## Recent attacks allow replacing content in signed PDF files


*Security Researchers from the Ruhr University Bochum (Germany) have disclosed a series of new attack methods, dubbed **Shadow attacks**, against signed PDF files.*

## Modus Operandi

Researchers from the Ruhr University Bochum (Germany) have devised a series of new attack techniques, dubbed **Shadow attacks**, against signed PDF files.

Last February 2019, the same group of security experts discovered some flaws in popular PDF viewers and online validation services that allow to deceive the digital signature validation process.

This threat can allow an attacker to manipulate the content of a signed PDF document keeping its signature valid. The attacker can create a document with two different contents:

- the content expected by the authority reviewing and signing the PDF;
- the hidden content that will be displayed once the PDF document will be signed.

*According to the researchers, The Signers of the PDF receive the document, review it, and sign it. The attackers use the signed document, modify it slightly, and send it to the victims. After opening the signed PDF, the victims check whether the digital signature was successfully verified. However, the victims see different content than the Signers.*

## Attack Variants

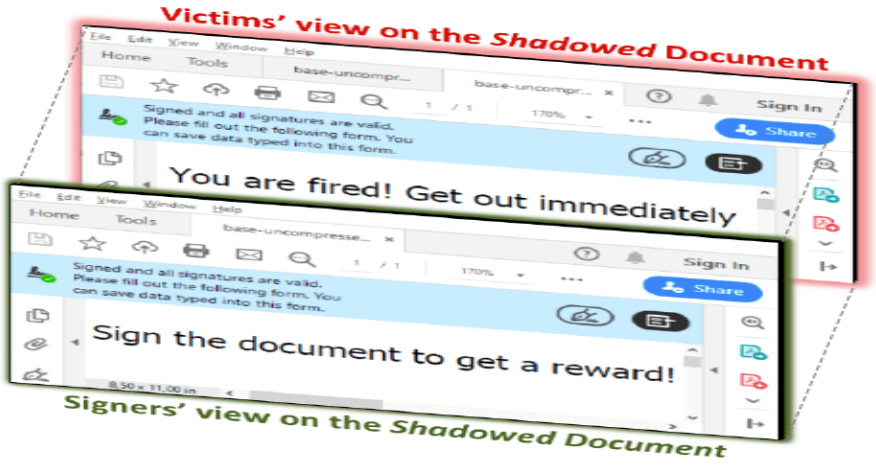
The researchers devised three different variants of the Shadow Attacks, allowing to ***Hide*, *Replace*, and *Hide-and-Replace*** content in digitally signed PDFs. The experts tested their attacks against 28 PDF viewer applications and later found out that 15 of them were vulnerable to at least one of the attacks. The list of vulnerable viewers includes **Adobe, Foxit,** and **LibreOffice.**

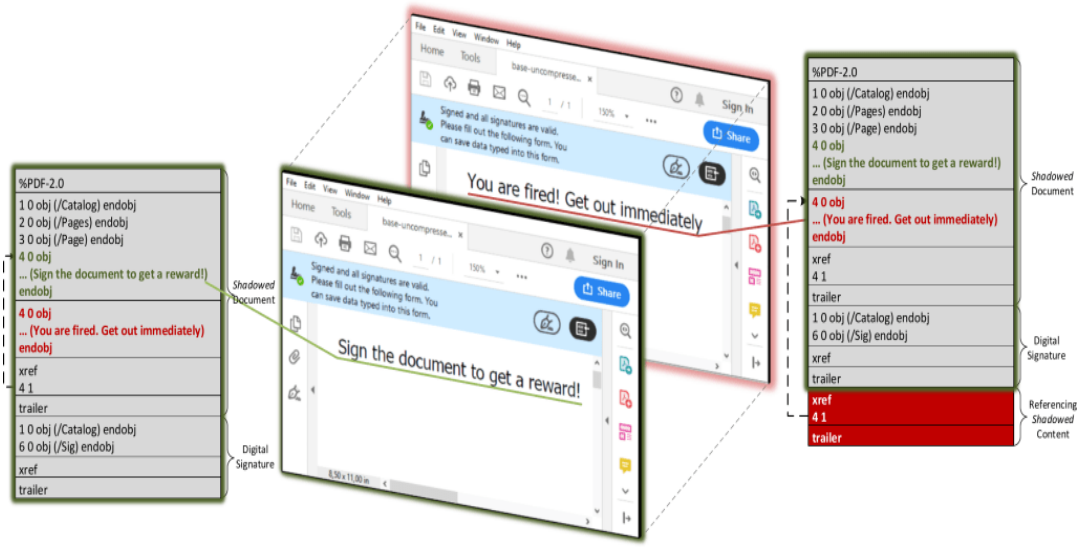
The software firms behind these three applications have already released security fix to prevent Shadows attacks, unfortunately, many other companies behind impacted apps did not respond to the researchers.

The vulnerabilities exploited by the researchers in the Shadow attacks are tracked as CVE-2020-9592 and CVE-2020-9596.

1. **Hide**

The “Hide” variant of the Shadow Attacks consists in hiding a portion of the content in a PDF behind another layer, such as a full-page image. The attacker sends a document to the signer that contains an image placed on top of the content to hide. Once the document has been signed and sent back to the attacker, they can manipulate it to hide the image from the PDF viewer.



2. **Replace**

The “Replace” attack sees the attacker appending an object to a signed document, the object is considered harmless and can impact the way the content is presented. This variant' main purpose is to append new objects to the signed document which are considered harmless but directly influence the presentation of the signed content.

3. **Hide and Replace**

The “Hide-and-Replace” variant, allows an attacker to change the entire content of a signed document. The attacker inserts both hidden and visible content into the document using two objects that have the same object ID, and sends it to the signer. Once the attacker receives the signed document, they will append a new Xref table and a new Trailer so that the hidden content is displayed.

In Hide-and-Replace attack variant, the PDF document contains a second, hidden document with different content. Since the signers cannot detect the hidden (malicious) content, they sign the document. After signing, the attackers receive the document and append only a new Xref table table and Trailer. Within the Xref table table, only one change takes place: the reference to the Description.”

**References:**

https://www.zdnet.com/article/new-shadow-attack-can-replace-content-in-digitally-signed-pdf-files/

https://www.google.com/url?sa=i&source=imgres&cd=&cad=rja&uact=8&ved=2ahUKEwjepOa06-7qAhXYFIgKHZ5RDkYQjRx6BAgBEAQ&url=https%3A%2F%2Fappleinsider.com%2Farticles%2F19%2F02%2F25%2Fthe-best-pdf-apps-to-use-for-editing-redacting-and-for-ocr-in-macos-mojave&psig=AOvVaw0NG6L7bWIAR03HJSjqa17M&ust=1595987636696438

https://securityaffairs.co/wordpress/106403/hacking/shadow-attacks.html?web_view=true

https://www.forbes.com/sites/zakdoffman/2019/10/05/critical-pdf-warning-new-threats-leave-millions-at-riskupdate-all-pdf-apps-now/#6a7df227739d