INSTITUTO FEDERAL DE TELECOMUNICACIONES

Seminario Ciberseguridad: Retos y Oportunidades
14 y 15 de octubre de 2020

Tecnológico de Monterrey

Planes de contingencia y gestión de crisis en México

Panorama

6 de julio de 2020 – CONDUSEF

EL ECONOMISTA

Anonymous hackea el portal de Condusef y amaga con derribar el sitio web de Banxico

Los fallos obedecerían a hackeos de parte del grupo Anonymous México, en reclamos contra el presidente Andrés Manuel López Obrador respecto a la transparencia en instituciones del gobierno federal.

Redacción
06 de julio de 2020, 18:47

1 de 2 Minutos después de los hackeos, el portal de la Condusef fue desactivado. Foto: Especial.

7 de julio de 2020 – Banco de México

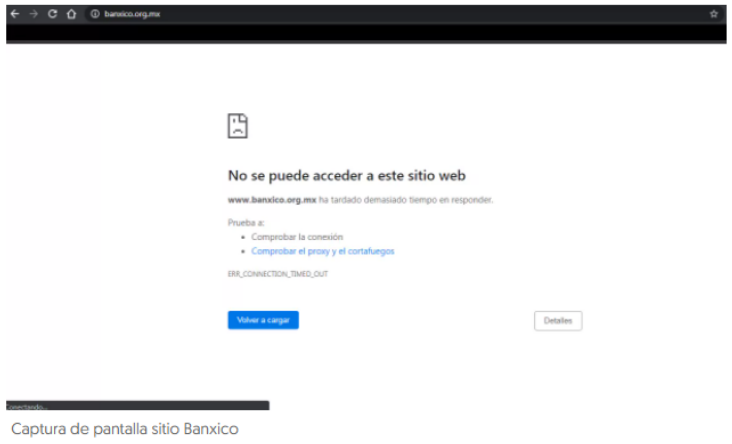
EL FINANCIERO ECONOMÍA MERC
ECONOMÍA, MERCADOS Y NEGOCIOS EN ALIANZA CON Bloomberg

ECONOMÍA

Banxico confirma intento de hackeo a su sitio web

- Esto se da luego de que el lunes se cayera también la página de Condusef, luego de un presunto hackeo.

REDACCIÓN 07/07/2020 Actualización 07/07/2020 - 16:25

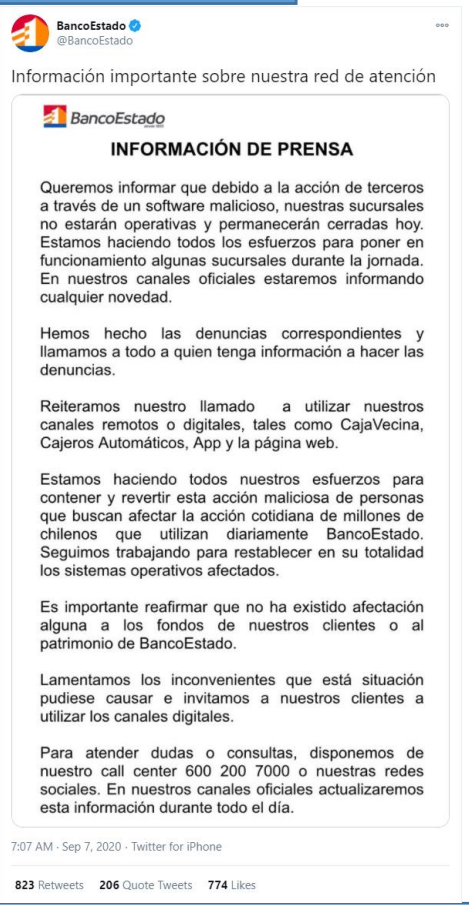


Captura de pantalla sitio Banxico

Fuente CONDUSEF: https://www.eleconomista.com.mx/politica/Anonymous-hackea-el-portal-de-Condusef-y-amaga-con-derribar-el-sitio-web-de-Banxico-durante-la-mananera-de-AMLO-20200706-0088.html
Fuente Banco de México: https://www.elfinanciero.com.mx/economia/se-cae-sitio-de-banxico-anonymous-mexico-se-adjudica-hackeo

Panorama

5 de septiembre de 2020 – Banco Estado (Chile)



Fuente: https://www.fayerwayer.com/2020/09/banco-estado-hackeo-ransomware/

Panorama

11 de septiembre de 2020 – Adeslas (España)

El Confidencial

EL PROBLEMA PUEDE DURAR AÑOS SI NO SE PAGA

Tres semanas KO por un ciberataque: así tienen secuestrados los sistemas de Adeslas

La compañía de salud, una de las más grandes de España, lleva desde el 11 de septiembre sin poder operar con normalidad debido a un potente ataque 'ransomware'

Sede de SeguCaixa Adeslas. (Foto: Wikimedia)

AUTOR
GUILLERMO CID
Contacta al autor
guillecid
Á. MORENO
Contacta al autor
@aitenalvaro
A. ALAMILLOS
Contacta al autor
@All_Arena

TAGS
RANSOMWARE CIBERATAQUE – HACKERS

TIEMPO DE LECTURA 8 min

03/10/2020 05:00 - ACTUALIZADO: 05/10/2020 16:39

La primera información llegó el pasado 11 de septiembre. La aseguradora Adeslas, una de las más grandes de su sector en España, anunciaba que había sufrido **un grave ataque informático** y que tenía problemas para seguir trabajando con normalidad. En ese primer momento **no se dieron más detalles sobre el tipo de ataque** ni el calado total del mismo, pero tres semanas después, el problema sigue sin resolverse y se empiezan a esclarecer algunos puntos. Como ha confirmado la empresa, son víctimas de **uno de los temidos 'ransomware'** que ya han afectado a muchísimas otras instituciones y ahora han metido en serios problemas a esta gran empresa.

Los estragos de este ataque, centrado en bloquear toda la estructura informática, se muestran claramente con un pequeño vistazo. Se ven **en las webs de la empresa**, y se dejan notar incluso **en las redes sociales**, donde su cuenta oficial responde cada día a quejas de todo tipo de pacientes. Tal es la situación que a día de hoy **ni siquiera se puede acceder al área de cliente en la web**, casi cualquier apartado de sus páginas viene acompañado de un mensaje en el que se avisa que ahora mismo no está todo el servicio disponible y la situación interna es de lo más delicada, como comentan a este periódico fuentes conocedoras de la situación. Tanto los hospitales asociados a la aseguradora como los trabajadores llevan semanas bajo mínimos u obligados a recuperar métodos de hace años.

Chantaje a Adif: cibercriminales amenazan con difundir 800GB de información sensible

C. OTTO

El grupo REVil asegura que, si la empresa pública no se aviene a sus condiciones (previsiblemente, un rescate económico), difundirá 'online' sus contratos y facturas,

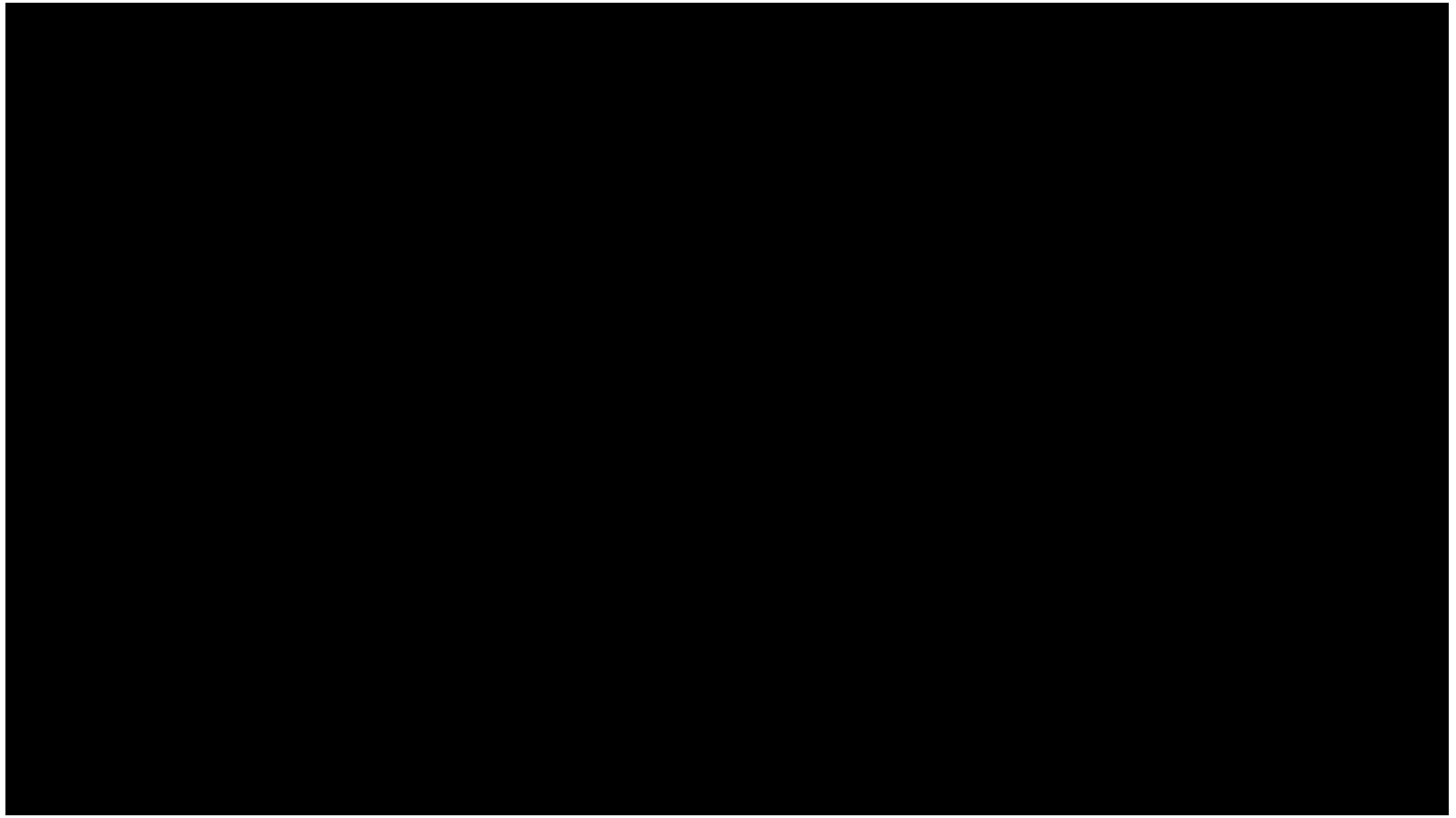
"No se puede ni encender un ordenador. Está todo fatal, no puedes ver, ni hacer radiografías, **no se puede ver a quién tienes [en agenda] y quién no**, no se puede ver quién ha venido y qué les están haciendo, el historial [médico]", explica una fuente conocedora de la situación y que convive a diario con estos

Fuente: https://www.elconfidencial.com/tecnologia/2020-10-03/adeslas-ransomware-hackers-ciberataque-datos_2773032/

Panorama

Los ataques han cambiado de objetivo, pasando a dirigirse contra las grandes multinacionales, instituciones financieras, instituciones de gobierno e infraestructuras esenciales, a través de sus empleados y clientes.

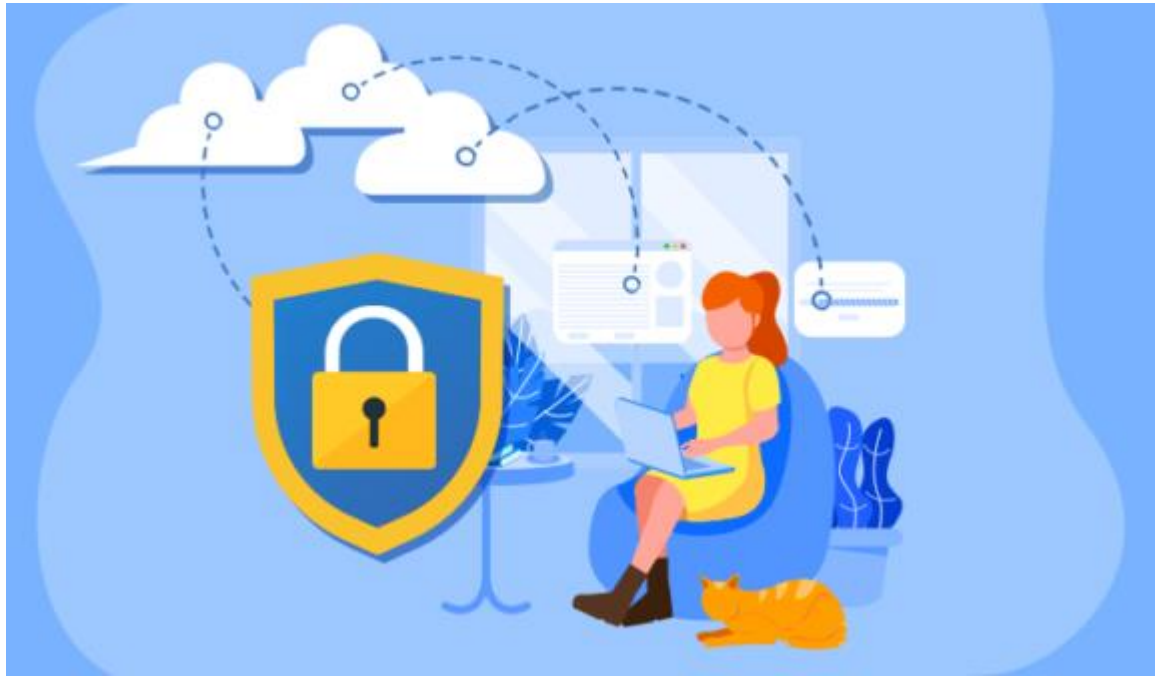
Ataque Watering Hole



Herramientas mas comunes utilizadas
para perpetrar delitos cibernéticos durante el COVID-19

Ataque y explotación de las plataformas y procesos remotos

- Manipulación digital de documentos de identidad en plataformas de identificación remota.
- Aprovechamiento de credenciales comprometidas para acceder y controlar cuentas remotamente.

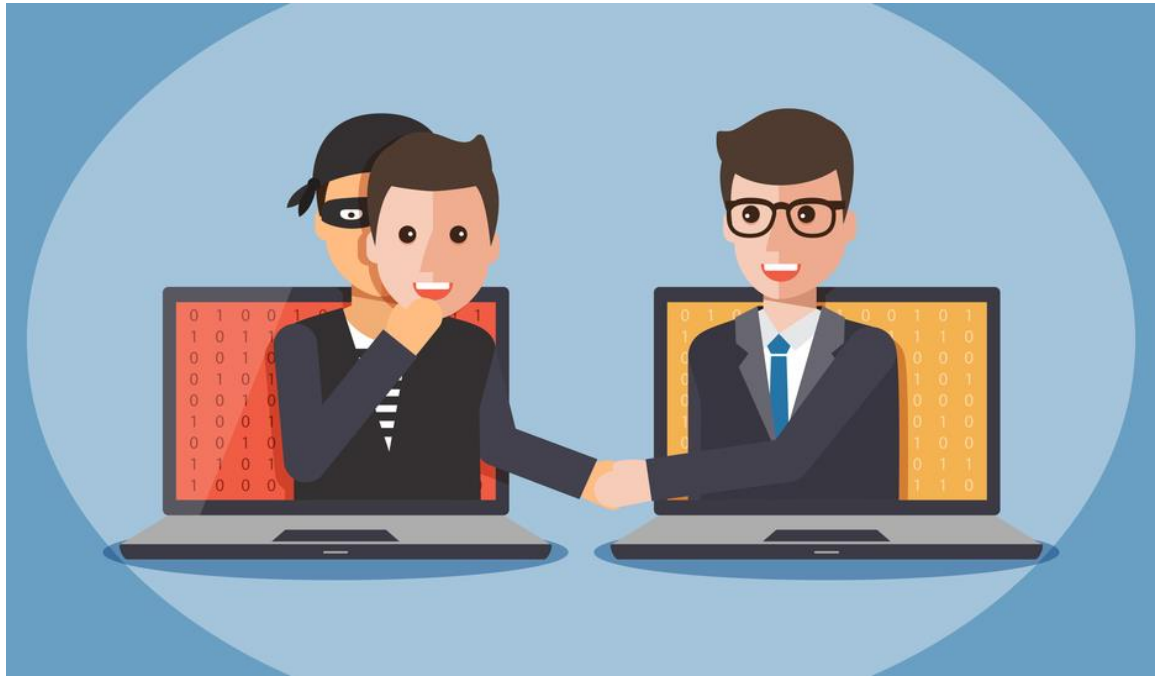


Herramientas mas comunes utilizadas

para perpetrar delitos cibernéticos durante el COVID-19

Suplantación de la identidad, programas malignos y extorsión

- Comunicaciones a clientes o usuarios aparentemente legítimas a través de email.
- Distribución de malware a través de correos apócrifos, descargas, sitios web maliciosos o aplicaciones fraudulentas.
- Campañas en redes sociales con cuentas secuestradas de usuarios famosos.



Herramientas mas comunes utilizadas

para perpetrar delitos cibernéticos durante el COVID-19

Compromiso de correo electrónico de negocios (BEC)

- Estafas utilizando cuentas de correo electrónico comprometidas.
- Utilizar ingeniería social para convencer a compañías para dirigir pagos a nuevas cuentas.
- Hacer uso de solicitudes urgentes como consecuencia de la pandemia.

Aspectos que han cobrado relevancia en el 2020

Estafas por Internet y el phishing

Aspectos que han cobrado relevancia en el 2020

Malware disruptivo (ransomware y DDoS)

Aspectos que han cobrado relevancia en el 2020

Malware destinado a la obtención de datos

Aspectos que han cobrado relevancia en el 2020

Dominios maliciosos

Aspectos que han cobrado relevancia en el 2020

Desinformación

Importancia de contar con un plan de continuidad

Elementos relevantes

- Definir los escenarios que requieren un plan de continuidad
- Identificar y acordar los **procesos más críticos** y sus **tiempos máximos de inactividad**.
- Contar con **alternativas reales** que aseguren la continuidad de estos procesos.
- Tener definidos **roles y responsabilidades**.
- Saber cómo **actuar frente a los posibles escenarios de riesgo**.
- Planificar la **prueba periódica del plan.**
- Conocer los **aspectos a mejorar**, según los resultados de las pruebas.
- Ser conscientes de la importancia de **mantener actualizado el Plan**.

Reflexiones sobre COVID-19

- La necesidad de acelerar los procesos de transformación digital
- La seguridad debe acompañarnos en todo lugar y en cada momento
- Las amenazas informáticas no están en confinamiento
- El impacto y el volumen de los ciberataques es cada vez mayor
- Los planes de contingencia deben estar actualizados y probados
- La continuidad en las operaciones debe considerar siempre la seguridad de la información
- Las crisis también traen oportunidades