Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EL FBI Y CISA ADVIERTEN SOBRE EL AUMENTO DE LOS RIESGOS DE ATAQUES DE ROYAL RANSOMWARE

06 /Marzo /2023

CONTENIDO

INTRODUCCIÓN 3
RESUMEN 4
INDICADORES DE COMPROMISO 5
RECOMENDACIONES 8
NOTICIA COMPLETA 8
CONTACTOS DE SOPORTE 9

INTRODUCCIÓN

EL FBI y la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA), han publicado conjuntamente un nuevo aviso sobre el grupo de ciberdelincuentes denominado como Royal Ransomware, que se dio a conocer el año pasado.

EL FBI Y CISA ADVIERTEN SOBRE EL AUMENTO DE LOS RIESGOS DE ATAQUES DE ROYAL RANSOMWARE

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

ID de alerta:	DSOC-CERT_2023_06_03_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	06/03/2023
Es día cero (0 day):	No

RESUMEN

EL FBI y la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA), han publicado conjuntamente un nuevo aviso sobre el grupo de ciberdelincuentes denominado como Royal Ransomware, que se dio a conocer el año pasado.

“Después de obtener acceso a las redes de las víctimas, los actores desactivan el software de antivirus y filtran grandes cantidades de datos antes de desplegar finalmente el ransomware y cifrar los sistemas”, dijo CISA.

Se cree que el grupo delictivo de ransomware, que se ha dirigido a organizaciones estadounidenses e internacionales desde septiembre de 2022, ha evolucionado a partir de iteraciones anteriores que se denominaron Zeon.

Además, se dice que es operado por actores de amenazas experimentados que solían formar parte de Conti Team One, reveló la compañía de ciberseguridad Trend Micro en diciembre de 2022.

Royal ransomware, emplea el phishing de devolución de llamadas como un medio para entregar su ransomware a las víctimas, una técnica ampliamente adoptada por los grupos criminales de la empresa Conti el año pasado después de su cierre.

También emplean otros modos de acceso inicial que incluyen el protocolo de escritorio remoto (RDP), la explotación de aplicaciones públicas y a través de agentes de acceso inicial (IAB).

Las demandas de rescate hechas por Royal varían de $ 1 millón a $ 11 millones, con ataques dirigidos a una variedad de sectores críticos, incluidas las comunicaciones, la educación, la atención médica y la comunicación.

“El ransomware Royal utiliza un enfoque de cifrado parcial único que permite al actor de amenazas elegir un porcentaje específico de datos en un archivo para cifrar”, señaló CISA. “Este enfoque permite al actor reducir el porcentaje de cifrado para archivos más grandes, lo que ayuda a evadir la detección”.

La agencia de ciberseguridad dijo que se han utilizado múltiples servidores de comando y control (C2) asociados con Qakbot en intrusiones de ransomware de Royal, aunque actualmente no se ha determinado si el malware se basa exclusivamente en la infraestructura de Qakbot.

Las intrusiones también se caracterizan por el uso de Cobalt Strike y PsExec para el movimiento lateral, así como por confiar en el servicio de instantáneas de volumen de Windows para eliminar instantáneas y evitar la recuperación del sistema. Cobalt Strike se reutiliza aún más para la agregación y exfiltración de datos.

A partir de febrero de 2023, Royal ransomware es capaz de dirigirse a entornos Windows y Linux y se ha relacionado directamente con 19 ataques solamente en el mes de enero de 2023, lo que lo coloca detrás de LockBit, ALPHV y Vice Society.

INDICADORES DE COMPROMISO

Algunos de los indicadores de compromiso son:

IPs Maliciosas	Ultima Actividad
102.157.44[.]105	Noviembre 2022
105.158.118[.]241	Noviembre 2022
105.69.155[.]85	Noviembre 2022
113.169.187[.]159	Noviembre 2022
134.35.9[.]209	Noviembre 2022
139.195.43[.]166	Noviembre 2022
139.60.161[.]213	Noviembre 2022
148.213.109[.]165	Noviembre 2022

163.182.177[.]80	Noviembre 2022
181.141.3[.]126	Noviembre 2022
181.164.194[.]228	Noviembre 2022
185.143.223[.]69	Noviembre 2022
186.64.67[.]6	Noviembre 2022
186.86.212[.]138	Noviembre 2022
190.193.180[.]228	Noviembre 2022
196.70.77[.]11	Noviembre 2022
197.11.134[.]255	Noviembre 2022
197.158.89[.]85	Noviembre 2022
197.204.247[.]7	Noviembre 2022
197.207.181[.]147	Noviembre 2022
197.207.218[.]27	Noviembre 2022
197.94.67[.]207	Noviembre 2022
23.111.114[.]52	Noviembre 2022
41.100.55[.]97	Noviembre 2022
41.107.77[.]67	Noviembre 2022
41.109.11[.]80	Noviembre 2022
41.251.121[.]35	Noviembre 2022
41.97.65[.]51	Noviembre 2022
42.189.12[.]36	Noviembre 2022
45.227.251[.]167	Noviembre 2022
5.44.42[.]20	Noviembre 2022
61.166.221[.]46	Noviembre 2022
68.83.169[.]91	Noviembre 2022
81.184.181[.]215	Noviembre 2022
82.12.196[.]197	Noviembre 2022
98.143.70[.]147	Noviembre 2022
140.82.48[.]158	Diciembre 2022
147.135.36[.]162	Diciembre 2022
147.135.11[.]223	Diciembre 2022

152.89.247[.]50	Diciembre 2022
172.64.80[.]1	Diciembre 2022
179.43.167[.]10	Diciembre 2022
185.7.214[.]218	Diciembre 2022
193.149.176[.]157	Diciembre 2022
193.235.146[.]104	Diciembre 2022
209.141.36[.]116	Diciembre 2022
45.61.136[.]47	Diciembre 2022
45.8.158[.]104	Diciembre 2022
5.181.234[.]58	Diciembre 2022
5.188.86[.]195	Diciembre 2022
77.73.133[.]84	Diciembre 2022
89.108.65[.]136	Diciembre 2022
94.232.41[.]105	Diciembre 2022
47.87.229[.]39	Enero 2023

Dominios Maliciosos	Ultima Actividad
ciborkumari[.]xyz	Octubre 2022
sombrat[.]com	Octubre 2022
gororama[.]com	Noviembre 2022
softeruplive[.]com	Noviembre 2022
altocloudzone[.]live	Diciembre 2022
ciborkumari[.]xyz	Diciembre 2022
myappearinc[.]com	Diciembre 2022
parkerpublic[.]com	Diciembre 2022
pastebin.mozilla[.]org/Z54Vudf9/raw	Diciembre 2022
tumbleproperty[.]com	Diciembre 2022
myappearinc[.]com/acquire/draft/c7lh0s5jv	Enero 2023

RECOMENDACIONES

- Implementar un plan de recuperación, mantener y retener múltiples copias de datos y servidores confidenciales, en una ubicación físicamente separada, segmentada y segura.
- Requerir las cuentas de usuario con inicio de sesión y contraseña (por ejemplo, cuentas de servicio cuentas de administrador y cuentas de administrador de dominio) que cumplan con los estándares de NIST para desarrollar y administrar políticas de contraseñas.
- Utilice factor de doble autenticación para todos los servicios en la medida de lo posible, especialmente para correo, VPN, y cuentas que accedan a sistemas críticos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Segmentos de red La segmentación de la red puede ayudar a prevenir la propagación del ransomware.
- Instale, actualice y habilite la detección en tiempo real del AV.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables

NOTICIA COMPLETA

https://devel.group/blog/el-fbi-y-cisa-advierten-sobre-el-aumento-de-los-riesgos-de-ataques-de-royal-ransomware/

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://www.devel.group/reporta-un-incidente