ALERTA DE SEGURIDAD CIBERNÉTICA

RANSOMWARE AVOSLOCKER APUNTA A MÁQUINAS VIRTUALES VMWARE

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comunica el reciente surgimiento de una campaña con una variante Linux del ransomware conocido como **AvosLocker**, que apunta a las máquinas virtuales VMware ESXi y a los archivos VMFS (Virtual Machine File System). Se conoce de al menos una víctima que recibió la exigencia de US$ 1 millón como extorsión a cambio de desencriptar sus archivos y no divulgar su información confidencial[1].

Atacar a las máquinas virtuales es cada día más valioso para los ciberdelincuentes, ya que cada día más empresas las usan en sus operaciones. Además, basta un solo comando para encriptar varios servidores. Ya desde octubre se han apreciado campañas similares que cifran tanto sistemas Linux en general como específicamente los de VMware, por parte de bandas que incluyen a REvil, Babuk, Mespinoza, GoGoogle, DarkSide, RansomExx/Defray y Hello Kitty.

Modo de operación

Esta campaña de ransomware no está explotando una vulnerabilidad específica de los productos VMware, sino que usando Proxyshell para aprovechar vulnerabilidades conocidas en sistemas de Microsoft[2], como CVE-2021-34473[3], CVE-2021-31206, CVE-2021-34523 y CVE-2021-31207[4].

Cuando es lanzado en un sistema Linux, **AvosLocker** baja todas las máquinas ESXi en el servidor. Cuando empieza a trabajar en el sistema comprometido, el ransomware agrega la extensión .avoslinux a los archivos encriptados. También deja notas indicando que no se apaguen los computadores para evitar la corrupción de sus datos y que visiten un sitio de la red Tor para tener más datos sobre cómo pagar el rescate.

De acuerdo con Sophos[5], para poder desplegar su ransomware, los atacantes usan la herramienta PDQ Deploy, con scripts que pueden deshabilitar en segundos los productos de seguridad que se pueden ejecutar en modo seguro, deshabilitar Windows Defender y permitir que AnyDesk del delincuente se ejecute en modo seguro. Los scripts también conectan al controlador de dominio del objetivo para acceder a él de forma remota y ejecutar el ransomware.

Información oficial entregada por VMware, que comparte además indicadores de compromiso: https://blogs.vmware.com/security/2022/02/avoslocker-modern-linux-ransomware-threats.html

---

[1] https://www.bleepingcomputer.com/news/security/linux-version-of-avoslocker-ransomware-targets-vmware-esxi-servers/
[2] https://blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers/
[3] https://www.csirt.gob.cl/media/2021/07/9VSA21-00466-01.pdf
[4] https://www.csirt.gob.cl/media/2021/05/9VSA21-00443-01.pdf
[5] https://www.sophos.com/en-us/press-office/press-releases/2021/12/avoslocker-ransomware-uses-anydesk-in-safe-mode-to-launch-attacks

Sugerencias para no ser víctima del ransomware

Listado aquí: https://www.csirt.gob.cl/recomendaciones/proteccion-del-ransomware/

- Diseñar y difundir dentro de la organización planes de contingencia ante ransomware, incluyendo detallar claramente quiénes estarán encargados de los procesos que involucra la respuesta al incidente y la recuperación cuanto antes de los servicios
- Realizar respaldos regularmente los que deben mantenerse separados del resto de la red.
- Llevar a cabo frecuentemente ejercicios de respaldo.
- Mantener equipos y software autorizados. Conviene activar actualizaciones automáticas o recordatorios periódicos.
- Utilizar antivirus y antimalware de proveedores de confianza.
- Evitar caer en el phishing, no haciendo clic en enlaces de proveniencia desconocida (más consejos: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-caer-en-el-phishing-durante-la-operacion-renta/)

Si se fue víctima de ransomware

- No pagar el rescate por los datos secuestrados. No solo para no financiar a lis ciberdelincuentes, sino porque nada garantiza que se recupere realmente la información secuestrada.
- Desconectar inmediatamente los equipos afectados del resto de la red, y desconectar a su vez de aquellos cualquier memoria externa que pudieran tener conectadas.
- Revisar los logs en búsqueda de eventos sospechosos.
- Denunciar el hecho ante la Policía de Investigaciones.
- Alertar al CSIRT de Gobierno al email: soc@interior.gob.cl

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.03.17 16:45:36 -03'00'