Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERATAQUES PATROCINADOS POR EL ESTADO CHINO AMENAZAN LA INFRAESTRUCTURA CRÍTICA DE LOS EE. UU.

09 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

Una nueva amenaza cibernética ha surgido en el horizonte, con actores respaldados por el Estado Chino infiltrándose en las redes de infraestructuras críticas de los Estados Unidos. Con un enfoque meticuloso y persistente, estos ciberdelincuentes, conocidos como Volt Typhoon, están preposicionándose en las redes para facilitar ataques disruptivos en momentos de crisis geopolítica o conflictos militares. Su modus operandi sofisticado y sigiloso plantea una seria preocupación para la seguridad cibernética y la estabilidad de las operaciones comerciales.

CIBERATAQUES PATROCINADOS POR EL ESTADO CHINO AMENAZAN LA INFRAESTRUCTURA CRÍTICA DE LOS EE. UU

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

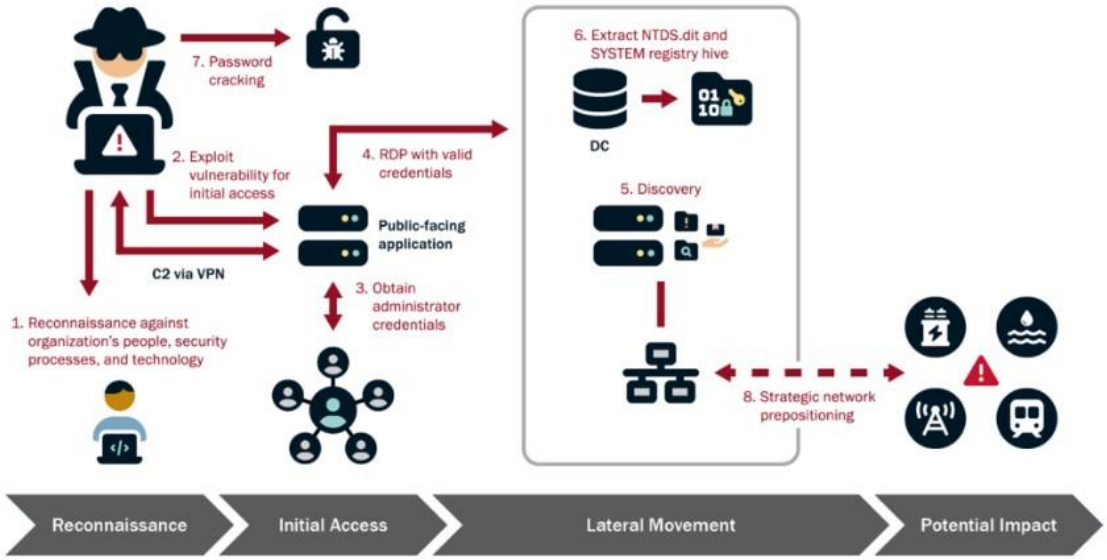
ID de alerta:	DSOC-CERT_2024_02_09_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/02/2024
Es día cero (0 day):	No

RESUMEN

En una reciente advertencia emitida por la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Agencia de Seguridad Nacional (NSA) y el Buró Federal de Investigaciones (FBI), se ha revelado una preocupante situación: actores cibernéticos respaldados por el Estado chino están infiltrando silenciosamente las redes de infraestructuras críticas en los Estados Unidos.

Este grupo, conocido como Volt Typhoon, ha sido identificado como responsable de comprometer los sistemas informáticos de múltiples organizaciones de infraestructura crítica en sectores como Comunicaciones, Energía, Sistemas de Transporte, y Sistemas de Agua y Aguas Residuales. Lo alarmante es su modus operandi: en lugar de realizar espionaje tradicional, estos actores están preposicionándose en las redes para facilitar ataques disruptivos en caso de tensiones geopolíticas o conflictos militares.

La táctica de Volt Typhoon implica una cuidadosa planificación y persistencia. Primero, realizan una exhaustiva recolección de información sobre la organización objetivo, incluyendo su arquitectura de red, protocolos operativos y personal clave. Luego, aprovechan vulnerabilidades conocidas o recién descubiertas en dispositivos de red para obtener acceso inicial. Una vez dentro, emplean técnicas sofisticadas para moverse lateralmente por la red y obtener credenciales de administrador.



Lo más preocupante es que estos actores mantienen un bajo perfil una vez dentro de la red comprometida, realizando actividades de descubrimiento y manteniendo su acceso durante períodos prolongados, a veces por años. Esto les permite acumular información sensible y, potencialmente, causar daños catastróficos en las operaciones de infraestructura crítica, como manipular sistemas de control de energía y agua.

Ante esta situación, es crucial que las organizaciones de infraestructura crítica tomen medidas inmediatas para protegerse. Se recomienda la aplicación de parches de seguridad, la implementación de autenticación multifactor (MFA) resistente al phishing y el monitoreo constante de registros de actividad. Además, se insta a las organizaciones a estar alerta y preparadas para detectar y responder a cualquier actividad sospechosa en sus redes.

La colaboración entre agencias gubernamentales y el sector privado es fundamental para combatir esta creciente amenaza cibernética. Solo con una respuesta coordinada y proactiva podremos proteger nuestras infraestructuras críticas y mantener la seguridad en un mundo cada vez más interconectado. ¡La vigilancia y la acción son la clave para defenderse contra los ataques de Volt Typhoon y otros actores cibernéticos maliciosos!

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240209_1_VoltTyphoon

NOTICIA COMPLETA

https://devel.group/blog/ciberataques-patrocinados-por-el-estado-chino-amenazan-la-infraestructura-critica-de-los-ee-uu/

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