Identificador
[COLCERT- AL-0531- 0021]

2023/05/31 | **Alerta de Seguridad Digital**

.**TLP:CLEAR**

Contexto Ataques de Seguridad Digital a Entidades de Gobierno

Contexto

Los ataques realizados por grupos dedicados a actividades disruptivas en el ciberespacio, entre los que se destacan “SiegedSec”, “GhostSec”, “Anonymous”, “LockBit 3.0”, “Conti” y “Medusa”, en lo que sería una represalia por la captura por parte de autoridades colombianas de uno de sus lideres denominado 'Org0n' y que tendría por objetivo la búsqueda de vulnerabilidades en infraestructuras del Estado a nivel nacional y territorial, buscando obtener un beneficio económico y afectar el prestigio, legitimidad del Estado y la estabilidad institucional.

Estos ataques han logrado, afectar la disponibilidad de servicios, exfiltrar información, acceso a dispositivos, compromiso de credenciales de usuario, así las cosas, es altamente probable que continúen con estos ataques y que sigan siendo efectivos sobre entidades del orden nacional, territorial y empresas que carecen de una postura y estrategia de seguridad digital. Es importante resaltar que la oleada de ataques no se encuentra únicamente ligada a esta campaña, y por ello compartimos información adicional que puede ayudar a prevenir incidentes de alto impacto en organizaciones y entidades del sector público

Proyecciones

Los ataques cibernéticos a las instituciones y organizaciones, se vienen enfocando en la explotación de vulnerabilidades conocidas, que no han sido corregidas a pesar de existir actualizaciones publicadas por los fabricantes de equipos, así mismo la obsolescencia tecnológica y aplicaciones legadas que soportan procesos misionales en entidades y privados, aumentan la superficie de exposición, estas debilidades permiten a los ciberdelincuentes ingresen a los sistemas de información e infraestructuras tecnológicas fácilmente, logrando tener acceso a los dispositivos para comprometerlos, y a la información para luego ser exfiltrada, puesta en venta y publicada en redes para iniciar campañas de desacreditación institucional.

Se ha venido detectando que los nuevos actores de amenazas que vienen operando en América Latina, como “Royal Ransomware Group”, utilizan no solo técnicas de ataque conocidas, sino que evolucionan y que permiten explotar vulnerabilidades a sistemas Windows, Linux, dispositivos de comunicación y equipos activos a medida que son publicados en internet.

Acorde con lo señalado por CISA en se sabe *“que esta variante, que utiliza su propio programa de encriptación de archivos personalizado, evolucionó a partir de iteraciones anteriores que usaban "Zeon" como cargador. Después de obtener acceso a las redes de las víctimas, los actores de Royal desactivan el software antivirus y filtran grandes cantidades de datos antes de finalmente implementar el ransomware y cifrar los sistemas.*

… En los incidentes observados, los actores de Royal no incluyen montos de rescate ni instrucciones de pago como parte de la nota de rescate inicial. En cambio, la nota, que aparece después del cifrado, requiere que las víctimas interactúen directamente con el actor de la amenaza a través de un.onionURL (accesible a través del navegador Tor).

En el siguiente link se pueden encontrar los IoC relacionados a la temática:

https://www.cisa.gov/sites/default/files/2023-03/aa23-061a.stix__0.xml

Se prevé que estos grupos masifiquen sus ataques afectando Infraestructura Critica Cibernética – ICC del país, aprovechándose de las vulnerabilidades y configuraciones incorrectas de los sistemas de control industrial (ICS) y los dispositivos de tecnología operativa (OT) expuestos a Internet.

La constante evolución de las técnicas, tácticas y procedimientos de los actores de amenazas hace necesario que las entidades y organizaciones puedan identificar qué actores de amenazas potenciales pueden atacar sus infraestructuras tecnológicas y para ello pueden emplear la implementación del marco de trabajo de MITRE ATT&CK. Ver más información: https://www.cisa.gov/news-events/news/helping-cyber-defenders-decide-use-mitre-attck.

De la misma forma, las entidades y empresas deben establecer una postura de seguridad digital orientada a la prevención, protección y reacción para la gestión de sus incidentes, y para ello, una de las estrategias que deben adoptar es conocer el ciclo de vida de los ataques (Cyber Kill Chain), lo cual permite detectar, detener, e interrumpir las acciones de los actores maliciosos, gracias a la identificación de indicadores de ataque – IoA.

Ante los ataques a entidades de gobierno y privados, invitamos a los interesados a conocer y utilizar el apoyo y la coordinación que pueden obtener con el COLCERT, para dar los primeros pasos en el restablecimiento de las operaciones, así como en el ciclo de gestión de los incidentes; en este sentido al final de este informe se encuentran los canales de comunicación habilitados para la comunicación que sea requerida.

Como respuesta a las condiciones mencionadas, se dejan algunas recomendaciones para que sean revisadas por los equipos técnicos y se tomen las respectivas acciones de evaluación y aseguramiento de la infraestructura.

Acciones inmediatas

- Implementar el doble factor de autenticación en las cuentas de correo. En el siguiente link encontrara información sobre la configuración de MFA en Office 365:

  https://learn.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

  Evitar a toda costa compartir credenciales (usuario/contraseña) de cuentas de correo corporativas, así mismo evitar utilizar éstas en redes sociales, apertura de servicios en línea, servicios financieros externos a la entidad, entre otras. En el siguiente link encontrara una herramienta en línea para crear contraseñas seguras.

  https://support.microsoft.com/es-es/topic/use-generador-de-contrase%C3%B1as-para-crear-contrase%C3%B1as-m%C3%A1s-seguras-en-microsoft-edge-e9247e35-684b-4114-bb5e-fdea3e4ae3ff#:~:text=C%C3%B3mo%20funciona%20el%20generador%20de,segura%20en%20un%20men%C3%BA%20desplegable.

- Actualizar la matriz de riesgos y ajustar los controles para proteger activos vulnerables, sistemas y aplicaciones legadas.
- Actualizar a su última versión los sistemas de gestión de contenido CMS (Content Management System) y realizar el afinamiento a la configuración para evitar exponer información de configuración a través de directorios.
- Validar el despliegue de los agentes de antivirus en computadores y servidores, en la consola para validar el cubrimiento total de la infraestructura tecnológica de la entidad.
- Establecer y operacionalizar procedimientos detallados para la generación de copias de seguridad
- Realizar actualización de seguridad a sistemas operativos a computadores, servidores, equipos activos de red y seguridad informática.
- Realizar un monitoreo a los eventos de seguridad y logs de las plataformas (FW, IDS/IPS, DA, AV, WAF, Balanceador, BD, SW) para identificar Indicadores de Amenaza – IoA.
- Implementación protocolo autenticación como SPF, DKIM y DMARC para su dominio de correo.

Recomendaciones Generales

- Establecer una política de gestión de contraseñas.
- Establecer una política de control de acceso.
- Actualizar el inventario de activos de información incluyendo los de nube.
- Actualizar la matriz de riesgos de la entidad contemplando las infraestructuras on-premises y de nube.

- Realizar análisis de vulnerabilidades plataformas expuestas en internet y realizar planes de mitigación de éstas.
- Actualizar y operacionalizar el Plan de Recuperación ante Desastres DRP.
- Realizar pruebas de continuidad de la operación, para cada una de las copias de seguridad generadas.
- Actualizar o implementar soluciones de antivirus para tener mayor visibilidad como soluciones EDR (Endpoint Detection and Response) para proteger dispositivos y XDR (Extensive Detection and Response) para proteger redes, aplicaciones y datos
- Implementación de DNSSEC, en su sistema de Dominio, para garantizar la confiabilidad y credibilidad de éste en la entidad.

Cumplimiento Normativo de Seguridad Digital

- Dar cumplimiento al habilitador transversal de seguridad y privacidad, establecido en la Política de Gobierno Digital - Decreto 767 de 2022, con la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.
- Dar cumplimiento a lo establecido en la Resolución 500 del 2021 del MinTIC, sobre la implementación de una estrategia de seguridad digital para la entidad, así como la implantación de un procedimiento de gestión de incidentes.
- Establecer frente a los documentos que genera, obtiene, adquiera, transforme y controle la entidad, que éstos cuente con las siguientes características; Información, pública, pública clasificada y pública reservada, lo anterior en cumplimiento a la ley 1712 del 2014
- Establecer la política de protección de datos personales – Ley 1581 del 2012. que garantice la protección de los datos sensibles de los usuarios.

Referencias y fuentes de información

https://twitter.com/FalconFeedsio/status/1662324942921248769
https://twitter.com/cyberthint/status/1663190085804670978?t=i1zd7BclE_1u_iOBii4JQQ&s=08
http://muchohacker.lol/
https://thecyberexpress.com/colombian-radio-broadcasts-cyber-attack/
https://www.cisa.gov/news-events/news/helping-cyber-defenders-decide-use-mitre-attck
https://blog.cyble.com/2023/05/31/evolving-threat-landscape-of-hacktivism-in-colombia/
https://www.cisa.gov/news-events/cybersecurity-advisories

Canales de Atención

Si tiene desea reportar un incidente de seguridad digital, puede comunicarse con el COLCERT, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT