Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Uber pirateado, los sistemas internos violados y los informes de vulnerabilidad robados.

16/Septiembre/2022

Contenido

INTRODUCCIÓN

Uber sufrió un ciberataque el jueves por la tarde cuando un hacker obtuvo acceso a los informes de vulnerabilidad y compartió capturas de pantalla de los sistemas internos de la empresa, el panel de correo electrónico y el servidor de Slack.

UBER HA SIDO VULNERADO MEDIANTE INGENIERÍA SOCIAL

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

ID de alerta:	DSOC-CERT_2022_09_14_01
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/14/2022
Es día cero (0 day):	Si

RESUMEN

Las capturas de pantalla compartidas por el pirata informático y vistas en Twitter muestran lo que parece ser un acceso completo a muchos sistemas críticos de TI de Uber, incluido el software de seguridad de la empresa y el dominio de Windows.

Otros sistemas a los que accedió el pirata informático incluyen la consola de Amazon Web Services de la empresa, las máquinas virtuales VMware ESXi, el panel de administración de correo electrónico de Google Workspace y el servidor Slack, en el que el pirata informático publicó mensajes.

Desde entonces, Uber ha confirmado el ataque, tuiteando que están en contacto con la policía y publicarán información adicional a medida que esté disponible.

"Actualmente estamos respondiendo a un incidente de seguridad cibernética. Estamos en contacto con la policía y publicaremos actualizaciones adicionales aquí a medida que estén disponibles", tuiteó la cuenta de Uber Communications.

The New York Times, que fue el primero en informar sobre la violación, dijo que habló con el actor de amenazas, quien dijo que violaron a Uber después de realizar un ataque de ingeniería social contra un empleado y robar su contraseña.

INFORMES DE VULNERABILIDAD DE HACKERONE EXPUESTOS

Si bien es posible que el actor de amenazas robara datos y código fuente de Uber durante este ataque, también tuvo acceso a lo que podría ser un activo aún más valioso.

Según el ingeniero de seguridad de Yuga Labs, Sam Curry , el hacker también tuvo acceso al programa de recompensas por errores HackerOne de la compañía, donde comentaron sobre todos los boletos de recompensas por errores de la compañía.

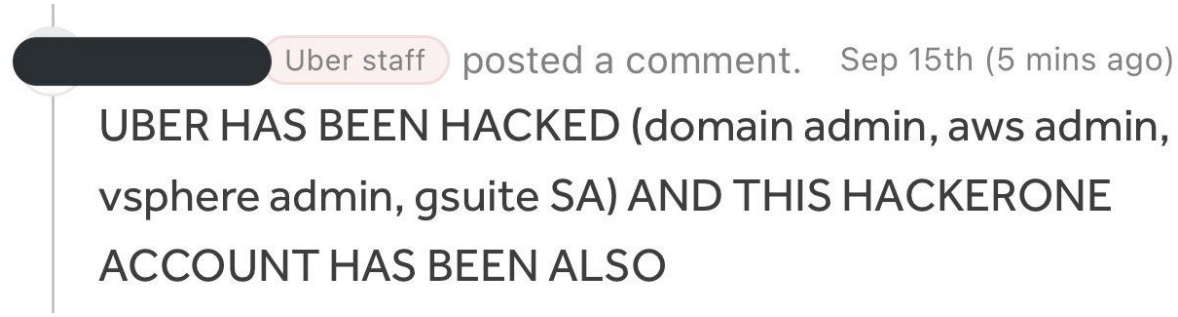
Desde entonces, HackerOne ha desactivado el programa de recompensas por errores de Uber, cortando el acceso a las vulnerabilidades reveladas.

ALCANCES DEL HACKEO.

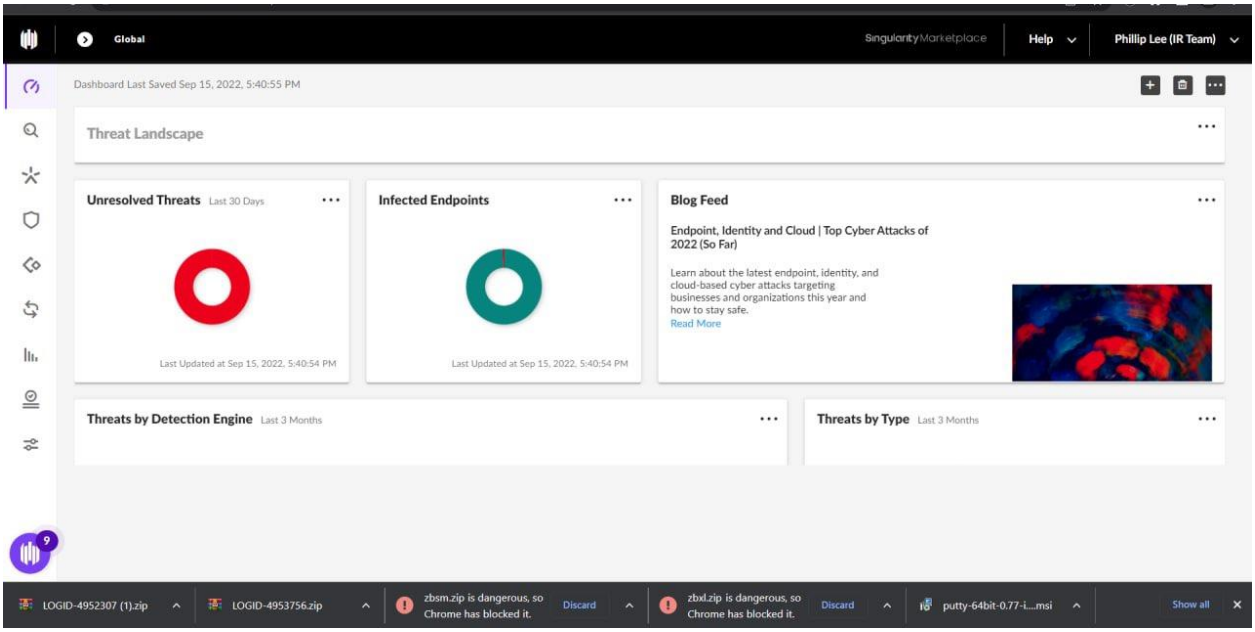
Después de escanear su red interna, el atacante obtuvo credenciales de administrador para Thycotic a través de un script de PowerShell en un recurso compartido de red.

Se ha vulnerado completamente las plataformas internas de Uber, lo compartido hasta el momento es:

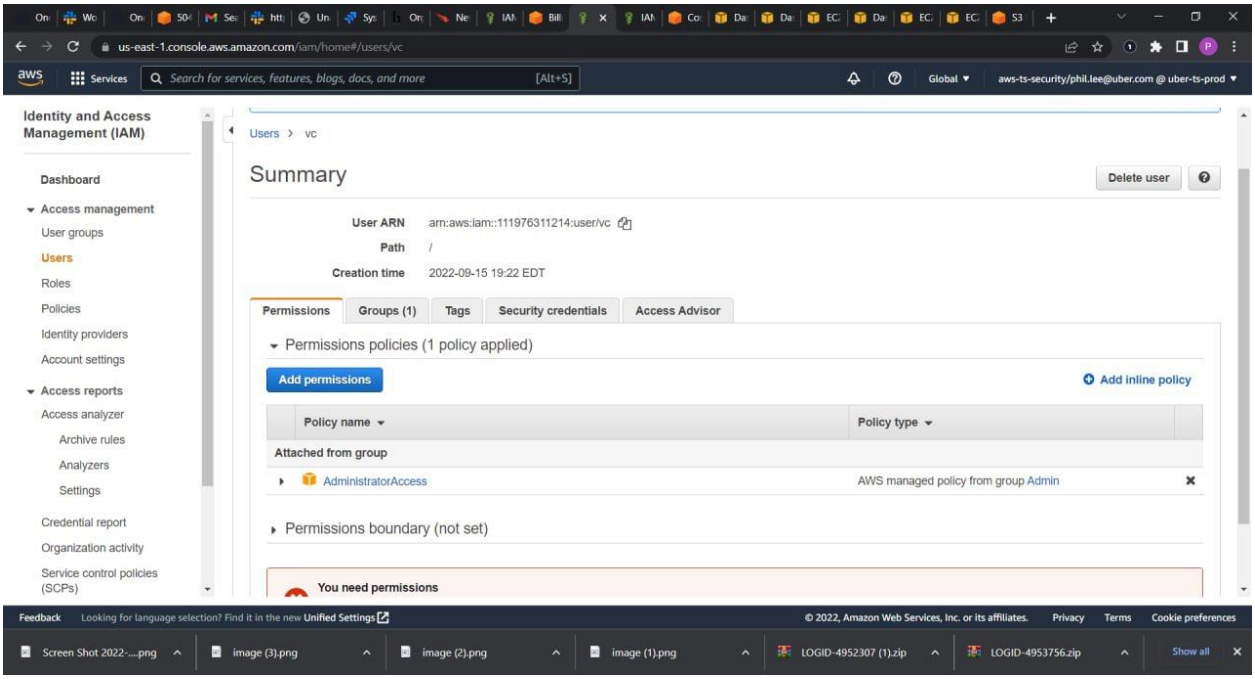
Slack:



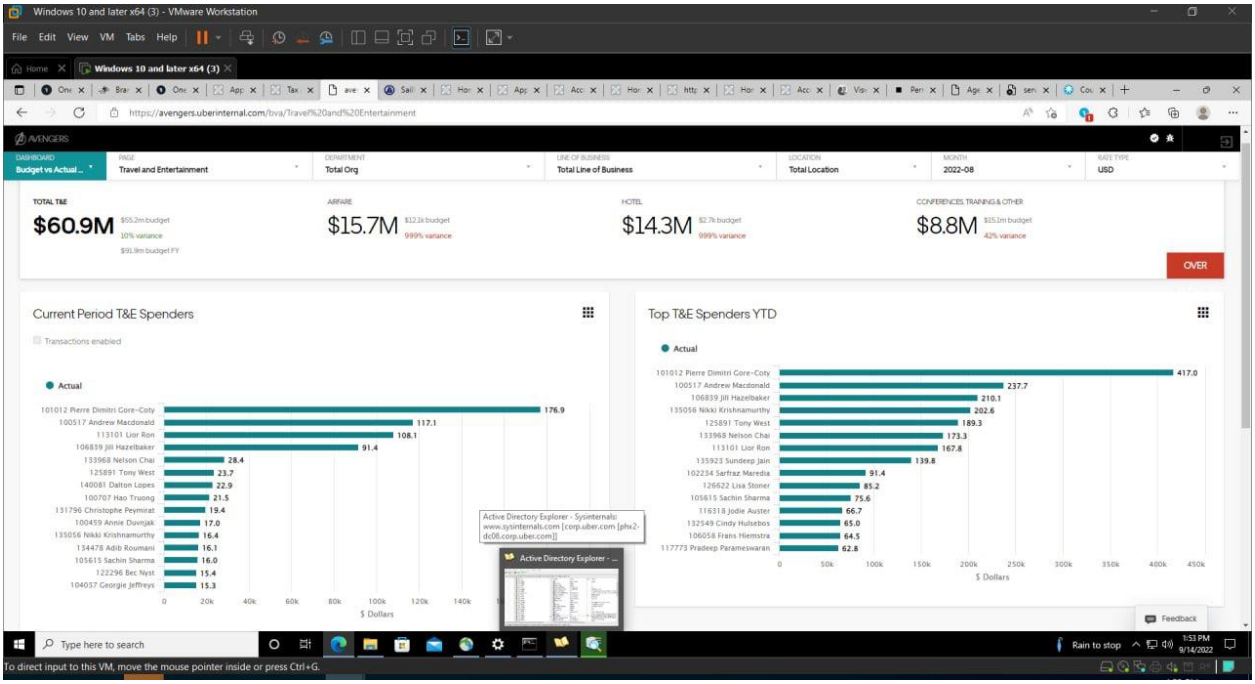
EDR:



AWS:



Información Financiera:



Adicional, es conocido que su Active Directory también fue vulnerado. Teniendo toda la información sensible el atacante.

El autor, según ha confirmado él mismo al periódico The New York Times, es un joven de 18 años que ha tenido acceso a sistemas e información confidencial de la empresa. Y uso un ataque de ingeniería social que habría dado acceso a la cuenta en Slack de uno de los empleados.

La compañía ha confirmado a través de Twitter que están "respondiendo a un incidente de ciberseguridad". "Estamos en contacto con la policía y publicaremos actualizaciones adicionales aquí a medida que estén disponibles", recoge la publicación. Está por ver si el atacante decide publicar información confidencial de la empresa o el incidente se queda ahí.

Recomendaciones

- Hacer conciencia a su personal sobre los ataques de ingeniería social, como detectarlos y a quien reportarlos.

- Habilitar 2fa en todas sus plataformas

- Procure que su personal no almacene contraseñas en el navegador o en ficheros de texto sin protección alguna.

Noticia Completa

https://devel.group/blog/uber-sufre-ataque-mediante-ingenieria-social/

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