Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

DARK ANGELS CONSIGUE UN RESCATE HISTÓRICO EN UN ATAQUE DE RANSOMWARE

06 / 08 / 2024

CONTENIDO

INTRODUCCIÓN

En el dinámico y cada vez más desafiante panorama de la ciberseguridad, los ataques de ransomware han evolucionado hasta convertirse en una de las amenazas más significativas para las organizaciones de todo el mundo. Recientemente, el grupo de cibercriminales conocido como Dark Angels ha logrado captar la atención de la comunidad de seguridad al obtener un rescate récord, superando todas las cifras documentadas previamente. Este incidente no solo destaca la creciente sofisticación y audacia de los atacantes, sino que también subraya la urgente necesidad de que las empresas refuercen sus estrategias de defensa contra estos tipos de amenazas.

Dark Angels, conocido por sus tácticas de doble extorsión y su capacidad para atacar tanto sistemas Windows como Linux/ESXi, ha demostrado una notable habilidad para infiltrarse en redes corporativas y cifrar datos críticos. Este artículo ofrece un análisis detallado del modus operandi de Dark Angels, proporciona indicadores de ataque (IoCs) cruciales para su detección, y presenta recomendaciones para la mitigación y prevención de futuros incidentes. Con esta información, las organizaciones pueden equiparse mejor para enfrentar y neutralizar la amenaza del ransomware, protegiendo así sus activos más valiosos y manteniendo la integridad de sus operaciones.

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

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

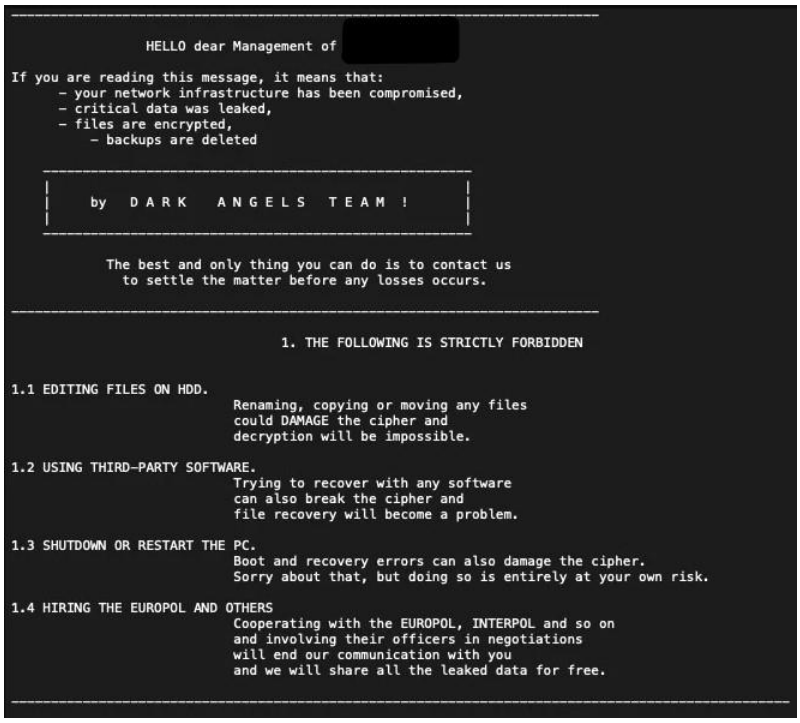
ID de alerta:	DSOC-CERT_2024_08_06_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	06/08/2024
Es día cero (0 day):	No

RESUMEN

En un suceso que marca un antes y un después en el ámbito de la ciberseguridad, el grupo de ransomware conocido como Dark Angels ha logrado un rescate sin precedentes, la suma obtenida supera cualquier cifra registrada en la historia de los ataques de ransomware, destacando la creciente amenaza que representan estos ciberataques.

Análisis del Grupo Dark Angels

Dark Angels Team surgió en mayo de 2022 y es conocido por su práctica de doble extorsión: exigen pago por un descifrador y por la no publicación de los datos robados. Su código para Windows deriva de Babuk, mientras que las variantes para Linux/ESXi usan una base de código personalizada similar a RagnarLocker.



El ransomware intenta detener los siguientes servicios tras la ejecución:

Memtas	MEPOCs	Sophos
Veeam	copia de seguridad	GxVss
GxBlr	GxFWD	GxCVD
GxCIMgr	DefWatch (Vigilancia de la Defensa)	ccEvtMgr
ccSetMgr	SavRoam (en inglés)	Escaneo RTV
QBFCServicio	QBIDPServicio	Intuit.QuickBooks.FC
QBCFMonitorService	YooCopia de seguridad	YooIT
Zhudongfangyu	Sophos	stc_raw_agent
VSNAPVSS	VeeamTransportSvc	VeeamDeploymentSe
VeeamNFSSvc	Veeam	PDVFSServicio
BackupExecVSSProvider	BackupExecAgentAccelerator	BackupExecAgentBr
BackupExecDiveciMediaService	BackupExecJobEngine	BackupExecManage
BackupExecRPCService	AcrSch2Svc	AcronisAgent
CASAD2DWebSvc	CAARCUpdateSvc	

Las cargas útiles de Dark Angels tienen la capacidad de propagarse a los recursos compartidos de red disponibles y pueden aceptar parámetros asociados. Los parámetros de línea de comandos 'paths' y 'shares' están disponibles. El método de detección de recursos compartidos puede variar en función de la opción proporcionada.

```
u_shares_00403c24                               XREF[1]:     entry:0040ad51(*)
     unicode     u"shares"

     ??          00h
     ??          00h

u_paths_00403c34                                XREF[1]:     entry:0040ad69(*)
     unicode     u"paths"

s_DarkAngels_00403c40                           XREF[1]:     entry:0040af50(*)
     ds          "DarkAngels"

     ??          00h

s_DarkAngels_00403c4c                           XREF[1]:     entry:0040af66(*)
     ds          "DarkAngels"
```

En ausencia de opciones de línea de comandos, el malware enumera todas las unidades locales y cifra todos los archivos objetivo. Tras el cifrado, a los archivos se les da la extensión..crypt

Un Nuevo Hito en la Ciberseguridad

Este rescate histórico no solo es un logro notable para Dark Angels, sino que también establece un nuevo punto de referencia para otros grupos de cibercriminales que buscan replicar su éxito. La sofisticación y audacia demostradas por Dark Angels subrayan la urgencia de implementar medidas de ciberseguridad más robustas y efectivas.

Confirmación del Pago

La empresa Chainalysis, especializada en inteligencia de criptomonedas, confirmó la veracidad del pago a través de un tuit en la plataforma X. Anteriormente, el rescate más alto registrado había sido de 40 millones de dólares, pagado por la compañía de seguros CNA en respuesta a un ataque de Evil Corp.

La Víctima: Una Empresa Fortune 50

Aunque Zscaler no ha revelado la identidad de la empresa afectada, se sabe que pertenece a la lista Fortune 50. Entre las empresas de esta lista que sufrieron ataques significativos en 2024, destaca Cencora, un gigante farmacéutico que ocupa el puesto #10. La falta de una reclamación pública del ataque sugiere que se haya realizado un pago considerable para resolver el incidente.

Implicaciones y Consecuencias

Este récord en el pago de rescate pone de manifiesto la evolución y la gravedad del ransomware, así como su impacto potencial en grandes empresas. Los ataques no solo comprometen la integridad y confidencialidad de los datos, sino que también pueden tener consecuencias económicas devastadoras. La tendencia de pagos exorbitantes subraya la necesidad urgente de adoptar estrategias de ciberseguridad más eficaces.

Medidas Preventivas y Recomendaciones

Para enfrentar estas crecientes amenazas, es crucial que las organizaciones adopten medidas proactivas, tales como:

- Implementar soluciones avanzadas de protección contra ransomware.
- Capacitar continuamente al personal en buenas prácticas de ciberseguridad.
- Colaborar con expertos en seguridad para mantenerse al día con las tácticas de los atacantes.

Conclusión

El ataque de Dark Angels y el consiguiente pago récord de rescate son un llamado de atención para la comunidad de ciberseguridad. Las organizaciones deben adoptar un enfoque integral y coordinado para mitigar el riesgo de ser las próximas víctimas de este tipo de extorsión. Solo a través de la preparación y la resiliencia podrán enfrentar los desafíos de un panorama de amenazas cada vez más complejo y peligroso.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240806_DarkAngels

NOTICIA COMPLETA

https://devel.group/blog/dark-angels-consigue-un-rescate-historico-en-un-ataque-de-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