Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI
GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2021-03

Fecha de publicación: 26/02/2021

Tema: Técnica "'Shadow Attack'" de modificación de archivos PDF firmados digitalmente

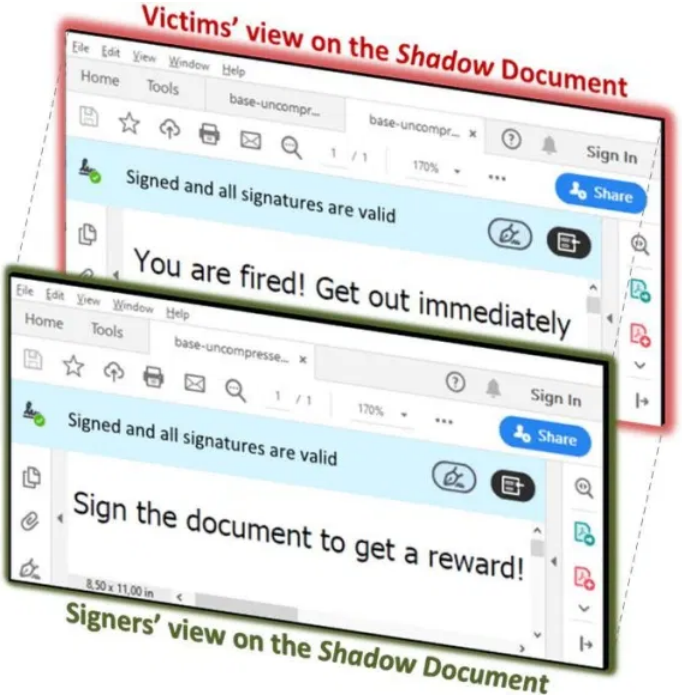
Sistemas afectados:

- Lectores de PDF populares como:
  - Acrobat (Reader, DC, Pro, etc)
  - Foxit (Reader, Phantom)
  - Nitro (Reader, Pro)
  - PDF-XChange
  - pdfforge GmbH Arquitecto PDF
  - eXpert / ExpertReader

Descripción

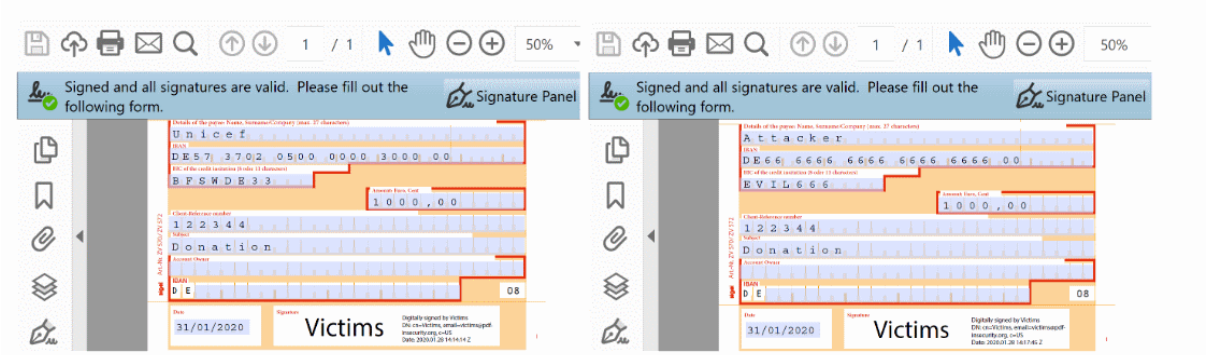
Un equipo de investigadores de seguridad han alertado sobre una técnica novedosa denominada Shadow Attack "ataques en la sombra", que permite a un atacante reemplazar el contenido de un archivos PDF firmados digitalmente eludiendo las contramedidas existentes y romper la protección de la integridad del documento.

.



El principio detrás de la técnica Shadow Attack es el concepto de "capas de vista", diferentes conjuntos de contenido que se superponen uno encima del otro dentro de un documento PDF. El atacante prepara un documento con diferentes capas y lo envía a una víctima. La víctima firma digitalmente el documento con una capa benigna encima, pero cuando el atacante lo recibe, cambia la capa visible por otra.

Debido a que la capa se incluyó en el documento original que firmó la víctima, cambiar la visibilidad de la capa no rompe la firma criptográfica y permite al atacante usar el documento legalmente vinculante para acciones maliciosas, cómo reemplazar el destinatario de pago o la suma en una orden de pago o modificación de cláusulas contractuales.



(a) A *shadow* PDF document digitally signed by the victims containing a donation amount.

(b) Manipulated PDF document after signing which contains attackers' account data.

Según el equipo de investigadores, existen tres variantes de la técnica de Shadow Attack:

- **Ocultar**: Cuando los atacantes utilizan la función Actualización incremental del estándar PDF para ocultar una capa, sin reemplazarla por ninguna otra cosa.
- **Reemplazar:** Cuando los atacantes utilizan la función de formularios interactivos del estándar PDF para reemplazar el contenido original con un valor modificado.
- **Ocultar y reemplazar:** Cuando los atacantes utilizan un segundo documento PDF contenido en el documento original para reemplazarlo por completo.

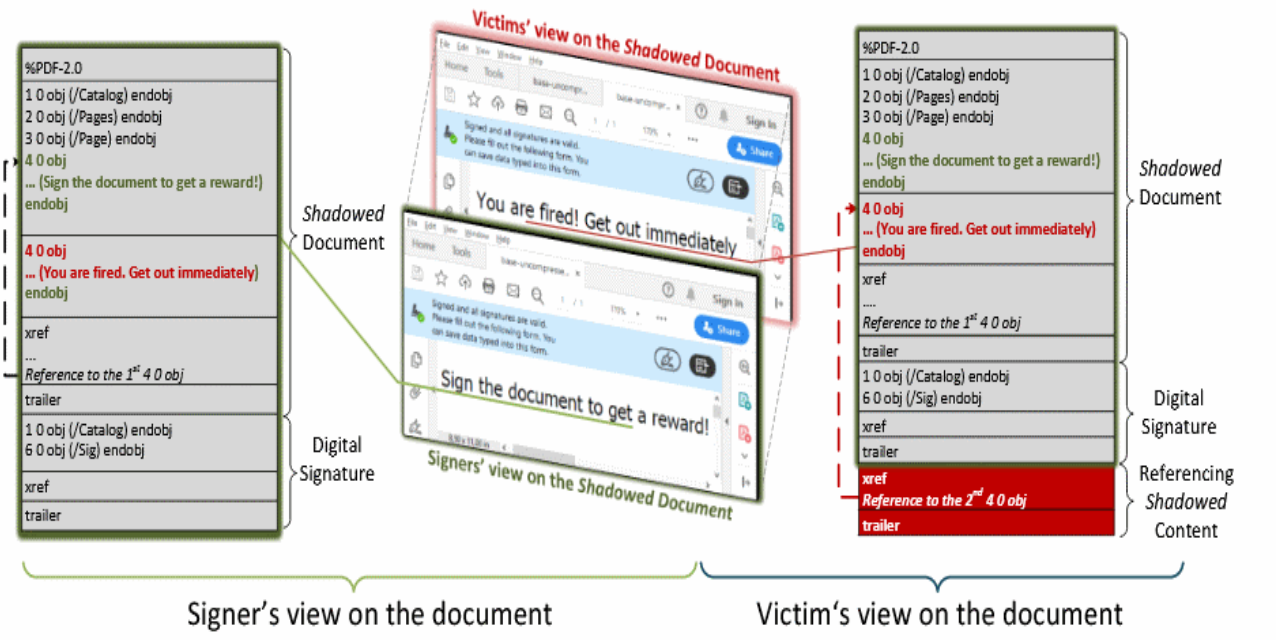


Figura: Esquema de ataque de la técnica Shadow Attack, variante : Ocultar y reemplazar".

La variante de ataque "Ocultar y reemplazar" es la más poderosa, ya que se puede intercambiar el contenido de todo el documento. El atacante puede crear un documento oculto completo que influya en la presentación de cada página, o incluso en el número total de páginas, así como en cada objeto que contiene.

La técnica se basa en vulnerabilidades en el algoritmo de verificación de firmas que afectan a los principales lectores PDF. La causa raíz de estas vulnerabilidades es que muchos lectores de documentos PDF, incluso cuando están firmados digitalmente, permiten que los objetos PDF no utilizados estén presentes dentro de su contenido. De 28 aplicaciones de visualización de PDF de escritorio analizadas, 15 son vulnerables al nuevo ataque.

En el caso de Acrobat, por ejemplo, las mismas fueron, identificadas con CVE-2020-9592 y CVE-2020-9596. Algunos de las aplicaciones afectadas son: Adobe Acrobat, Foxit Reader, LibreOffice Draw, Nitro, etc. La lista exhaustiva puede observarse en el siguiente cuadro:

Application	Version		Shadow Attack Category: Hide	Replace	Hide-and-Replace	Summary
Adobe Acrobat Reader DC	2019.021.20061	Windows	●	●	●	●
Adobe Acrobat Pro 2017	2017.011.30156		●	●	●	●
Expert PDF 14	14.0.25.3456 64-bit		◐	◐	◐	◐
Foxit Reader	9.7.0.29455		○	●	●	●
Foxit PhantomPDF	9.7.0.29478		○	●	●	●
LibreOffice Draw	6.2.5.2 (x64)		○	◐	◐	◐
Master PDF Editor	5.4.38, 64 bit		○	●	●	●
Nitro Pro	12.16.3.574		◐	◐	◐	◐
Nitro Reader	5.5.9.2		◐	◐	◐	◐
PDF Architect 7	7.0.26.3193 64-bit		◐	◐	◐	◐
PDF Editor 6 Pro	6.5.0.3929		●	●	●	●
PDFelement	7.4.0.4670		●	●	●	●
PDF-XChange Editor	8.0 (Build 331.0)		◐	◐	◐	◐
Perfect PDF Reader	V14.0.9 (29.0)		◐	◐	◐	◐
Perfect PDF 8 Reader	8.0.3.5		●	●	●	●
Perfect PDF 10 Premium	10.0.0.1		●	●	●	●
Power PDF Standard	3.0 (Patch-19154.100)		●	●	●	●
Soda PDF Desktop	11.1.09.4184 64-bit		○	◐	◐	◐
Adobe Acrobat Reader DC	2019.021.20061	macOS	●	●	●	●
Adobe Acrobat Pro 2017	2017.011.30156		●	●	●	●
Foxit Reader	3.4.0.1012		●	●	●	●
Foxit PhantomPDF	3.4.0.1012		●	●	●	●
Master PDF Editor	5.4.38, 64 bit		○	○	○	○
PDF Editor 6 Pro	6.8.1.3450		○	○	○	○
PDFelement	7.5.7.2895		○	○	○	○
Master PDF Editor	5.4.38, 64 bit	Linux	○	●	●	●
LibreOffice Draw	6.0.7.3		○	◐	◐	◐
		∑ 27	11● 6◐	15● 9◐	15● 9◐	15● 9◐

● Application vulnerable ◐ Vulnerability limited ○ Not vulnerable

Las aplicaciones de visor de PDF que eliminan objetos PDF no utilizados al firmar un documento son inmunes a la técnica de Shadow Attack.

Además, se descubrieron otras vulnerabilidades críticas en Adobe Acrobat y Reader, algunas de ellas pueden derivar en la ejecución de código arbitrario.

Solución y prevención

- En caso de que utilice alguno de los lectores de PDF afectados, actualícelo. En el caso de Adobe Acrobate, puede hacerlo mediante uno de los siguientes métodos:
    - Los usuarios pueden actualizar sus instalaciones de productos manualmente seleccionando Ayuda> Buscar actualizaciones.
    - Los productos se actualizarán automáticamente, sin requerir la intervención del usuario, cuando se detecten actualizaciones.
    - El instalador completo de Acrobat Reader se puede descargar desde el Centro de descarga de Acrobat Reader.

- Para administradores de TI (entornos gestionados):
    - Identifique todos los sistemas que cuenten con alguno de los software afectados y actualícelos.
- En caso de que su organización cuente con documentos firmados digitalmente con una versión vulnerable, en caso de que tenga dudas de que pueda haber sido alterado con esta técnica, verifíquelos con la versión actualizada de tal manera a asegurar su integridad.

Referencias

- https://pdf-insecurity.org/download/report-pdf-signatures-2020-03-02.pdf
- https://helpx.adobe.com/security/products/acrobat/apsb20-24.html
- https://thehackernews.com/2021/02/shadow-attacks-let-attackers-replace.html
- https://unaaldia.hispasec.com/2021/02/tecnica-permite-modificar-ficheros-pdf-con-firma-digital.html