

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

RANSOMHUB: LA AMENAZA CIBERNÉTICA QUE AUMENTA EN GUATEMALA

22/08/2024

CONTENIDO

| | |
|---------------------------------|---|
| INTRODUCCIÓN | 3 |
| RESUMEN | 5 |
| INDICADORES DE COMPROMISO | 7 |
| NOTICIA COMPLETA | 7 |
| CONTACTOS DE SOPORTE | 8 |

INTRODUCCIÓN

RansomHub, un colectivo de cibercriminales que ha emergido con fuerza en el panorama cibernético, ha puesto a Guatemala en su mira con una serie de ataques altamente sofisticados. Estas incursiones han afectado a diversos sectores, desde finanzas hasta telecomunicaciones, empleando un ransomware de última generación diseñado para evadir las defensas tradicionales y maximizar el daño. La capacidad técnica de RansomHub, combinada con su enfoque en la doble extorsión, ha generado una creciente preocupación entre las empresas guatemaltecas que ahora enfrentan no solo la amenaza de perder el acceso a sus datos, sino también el riesgo de que su información más sensible sea expuesta públicamente.

El ransomware utilizado por RansomHub se distingue por su complejidad, implementando cifrados robustos como AES-256 y RSA-2048, lo que asegura que los datos secuestrados sean prácticamente irrecuperables sin la clave de descryptación adecuada. Además, este malware incorpora técnicas avanzadas de evasión y anti-forense, dificultando su detección y análisis posterior. Ante esta creciente amenaza, es imperativo que las empresas guatemaltecas refuercen sus estrategias de ciberseguridad, adoptando soluciones tecnológicas avanzadas y protocolos que minimicen la posibilidad de ser víctimas de estos ataques devastadores.

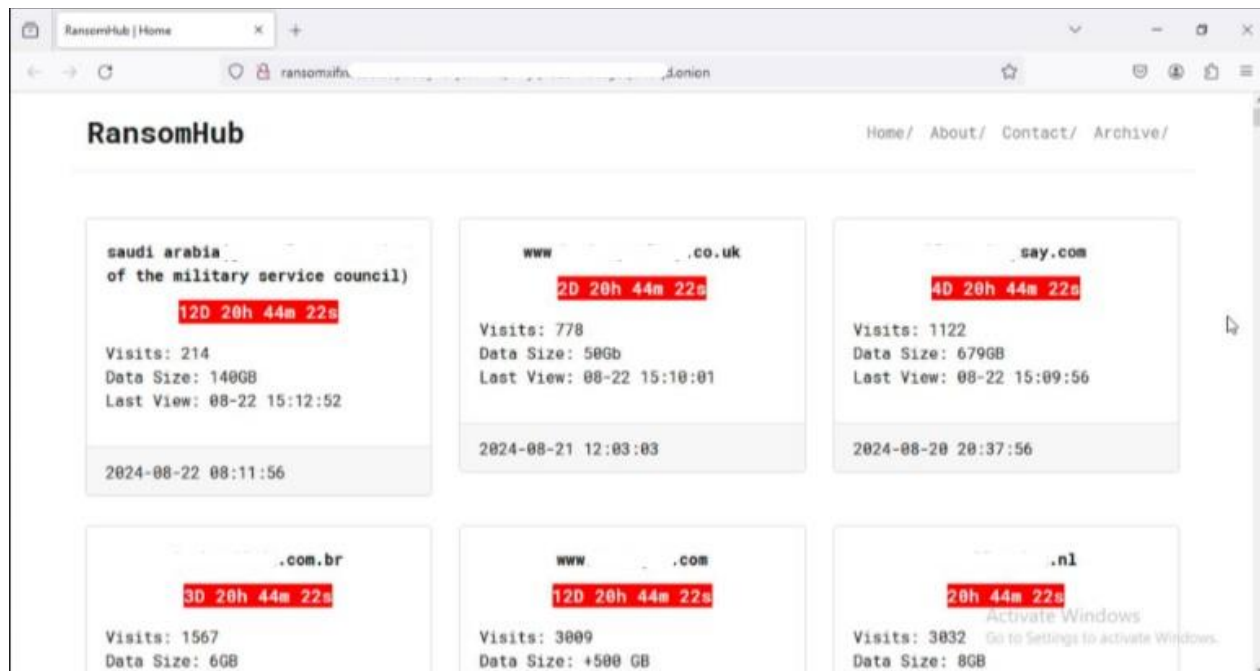
RANSOMHUB: LA AMENAZA CIBERNÉTICA QUE AUMENTA EN GUATEMALA

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|-------------------------------------|------------------------|
| ID de alerta: | DSOC-CERT_2024_08_22_1 |
| Clasificación de alerta: | Noticia |
| Tipo de Impacto: | Alta |
| TLP (Clasificación de información): | CLEAR |
| Fecha de publicación: | 22/08/2024 |
| Es día cero (0 day): | No |

RESUMEN

Guatemala ha sido blanco de ciberataques realizados por el grupo RansomHub, un colectivo de cibercriminales que ha ganado notoriedad por secuestrar datos sensibles de empresas y exigir pagos en criptomonedas a cambio de su liberación. En este artículo, analizamos cómo RansomHub ha logrado infiltrarse en diversas organizaciones guatemaltecas, con un enfoque en los aspectos técnicos de su ransomware y cómo las empresas pueden protegerse.



Detalles Específicos

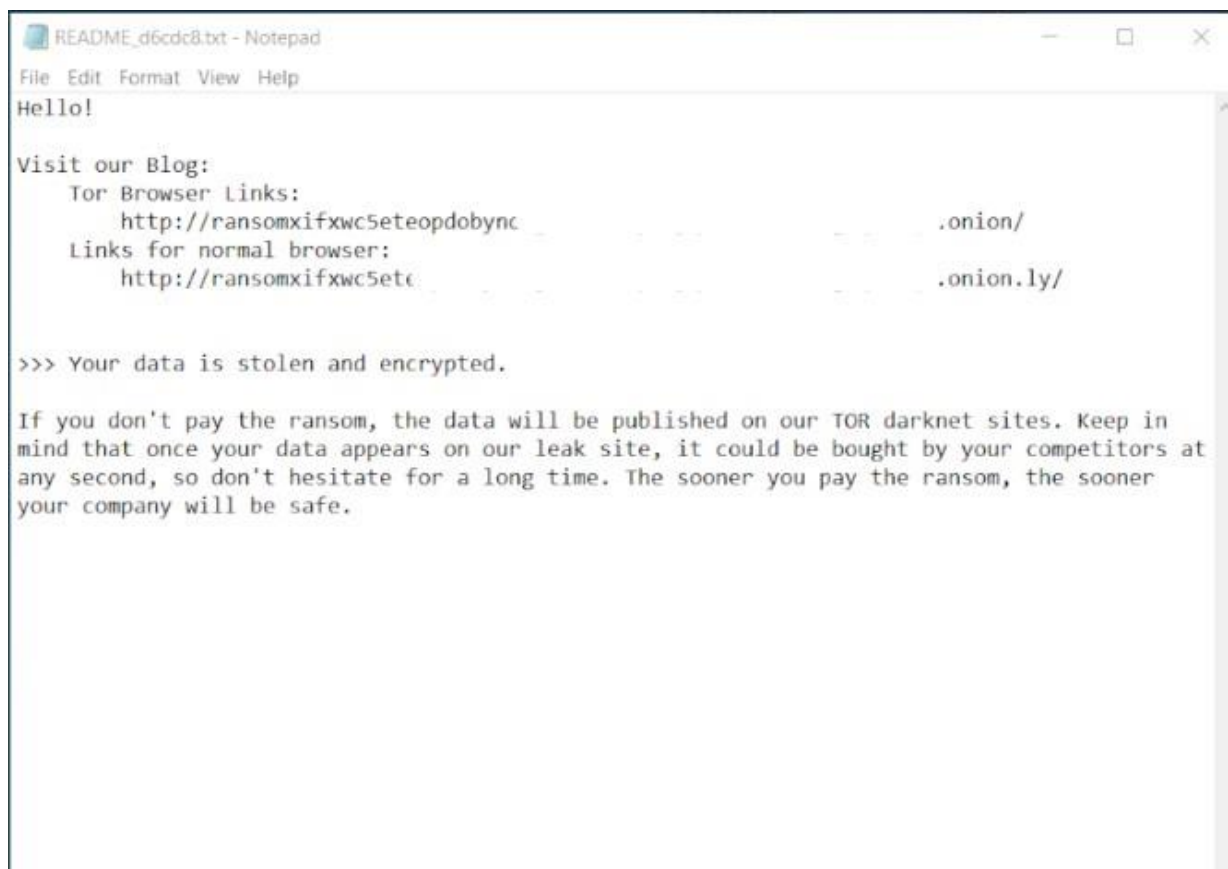
RansomHub se ha destacado por la sofisticación técnica de su ransomware, que emplea una combinación de cifrado avanzado y técnicas de evasión de detección. Este ransomware utiliza cifrados AES-256 para archivos individuales, combinados con RSA-2048 para la clave de cifrado. Este doble cifrado asegura que, sin la clave privada correspondiente, los archivos permanecen inaccesibles. El uso de RSA-2048 para cifrar la clave AES-256 permite a los cibercriminales mantener la clave de descifrado fuera del alcance de las víctimas, incluso si logran capturar la clave simétrica.

Además, el ransomware de RansomHub se caracteriza por su capacidad para evadir detección mediante técnicas como el cifrado de carga útil y el uso de dropper files, que son pequeños ejecutables diseñados para instalar el ransomware en el sistema sin levantar sospechas. Una vez desplegado, el ransomware también utiliza técnicas de "living off the land" (LotL), donde aprovecha herramientas legítimas del sistema operativo, como PowerShell y Windows Management Instrumentation (WMI), para propagarse y ejecutar su carga maliciosa.

RansomHub también emplea técnicas de exfiltración de datos antes de realizar el cifrado, lo que no solo les permite extorsionar a las empresas con la recuperación de archivos, sino también con la amenaza de

divulgar información confidencial. Esta táctica de doble extorsión se ha vuelto común entre los cibercriminales más sofisticados.

Otro aspecto técnico notable del ransomware de RansomHub es su uso de técnicas anti-forense. El malware está diseñado para eliminar rastros de su actividad en el sistema infectado, dificultando la labor de los analistas forenses en identificar el vector de ataque original o reconstruir la cadena de eventos que llevó al cifrado de los archivos.

A screenshot of a Notepad window titled 'README_d6cdc8.txt - Notepad'. The window contains a ransom note with the following text:

```
File Edit Format View Help
Hello!

Visit our Blog:
  Tor Browser Links:
    http://ransomxifxwc5eteopdobync... .onion/
  Links for normal browser:
    http://ransomxifxwc5etc... .onion.ly/

>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in
mind that once your data appears on our leak site, it could be bought by your competitors at
any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner
your company will be safe.
```

Recomendaciones Prácticas

Para contrarrestar estas técnicas avanzadas, las empresas deben adoptar un enfoque de seguridad en profundidad. Esto incluye el uso de soluciones EDR (Endpoint Detection and Response) que puedan detectar comportamientos anómalos en los endpoints y detener el ransomware antes de que se propague. También es crucial la implementación de políticas de control de acceso basadas en el principio de privilegio mínimo, reduciendo las posibilidades de movimiento lateral dentro de la red.

La segmentación de la red y la implementación de firewalls internos pueden ayudar a contener el ransomware si logra ingresar al sistema. Las soluciones de cifrado de disco completo también pueden mitigar el impacto de la exfiltración de datos, haciendo que los archivos extraídos sean inutilizables sin la clave de descryptación correcta.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240405_1_RansomHub

NOTICIA COMPLETA

<https://devel.group/blog/ransomhub-la-amenaza-cibernetica-que-aumenta-en-guatemala/>

CONTACTOS DE SOPORTE



Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://devel.group/>