Devel
CYBERSECURITY REDEFINED

Guatemala • El Salvador • Honduras • R. Dominicana

AvosLocker Ransomware

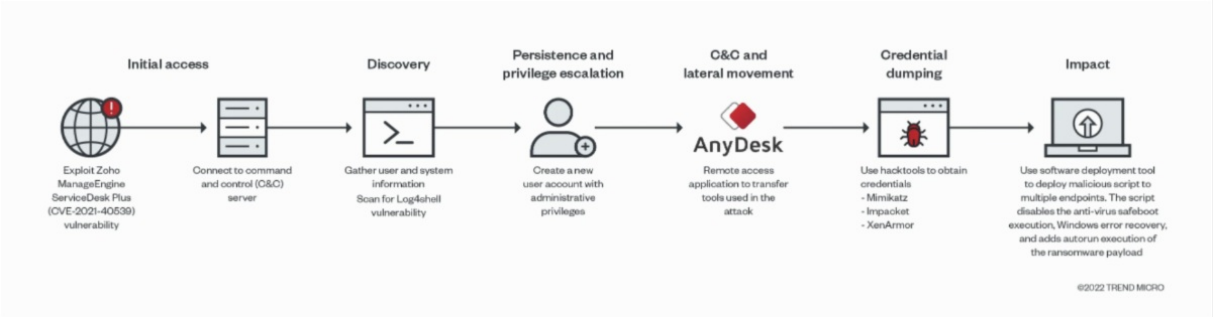
Investigadores han revelado una nueva variante de este ransomware, que desactiva las soluciones antivirus para evadir la detección.

AvosLocker, una de las familias de ransomware más nuevas para llenar el vacío dejado por REvil , se ha relacionado con una serie de ataques dirigidos a infraestructura crítica en los EE.UU. incluidos los servicios financieros e instalaciones gubernamentales.
Un grupo basado en afiliados de ransomware como servicio (RaaS) descubierto por primera vez en julio de 2021, AvosLocker va más allá de la doble extorsión al subastar los datos robados a las víctimas en caso de que las entidades objetivo se nieguen a pagar el rescate.
Otras víctimas objetivo reclamadas por el cartel de ransomware se encuentran en Siria, Arabia Saudita, Alemania, España, Bélgica, Turquía, los Emiratos Árabes Unidos, el Reino Unido, Canadá, China y Taiwán, según un aviso publicado por el FBI en marzo de 2022.

Se cree que el punto de entrada para el ataque se facilitó al aprovechar un exploit para una falla de ejecución remota de código en el software ManageEngine ADSelfService Plus de Zoho (CVE-2021-40539) para ejecutar una aplicación HTML (HTA) alojada en un servidor remoto.

Esto incluye recuperar un shell web ASPX del servidor, así como un instalador para el software de escritorio remoto AnyDesk , el último de los cuales se usa para implementar herramientas adicionales para escanear la red local, finalizar el software de seguridad y eliminar la carga útil del ransomware.

Algunos de los componentes copiados en el punto final infectado son un script Nmap para escanear la red en busca de la falla de ejecución remota de código de Log4Shell (CVE-2021-44228) y una herramienta de implementación masiva llamada PDQ para entregar un script por lotes malicioso a múltiples puntos finales.



Nuestras

Recomendaciones

Las recomendaciones para evitar o minimizar el riesgo de una infección de Malware son:

- Contar con un plan de recuperación de datos para conservar varias copias de datos y servidores considerados como primarios en un area fisica separada o en la nube de ser posible.
- Contar con varios segmentos de red y tener respaldos offline, esto garantiza un menor rango de impacto en caso de ataques de ransomware.
- Instale siempre los parches que sus proveedores de software liberen para contar con la menor cantidad de vulnerabilidades posibles.
- Usar RDP solo cuando sea necesario, asi como los softwares de acceso remoto (AnyDesk, TeamViewer)
- Concientizar a los usuarios en los riesgos y vulnerabilidades emergentes en general (Ransomware, Malware, Phishing)

Ver IOC's **Nota Completa** **Descargar Boletin**

Para un mejor asesoramiento y prevención de amenazas pueden avocarse a nosotros escribiendo a : info@develsecurity.com / soc@develsecurity.com

/ soporte@develsecurity.com.

¡ Con gusto le atenderemos !

GUATEMALA

PBX: + (502) 2307 5700
7ma. avenida 5-45, edificio XPO1 zona 4
nivel 9, Ciudad de Guatemala

EL SALVADOR

PBX: + (503) 2566 5320
Final 105 Av. norte calle Arturo Ambrogi
No. 440 colonia Escalón, San Salvador

HONDURAS

PBX: + (504) 2283 5904
Blv. Morazán, Condominios Centro Morazán
Torre 2, nivel 18 oficina 21804, Honduras

REPÚBLICA DOMINICANA

PBX: +1 (809) 335 4793
Santo Domingo John F. Kennedy 7,
Buenaventura Freites, 10601.T