ALERTA DE SEGURIDAD CIBERNÉTICA

El CSIRT de Gobierno hace un llamado a todas las instituciones del Estado a estar alertas y tomar las medidas de precaución necesarias ante el grupo de ransomware ruso Conti. Esto, debido a los ataques informáticos que afectaron a las instituciones públicas de Perú y Costa Rica en las últimas semanas.

Antecedentes de los ciberataques

En abril de 2022, el gobierno de Costa Rica confirmó haber sido víctima del ransomware Conti, el cual afectó, en su mayoría, al Ministerio de Hacienda y a entidades como la Junta Administrativa del Servicio Eléctrico de la provincia de Cartago (Jasec), el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones; el Ministerio de Trabajo y Seguridad Social; al Instituto Meteorológico Nacional (IMN), a Radiográfica Costarricense (Racsa) y la Caja Costarricense del Seguro Social (CCSS). Debido a esta situación, el gobierno se vio obligado a deshabilitar varios servicios informáticos y a declarar Estado de Emergencia Nacional desde el 8 de mayo.

Poco tiempo después, a principios de mayo, el mismo grupo ruso informó a través de un blog en la dark web que la Dirección General de Inteligencia de Perú había sido atacada por Conti. En esta ocasión, los delincuentes aseguran haber accedido a la red del organismo y haber realizado copias de información sensible, accediendo así infraestructura crítica, incluida las redes de agua y electricidad.

Sobre el ransomware Conti

Conti se considera una variante de modelo de ransomware como servicio (RaaS), es muy destructiva y funciona bajo la modalidad de doble extorsión, poniendo en riesgo la información y la reputación de la entidad afectada. Según la investigación de Cybereason, “Conti no sólo encripta los archivos en el host infectado, sino que también se propaga a través de SMB y encripta archivos en diferentes hosts, lo que podría comprometer el toda la red. La rutina de encriptación rápida tarda solo unos segundos o minutos, debido al uso de subprocesos múltiples, lo que también hace que sea muy difícil detenerla una vez que se inicia la rutina de encriptación”.

Al igual que la mayoría de los ataques de ransomware, Conti logra acceder a las redes de las instituciones por distintos medios:

1. Campañas de phishing, donde adjuntan documentos maliciosos en formato Word o envían enlaces. En ambos casos buscan que la persona descargue un malware como TrickBot o aplicaciones legítimas.
2. Buscan explotar vulnerabilidades.

3. Ataques sobre equipos con el servicio de RDP expuesto a Internet.

Recomendaciones

Ante el impacto que han tenido los países afectados por el ransomware Conti, el CSIRT de Gobierno solicita a las instituciones del Estado tomar las medidas de mitigación necesarias. Para ello, entregamos las siguientes recomendaciones:

- Implementar segmentación de red entre redes y funciones departamentales.
- Exigir autenticación multifactor a quienes acceden de forma remota a las redes.
- Activar filtros de spam para evitar que correos de phishing lleguen a los funcionarios de la organización, y filtrar los emails que contengan archivos ejecutables.
- Filtrar el tráfico de red para prohibir las comunicaciones de entrada y salida de direcciones IP maliciosas conocidas.
- Implementar bloqueo a las listas de sitios web maliciosos.
- Mantener actualizados los sistemas operativos, aplicaciones y firmware en los activos de la red. Considerar el uso de un sistema centralizado de administración de parches.
- Realizar escaneos regulares de antivirus/antimalware de los activos de la red, actualizar periódicamente las firmas.
- Monitorear o bloquear las conexiones entrantes de nodos de salida de redes Tor y otros servicios de anonimización a direcciones IP y puertos por los cuales no se esperan conexiones externas.
- Auditar y monitorear periódicamente cuentas de usuarios de administración.
- Auditar y monitorear la creación de cuentas de usuarios, donde sean usuarios legítimos.
- Eliminar aplicación que no se utilicen, evitando explotación de vulnerabilidades.
- Implementar capacitaciones y concientización a los funcionarios sobre ataques de phishing.
- Generar políticas de respaldos de la información, realizar pruebas periódicas, que los respaldo se encuentren en segmentos separados y en diferentes lugares físicos.

En caso de ser infectado, el CSIRT de Gobierno recomienda:

- Desconectar de la red los aparatos afectados e informar del hecho rápidamente al CSIRT de Gobierno. Esta desconexión debe ser física en caso de no poder hacerse de otra forma.
- Solo se recomienda apagar los aparatos infectados de la corriente cuando no hay otra forma de desconectarlos de la red, ya que esto eliminará potencial evidencia guardada en la memoria volátil.
- Asegurar que todos los discos compartidos y de red están desconectados, ya sean wifi o alámbricos.
- Asegurar los respaldos y que los datos de respaldo estén desconectados de las redes y seguros. Si es posible, se debe escanear sus datos de respaldo con un programa antivirus para asegurarse de que esté libre de malware.

- Apagar otros computadores y aparatos que se encuentren en la misma red del equipo infectado. Si no existe segmentación o protección entre segmento se red, se recomienda apagar todos los equipos que no se encuentren infectados hasta estar seguro que la amenaza se encuentre controlada.
- La recuperación de sistemas debe ser hecha según su criticidad para la operación de la institución.
- Se recomienda que la institución afectada tome las acciones judiciales pertinentes ante los organismos que corresponda.
- Es importante, después de haber recuperado la funcionalidad y vuelto a la normalidad (o tanto como fuera posible), hacer un análisis de lo sucedido y cómo evitarlo en el futuro.

Más detalles sobre Conti aquí:

https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware

https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

https://attack.mitre.org/software/S0575/