Incidente de Ciberseguridad, Medidas de Mitigación y Protección de Cuentas de Usuario

José Urzúa
jose@nic.cl

nic chile
SOMOS EL PUNTO CL

NIC Chile

- Centro de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile
- Administrador del ccTLD .CL
  - Cumplimos el rol de Registro (registry) y Agente Registrador (registrar)
  - Agente registrador que administra el 90% de los dominios .CL
- Obligación de reportar incidentes de ciberseguridad a CSIRT del Ministerio del Interior
  - Responsable actual de la coordinación nacional de Ciberseguridad
- Agente registrador con más de 680.000 cuentas de usuario habilitadas

nic chile
SOMOS EL PUNTO CL

Incidente

- 3 de julio 2024:
  - Servicio de Atención a Clientes informa situación anómala
    - Clientes reportan modificaciones de dominios no autorizadas
- 4 de julio 2024:
  - Confirmación de incidente, revisión de alcance e identificación de forma de operar
  - Activación de grupo de crisis según Plan de Continuidad de Negocios (BCP)
  - Aviso a CSIRT de Gobierno

nic chile
SOMOS EL PUNTO CL

Incidente

- 4 de julio 2024:
  - Cambio forzado de contraseñas de usuario que estaban comprometidas
    - Reversa de cambios realizados por atacantes
  - Bloqueo de direcciones IP identificadas (pocas)
  - Activación de nuevos mecanismos de registro de actividad (log) para accesos no autorizados
  - Anuncio público
    - https://www.nic.cl/anuncios/20240704-incidente.html

nic chile
SOMOS EL PUNTO CL

NIC Chile reporta incidente en cuentas de usuarios de clientes

NIC Chile informa que hemos detectado la ocurrencia de un incidente de ciberseguridad que ha afectado a las cuentas de algunos de nuestros usuarios durante el día 3 de julio de 2024.

En esta situación, nuestra evaluación inicial apunta a que un atacante aprovechó la debilidad de algunas contraseñas de cuentas de usuario de nuestros clientes, logrando tener acceso no autorizado a ellas y modificando en algunos casos la información asociada a sus servidores DNS. Continuamos analizando el incidente para establecer un diagnóstico definitivo.

Cabe mencionar que este incidente de ciberseguridad ha sido reportado al CSIRT de Gobierno.

Hemos levantado un catastro de las cuentas afectadas por este incidente y hemos reversado los cambios realizados sin autorización. Como precaución, hemos bloqueado las cuentas y los dominios afectados.

Lamentamos los inconvenientes que esta situación ha causado y aseguramos que estamos destinando nuestros mejores esfuerzos para robustecer los mecanismos de acceso a las cuentas de usuario. Asimismo, recomendamos tener en cuenta y seguir los consejos sobre manejo de contraseñas que tiene disponible el CSIRT de Gobierno en la página **https://ciberseguridad.gob.cl/documents/9/Proteccion-NivelBasico.pdf**.

NIC Chile
Santiago, 04 de julio de 2024.

Incidente

- 5 de julio 2024, 1 día después de incidente:
  - Envío de mensaje a los afectados informando procedimiento para recuperar acceso a su cuenta de usuario
  - Aplicación de nuevas reglas para contraseñas de cuentas de usuario

  - Nuevos mecanismos de registro de actividad en cuentas de usuario
  - Anuncio público informando acciones realizadas
    - https://www.nic.cl/anuncios/20240705-medidas.html

nic chile
SOMOS EL PUNTO CL

NIC Chile informa acciones por incidente de ciberseguridad

En relación al incidente de ciberseguridad descubierto el 4 de julio de 2024, que involucró el acceso a algunas cuentas de usuario de clientes de NIC Chile, entendemos la preocupación que este incidente pueda causar entre todos nuestros usuarios, por lo que nos parece importante precisar lo siguiente:

1. El número de cuentas de usuario afectadas es una fracción muy pequeña del total de cuentas en NIC Chile. A todas ellas se les contactó directamente por email para informarles del incidente y de las medidas tomadas, las que incluyen la inhabilitación temporal de sus contraseñas como medida preventiva.
2. El número de dominios afectados por la modificación de los DNS es una fracción mucho más pequeña todavía. En todos los casos, al momento de efectuarse la modificación, se le informó al usuario vía mail respecto de este hecho. En la mayoría de los casos, esto sirvió como una alerta que permitió al mismo usuario deshacer el cambio. En cualquier caso, NIC Chile se aseguró de que todos estos dominios volvieran a tener su información de DNS correcta.
3. De acuerdo a nuestra evaluación inicial, un atacante aprovechó el conocimiento de contraseñas utilizadas en algunas de las cuentas de usuario, probablemente expuestas por brechas de seguridad previas de otros sitios en Internet, para lograr tener acceso no autorizado a ellas. Hay indicios relacionados al uso de programas maliciosos llamados infostealers, como ha señalado en sus alertas la agencia gubernamental de ciberseguridad CSIRT (https://csirt.gob.cl/alertas/cnd24-00124/).
4. Para robustecer el acceso a las cuentas de usuario, hemos aplicado nuevas reglas de contraseñas para clientes nuevos y para clientes que deseen cambiar la misma.
5. Es importante señalar que, durante esta incidencia, nuestros sistemas no fueron comprometidos.

Lamentamos los inconvenientes que esta situación ha causado y aseguramos que seguimos destinando nuestros mejores esfuerzos para seguir fortaleciendo los mecanismos de seguridad en el acceso a las cuentas de usuario.

NIC CHILE
Santiago, 5 de julio de 2024.

Incidente

- Sábado 6 de julio (2 días de iniciado el incidente)
  - Identificamos nuevos intentos masivos distribuidos de acceso a cuentas de usuario
  - Se decide:
    - Cambiar todas las contraseñas de cuentas de usuarios
    - Para recuperar acceso a sus cuentas deben pasar por procedimiento de “recuperación de contraseña”
    - Se activa captcha para autenticación de usuario (evitar automatización)
  - Se publica anuncio informando las acciones:
    - https://www.nic.cl/anuncios/20240706-medidas.html

nic chile
SOMOS EL PUNTO CL

NIC Chile informa acciones adicionales por incidente de ciberseguridad

Tal como señalamos en el comunicado anterior, seguimos trabajando en fortalecer la seguridad de los mecanismos de acceso a las cuentas de usuario.

En este sentido, a pesar de que el impacto del incidente ha sido muy limitado, existe evidencia de que muchos usuarios utilizan las mismas contraseñas en muchos sitios, por lo que hemos considerado prudente iniciar un proceso de cambio de las contraseñas de acceso a todas las cuentas de usuario.

Hacemos presente que seguimos en contacto con el CSIRT de Gobierno para mantener informada a la autoridad competente en materia de Ciberseguridad.

NIC CHILE
Santiago, 6 de julio de 2024.

Incidente

- 18 de julio 2024:
  - Se activa MFA para todas las cuentas de usuario:
    - Luego de autenticarse con usuario/contraseña, se envía un código por correo electrónico para permitir el acceso a la cuenta
- 25 de julio 2024:
  - Nuevo anuncio informando las medidas aplicadas:
    - https://www.nic.cl/anuncios/20240725-medidas.html

nic chile
SOMOS EL PUNTO CL

Actualización respecto de medidas de seguridad

Como hemos informado, en el evento ocurrido el 4 de julio, no hubo vulneración de los sistemas de NIC Chile, pero se confirmó el acceso a algunas cuentas de usuario por parte de terceros no autorizados. Todo apunta a que esto habría ocurrido empleando contraseñas de cuentas obtenidas mediante el uso de programas maliciosos infostealers.

Si bien la principal responsabilidad del cuidado de las contraseñas recae en el usuario, entendemos que como NIC Chile podemos ayudar de manera importante en la protección de las cuentas de usuarios, para lo cual, hemos implementado algunas medidas, entre las que se encuentran las siguientes:

1. Mecanismos para dificultar intentos automáticos de login (captcha),
2. Nuevas reglas para robustecer las contraseñas de las cuentas de usuario,
3. Segundo factor de autenticación mediante código de verificación enviado al correo,
4. Mejoras en el monitoreo de los sistemas en línea.

Estas medidas se suman a la posibilidad, que ya existía desde 2013, en la cual el contacto administrativo puede "bloquear" un dominio que no se vaya a modificar con frecuencia.

Continuando con las mejoras, próximamente agregaremos el uso de un código TOTP (contraseña de un solo uso basadas en tiempo) como una opción para verificar el ingreso a la cuenta de usuario.

Éstas son solo algunas de las iniciativas en las que estamos trabajando, las que están siendo evaluadas periódicamente para lograr el mejor balance entre seguridad y usabilidad para nuestros usuarios.

NIC CHILE
Santiago, 25 de julio de 2024.

Comentarios

- Detección temprana:
  - Servicio de Atención a Clientes puede identificar comportamientos anómalos
  - Monitoreo de Redes Sociales
- Importancia de Comité de Crisis con múltiples enfoques:
  - Atención a Clientes, Legal, Seguridad, Técnico, Comunicaciones, Directivo
  - Comunicaciones: opinión pública queda la sensación que vulneraron sistemas de NIC Chile

nic chile
SOMOS EL PUNTO CL

Comentarios (2)

- Implementación de nuevas funcionalidades durante crisis:
  - Desarrolladores, QA y Operaciones
- Refinar monitoreo de servicios, operaciones y alertas asociadas
- Prevención proactiva
  - Dar prioridad a Seguridad
  - Monitoreo continuo
- Tener conciencia que la plataforma de ccTLD se puede usar para *hackear* a terceros

Incidente de Ciberseguridad, Medidas de Mitigación y Protección de Cuentas de Usuario

José Urzúa
jose@nic.cl

nic chile
SOMOS EL PUNTO CL