JORNADAS DE
SEGURIDAD INFORMÁTICA
3ª EDICIÓN | 2019

CHACO
Gobierno del Pueblo

Buenas Prácticas de Seguridad Informática

ECOM

POLICÍA DEL CHACO
División Cibercrimen

POLICÍA DEL CHACO

Ministerio de Seguridad Pública
Gobierno del Pueblo del Chaco

Subsecretaría de Niñez, Adolescencia y Familia
Gobierno del Pueblo del Chaco

Ministerio de Desarrollo Social
Gobierno del Pueblo del Chaco

Dirección General de Tecnologías de Información y Comunicación
Gobierno del Pueblo del Chaco

Subsecretaría de Modernización del Estado
Gobierno del Pueblo del Chaco

Secretaría General de Gobierno y Coordinación
Gobierno del Pueblo del Chaco

IPAP CHACO

CHACO
Gobierno del Pueblo

Estadísticas a tener en cuenta:

- Entre el 2016 y 2017 los ***hackeos*** detectados y procesados en la Argentina aumentaron un 700%.
  a) En el 2015: 2.252 casos registrados.
  b) En el 2016: 422.672 casos registrados.
  c) En el 2017: 3.131.268 casos registrados.

- ***ESET Security Report*** 2017 reveló:
  a) 60% de empresas en Argentina sufrieron algún tipo de incidente relacionado con seguridad informática.
  b) el 32% padeció algún caso de malware.

- La 23ª edición del ***Internet Security Threat Report (ISTR)*** que analiza 157 países, reveló:
  a) Argentina es el 4° país con más ataques y amenazas cibernéticas de Latinoamérica.
  b) El podio en la región lo ocupan Brasil, México y Venezuela.

- Según ***Fortinet***: En 2017 hubo aproximadamente 10 ataques detectados por año por empresa/organización.

Estadísticas a tener en cuenta:

- ***Ponemon Institute:*** 70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017.
- ***SC Media:*** Se estima que para el 2020, el número de contraseñas utilizadas crecerá a 300 billones.
- ***Panda Security:*** 230,000 nuevos malware son producidos cada día, y se predice que este número crecerá.
- ***ZD Net:*** A una compañía le toma entre 6 meses, o 197 días, detectar una brecha de seguridad.
- ***Computer World:*** Windows es el sistema operativo más atacado por hackers, Android viene en segundo lugar.
- ***Ponemon:*** El costo total de un ciberataque exitoso es de más de $5 millones de dólares, o $301 por empleado.
- ***Accenture:*** El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos.

Aseguramiento del sistema operativo:

1) Proteger cuentas con contraseñas fuertes y seguras:

❑***Contraseñas fuertes:*** contraseñas fáciles de recordar es otra de las debilidades que los códigos maliciosos suelen aprovechar. Cuentas de redes sociales o de correo electrónico, así como el acceso los activos más sensibles (banco, almacenamiento en la nube o tiendas online) deben estar protegidas por una contraseña larga y única. Debes evitar usar la misma clave en varios sitios importantes distintos.

❑***Controla la longitud de la contraseña:*** Crea una contraseña que tenga 8 o más caracteres, mientras más larga sea, más segura será, darle una longitud acorde a lo que va a guardar

❑***Forma una secuencia «aleatoria» de palabras o letras:*** Utiliza una frase o una serie de letras que sea aleatoria pero al mismo tiempo fácil de recordar que llamarás «palabra base»

❑***Añade el nombre del servicio que quieres proteger:*** puedes utilizar el nombre del servicio y añadirlo antes o después de la palabra base.

1) Protege tus cuentas con contraseñas fuertes y seguras:

- ***Añade letras mayúsculas:*** Una vez que tienes la palabra base sobre la que vas a trabajar todas tus contraseñas, tienes que añadir, al menos, 2 letras mayúsculas.
- ***Añade números a la contraseña:*** añade números a la palabra base que has creado previamente.
- ***Añade signos de puntuación y símbolos:*** para hacerla así infranqueable.
- ***Mantén tus contraseñas a salvo:*** "**NO** dejes notas con tus contraseñas en tu ***ordenador*** ni en tu ***escritorio***."
- ***Utiliza un administrador de contraseñas:*** utilizar administradores de contraseñas de confianza como **LastPass** o **Sticky Password** (estas aplicaciones sólo te hacen recordar una contraseña y las demás son creadas y almacenadas por ellos para ser usadas cuando las necesites).

Aseguramiento del sistema operativo:

2) **Carpetas compartidas :** verificar si archivos que se comparten no estén infectados, para no propagar el virus.

3) ***Dispositivos USB:*** se deben tomar precauciones y recaudos al querer conectar algún dispositivo externo a la CPU. Como ser: disco duro externo, pendrive.

Protección en el correo electrónico

- ***Correo electrónico*** es el método más empleado por los ***phishers***, estos envían correos masivos no solicitados por los usuarios (spam) haciéndose pasar por una empresa u organismo con la finalidad de obtener ciertos datos privados de la persona para su propio beneficio.

- ***Phishers:*** acceden a sistemas/redes sin permiso con el fines maliciosos, tales como propagar malware, robar datos o espiar sistemas.

- **SPAM:** Hoy en día, el 70-80% de todo el tráfico de correo es SPAM. La mayor parte de los casos, el ***spam*** es publicidad (spammers).

Protección en el correo electrónico

El 50% del SPAM pertenece a las categorías (según kaspersky):

- Contenido para adultos (enlaces a sitios de pornografía o anuncios eróticos)
- Salud y medicina (anuncios de pérdida de peso, cuidado de la piel, medicamentos no tradicionales)
- Tecnología Informáticas (ofertas de hardware y software, hosting de sitios web, registros de dominio)
- Finanzas personales (ofrece seguros, servicios de reducción de deuda, préstamos con bajas tasas de interés)
- Educación, entretenimiento (ofertas para seminarios, cursos, títulos en línea)

Recomendaciones ante presencia de SPAM:

- ✓ No responder el correo spam. Ignorarlos y/o borrarlos.
- ✓No pulses ni enlaces ni imagenes en mensajes de spam, porque de esta manera podrá verificar el remitente que tu cuenta exista.
- ✓ No confiar en correos spam con archivos adjuntos.
- ✓ Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos.
- ✓ Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, entre otros.
- ✓ Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
- ✓ En lo posible, evitar el re-envío de mensajes en cadena.
- ✓ Si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre Con Copia Oculta (CCO).

Ejemplo de correo electrónico SPAM

ruben [redacted] emisora[redacted]_ mhz@yahoo.com.ar 18 nov (hace 2 días)

para mí

Estimado

En primer lugar te quiero agradecer por tu atencion eso es una prueba que eres una persona en quien puedo confiar.Soy un poco avergonzado de pedir este tipo de ayuda.El gerante de mi hotel me explico que puede mandar esta suma a través de Western Union es un servicio de transferencia rapido y sin dificuldad de dinero en el mundo y la agencia se encuentra generalemente en las oficinas de correos postales y con las siguientes informaciónes puedes hacerme una transferencia rápida.

Aquí está la dirección exacta del lugar donde se debe realizar la transferancia en mi nombre:

Mi Nombre Completo: Ruben [redacted]
País: Costa de Marfil
Ciudad: abidjan
Dirección: 7, Rue Kapnikareas,10556

Asi cuando se hecho la transferancia debe comunicarme los datos siguientes: código MTCN, pregunta secreta y respuesta
tambien el importe enviado en mi correo electronico.

Eso es una emergencia y espero que puedo contar con su disponibilidad,no te preocupes te voy a dar más detalles y el objeto de mi viaje cuando regresara.

Phishing

- ***Concepto:*** modalidad delictiva la cual realiza estafas a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico.

❑ ***Entre las buenas prácticas de seguridad para no ser víctimas de phishing, recomendamos:***

1. **Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio.**
2. **Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles.**
3. **No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden redireccionar hacia sitios web clonados o hacia la descarga de malware.**
4. **No se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico.**
5. **Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https.**
6. **Comunicarse telefónicamente con la compañía si se tiene dudas sobre la legitimidad de un correo.**

TIPOS DE PHISHING

*Todas las técnicas que se describen a continuación están vinculadas a la **Ingeniería Social**. Esto sería, los atacantes se hacen pasar por una **entidad conocida** como podría ser una red social, alguna entidad financiera o algún sitio de ventas en línea, y **roban información confidencial** como podrían ser credenciales de acceso.*

1) ***Phishing Tradicional:*** *está vinculado a la copia de un sitio conocido por la víctima, en el cual se cambia la dirección a donde llegan los datos ingresados.*
2) ***Smishing SMS:*** *está relacionado con el uso de otro canal digital como son los teléfonos celulares. Normalmente los delincuentes se hacen pasar por entidades conocidas y envían un mensaje de texto alertando a la víctima de que ha ganado un premio.*
3) ***Vishing:*** *la víctima recibe un mensaje en que se pide que llame a un número de teléfono concreto para obtener un regalo u otra información. En la práctica, sin embargo, se estará contactando con falsos centros de atención telefónica que reclamarán datos privados.*

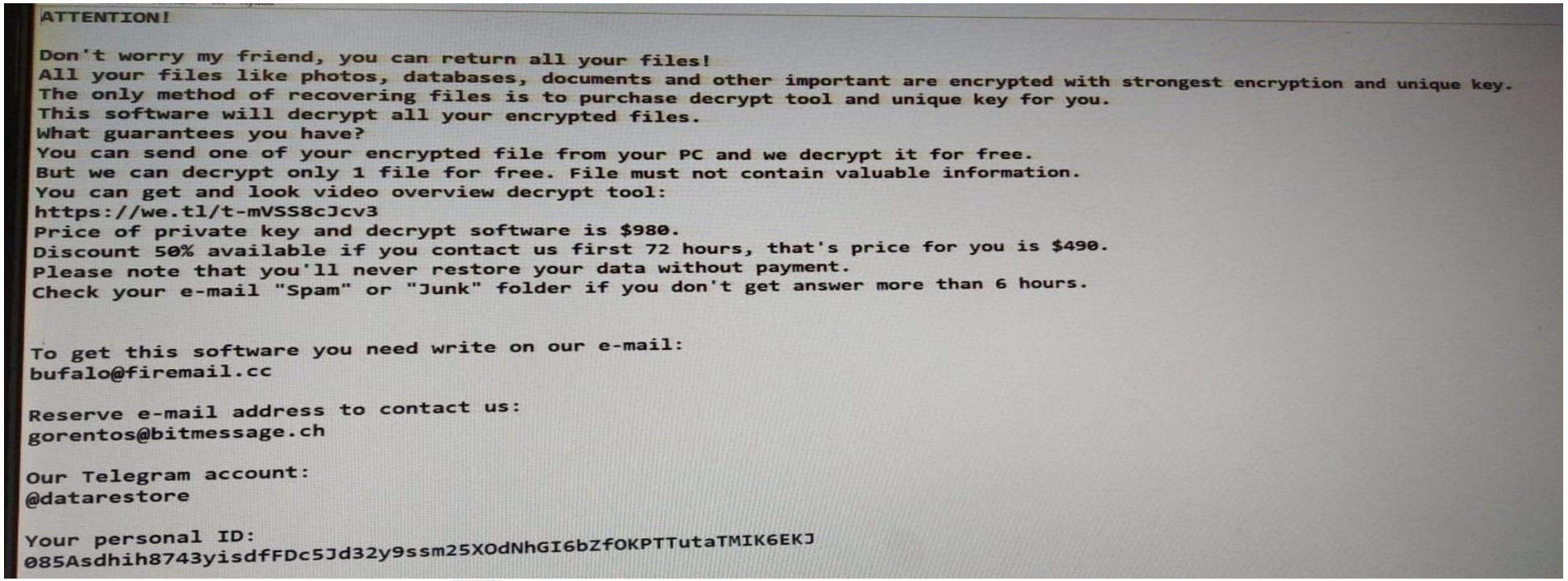
Ramsonware

- ***Concepto:*** software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados.

TIPOS DE RAMSONWARE

1. ***Winlocker:*** Ransomware de SMS, el cual bloquea el sistema y exige el envío de un Mensaje de texto a un número de tarifación adicional con un código. O tambien solicitando un pago para desbloquear el dispositivo por medio de algún sistema de pago en línea.
2. ***Ransomware de MBR:*** Este malware modifica el Master Boot Record (MBR) esto interrumpe el proceso de arranque, lo que origina que el usuario o pueda iniciar el sistema y por ende no puede eliminar la infección.
3. ***Cifrado de ficheros:*** Cifra los archivos de carpetas personales impidiendo el acceso a ellas, para poder recuperar la información o el acceso a las carpetas secuestradas se tiene que efectuar un pago a los ciberdelincuentes para que proporcionen la clave de descifrado, en algunos casos se bloquea el acceso al sistema.

Ejemplo de Ramsonware



```
ATTENTION!

Don't worry my friend, you can return all your files!
All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-mVSS8cJcv3
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
bufalo@firemail.cc

Reserve e-mail address to contact us:
gorentos@bitmessage.ch

Our Telegram account:
@datarestore

Your personal ID:
085Asdhih8743yisdfFDc5Jd32y9ssm25XOdNhGI6bZfOKPTTutaTMIK6EKJ
```

Definiciones a tener en cuenta

Malware: Consiste en un software malicioso que infecta a un equipo informático de manera ilícita, y puede ser de varios tipos, como: virus, troyanos, spyware, entre otros.

Virus: Son programas informáticos que tienen la capacidad de replicarse de manera oculta, tras instalarse sin permiso del usuario, y que pueden **generar graves afectaciones de funcionamiento en el equipo informático** infectado.

Gusano: Al igual que un virus, se replica automáticamente, sin embargo, se diferencia de este porque no requiere de un software para alojarse en la computadora de la víctima, y **ataca principalmente a la red y al ancho de banda**.

Definiciones a tener en cuenta

Troyano: Se presenta inicialmente como un software legítimo, pero al ser instalado, concede acceso remoto al atacante sobre el equipo informático de la víctima, pudiendo manejarlo casi a su antojo.

Spyware: **Software espía** se trata de un programa dedicado a la recopilación y transmisión de información del usuario a otro lugar, sin su consentimiento.

Buenas prácticas para minimizar los riesgos de un ataque informático

1- Contraseñas:

- ✓ No anotar las contraseñas en ningún lado que sea susceptible de robo
- ✓ No revelar sus contraseñas en ningún tipo de comunicación a través de Internet.
- ✓ Crear contraseñas sólidas
- ✓ No reutilizar sus contraseñas en distintas aplicaciones o en sus cuentas personales y corporativas.
- ✓ Cambiar regularmente las contraseñas. Se recomienda como mínimo cada 6 meses.

2 - Backups: Resguardar periódicamente la información crítica (documentos, planillas, archivos importantes, etc) en algún lugar fuera de la PC de trabajo (DVD, disco externo, pendrive, etc).

Buenas prácticas para minimizar los riesgos de un ataque informático

3- Protocolo HTTPS : Al utilizar la red informática de la empresa para visitar sitios web o registrarse para usar servicios , antes de enviar información, deben tratar de localizar el candado y el protocolo HTTPS en la barra de direcciones. Si el sitio web no está protegido, se debe evitar introducir ningún dato. La “s” final, significa que la página web es segura y que toda la información depositada en la misma viajará de manera cifrada.

4- Comprobar que el link es una url válida: URL: (Localizadores Uniformes de Recursos) que son un subconjunto de las URIs (Identificadores Universales de Recursos). Las URL contienen la forma de acceder a un recurso: el protocolo de acceso (http, ftp, news, etc.), el servidor en el que se encuentra el recurso (y el puerto) y el camino o ruta dónde se encuentra el recurso.

Cuáles son las partes de una URL?

http://www.miweb.com/carpeta/pagina.html#top

1 2 3 4 5 6 7

1- Protocolo
2 - Subdominio
3 - Dominio
4 - TLD (Top Level Domain), extensión o terminación
5 - Sub-carpeta o directorio
6 - Página
7 - Etiqueta

Cuáles son las partes de una URL?

1- a) El **HTTP** (Hypertext Transfer Protocol), **protocolo de transferencia de hypertexto** .

b) HTTPS (protocolo seguro de transferencia de hypertexto). Basado en el protocolo HTTP, el HTTPS es la versión segura de transferencia de datos en internet.

2- Subdominio es un subgrupo del nombre del dominio que se puede o no utilizar con fines organizativos

3- Dominio hace referencia al nombre único que identifica a un sitio web

Cuáles son las partes de una URL?

4- Extensión del dominio, también conocido como terminación o TLDs, es la parte final de una dirección web y que nos indica la naturaleza del mismo dominio.

5- Carpeta o directorio es esa parte de una URL que no indica que dentro del mismo hay una página y que se suele utilizar para organizar de forma ordenada la estructura de una página web.

6- Página o ruta hace referencia a un fichero o archivo de la página web.

7- Etiqueta es una referencia interna a un contenido de una página.

Seguridad en Redes Sociales

- **Las redes sociales son muy populares y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware.**

- **Se debe tener en cuenta y aplicar las siguientes medidas preventivas:**

a) ***Intentar no publicar información sensible y confidencial.***

b) ***Evitar la publicación de fotografías propias y de familiares.***

c) ***Mantener la privacidad del perfil.***

d) ***No responder las solicitudes de desconocidos.***

Seguridad en Redes Sociales

❑**Se debe tener en cuenta y aplicar las siguientes medidas preventivas:**

d) ***Ignorar los mensajes que ofrecen material pornográfico, pues usualmente a través de ellos suele canalizarse la propagación de malware.***

e) ***No abrir contenidos con spam a través de este medio.***

f) ***Cambiar periódicamente la contraseña.***

g) ***Configura correctamente la privacidad de tus perfiles sociales.***

Seguridad en Redes Sociales

h) Controla y elimina el acceso a tus datos de las aplicaciones que hayas instalado.

i) Ser cuidadosos y verificar que la red en la cual estoy conectado es segura. Si utilizo una red pública (wifi público) tiene ciertos riesgos ya que una red pública no tiene la protección que una red privada ofrece.

MUCHAS GRACIAS!!