerabilidad, ya están incluidos en REYES, por lo que **se recomienda que se traten de manera automática** a través de la ejecución del script preparado para tal efecto.

El **script de configuración para la descarga e incorporación de los IOCs automática** es el siguiente: ScriptIOCautomatic .sh . En este script hay que sustituir <*password_ftp*> por la clave. Contactar con ustic.stic.sspa@juntadeandalucia.es para el envío de dichas credenciales.

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por su atención. Reciba un cordial saludo,

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud