Untersuchung und Klarstellung zu den Angriffen

XiTrust, die eSignature Company, erklärt was es mit dem auf den Namen "Shadow Attacks" getauften Angriffsschema auf sich hat und stellt die aktuell möglichen Abläufe anhand der Signaturlösung MOXIS und dem am häufigsten genutzten PDF Reader der Firma Adobe transparent dar.

Auf Papier unterschriebene Dokumente lassen sich recht leicht manipulieren, indem man z.B. die Seiten vor jener mit der Unterschrift heimlich austauscht. In der digitalen Welt bieten sogenannte digitale PDF-Signaturen weit mehr Sicherheit. Digital unterschriebene PDFs sind nachträglich für gewöhnlich nicht mehr manipulierbar, ohne dass die Signaturprüfung der PDF-Software die Änderungen bemerkt und meldet.
Vor Kurzem hat aber ein Forscherteam der Ruhr-Universität Bochum drei potenzielle Methoden entdeckt, die Signaturprüfung bei PDF-Dokumenten zu manipulieren und zu umgehen.
Die Forscher kommunizierten die Schwachstellen über das CERT-Bund des BSI im Rahmen eines Responsible-Disclosure-Prozesses an die Hersteller. Das ist ein gängiger Prozess in der IT-Sicherheit und gibt Herstellern Zeit vor der Veröffentlichung von Schwachstellen ihre Software mit Updates abzusichern.

Die Manipulationsversuche lassen sich in drei theoretische Shadow Attack-"Angriffsszenarien" unterteilen die wir hier näher ausführen:

Hide Strategie

Bei der Hide Strategie werden schädliche Inhalte hinter Bildern oder durch die Erstellung von unsichtbarem Text versteckt. In diesem Fall ist der unsichtbare Text immer noch im PDF, Sie können ihn nur nicht sehen. Nach dem Signieren entfernt der Angreifer dieses Bild und das Dokument wurde von einigen PDF-Betrachtern nicht als ungültig angesehen.

Status in Moxis:

Moxis prüft vor dem Signieren nicht, ob Text durch ein Bild verdeckt ist. Wir testen noch ob es sinnvoll ist, dass Moxis in Zukunft prüft, ob Text hinter einem Bild versteckt ist, indem es prüft, ob ein Objekt über einem anderen Objekt liegt.

XITRUST THE ESIGNATURE COMPANY
Creating security, developing quality.

XITRUST
Secure Technologies GmbH

Am Nordpark 1
41069 Mönchengladbach
Deutschland
EUROPE

KONTAKT

Telefon DE | +49 2161 549 99 78
Telefon AT | +43 6 991 410 2032

E-Mail | office@xitrust.com
Web | https://www.xitrust.com

UNTERNEHMEN

HRB | 72554
Gerichtsstand | Düsseldorf
IBAN | DE38 3005 0110 1006 9191 85
BIC | DUSSDEDDXXX
USt-IdNr. | DE295158299

Status im Adobe Reader:

Die meisten Viewer wie der Adobe Reader prüfen bereits, ob das Dokument nach dem Unterzeichnungsprozess auf diese Weise verändert wurde, und kennzeichnen das Dokument in so einem Fall als ungültig.

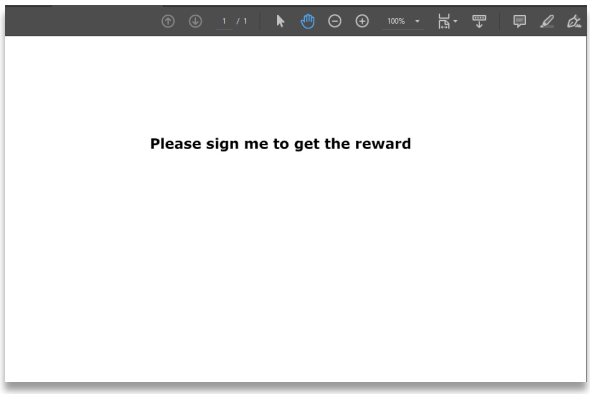


Bild 1.1: Dokument vor der Signatur

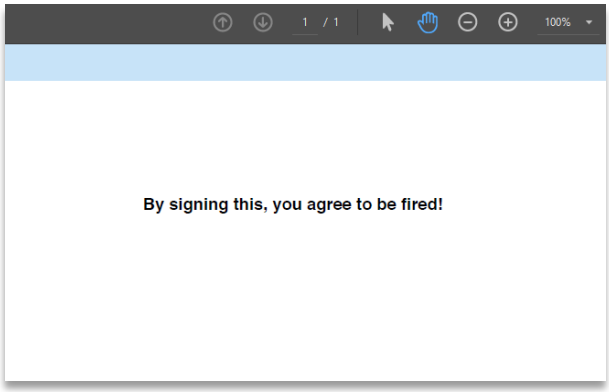


Bild 1.2: Dokument nach der Signatur und Manipulation durch Entfernen von Inhalten.

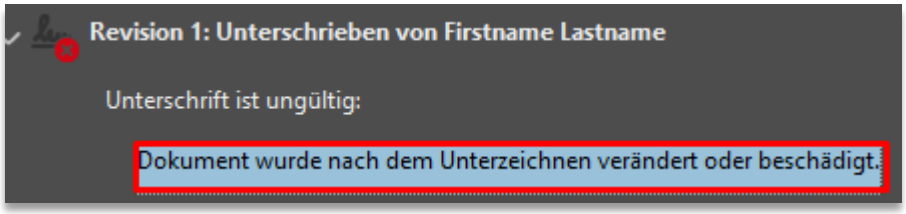


Bild 1.3: Warnung im Adobe Reader

XITRUST
THE ESIGNATURE COMPANY
Creating security, developing quality.

XITRUST
Secure Technologies GmbH
Am Nordpark 1
41069 Mönchengladbach
Deutschland
EUROPE

KONTAKT
Telefon DE | +49 2161 549 99 78
Telefon AT | +43 6 991 410 2032
E-Mail | office@xitrust.com
Web | https://www.xitrust.com

UNTERNEHMEN
HRB | 72554
Gerichtsstand | Düsseldorf
IBAN | DE38 3005 0110 1006 9191 85
BIC | DUSSDEDDXXX
USt-IdNr. | DE295158299

Replace Strategie

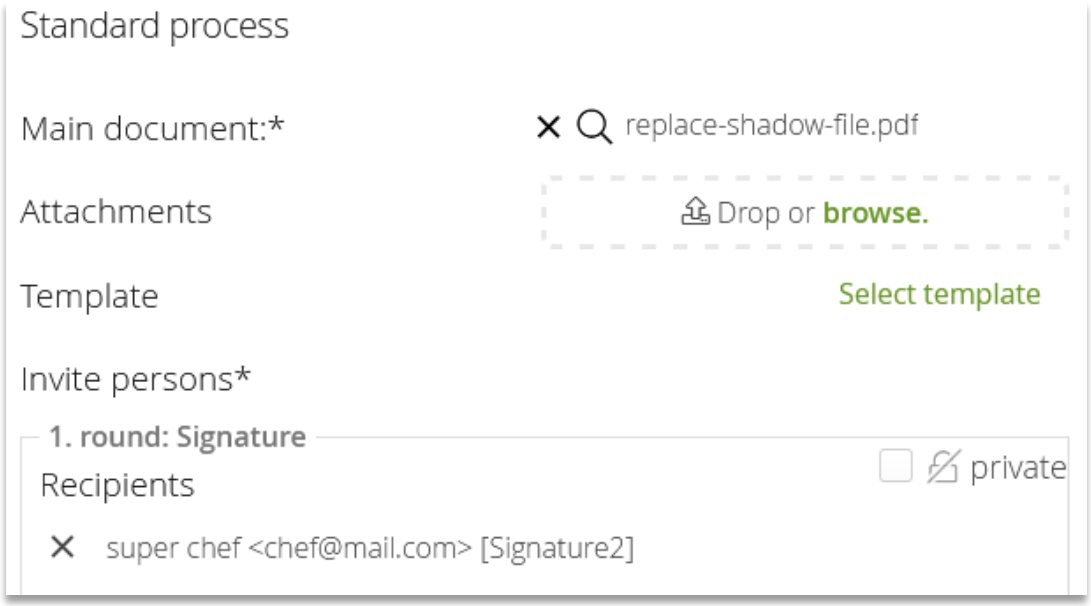
Bei dieser Strategie werden Objekte nach dem Signieren durch unerwünschte Inhalte ersetzt. In den meisten Fällen werden Textfelder verwendet. (In unserem Beispiel ist der Preview-Wert des Textfeldes: SaveWorldGmbh, Und der schädliche Wert des Feldes: Attacker) Nach dem Signieren manipuliert der Angreifer die Objekte durch eine "Schriftartänderung" mit einer eigens erstellten Schrift die andere Zeichen anzeigt. Normalerweise verändert die (Neu-)Definition von Schriften den Inhalt nicht direkt; selbst-definierte Schriften erlauben es aber, Zahlen oder Buchstaben beliebig zu vertauschen.

Status in Moxis:

MOXIS kann dies im Signaturprozess nicht überprüfen, da diese Änderung erst nach dem Unterzeichnungsprozess vorgenommen wird. Es wäre möglich, die Werte der definierten Textfelder auszulesen und zu überprüfen, ob die Vorschau und der Wert des Feldes gleich sind. Da dies aber zu falsch positiven Ergebnissen führen könnte ist eine Implementierung eines Prüfprozesses nicht sinnvoll. Auch zeigt MOXIS den primär angezeigten Text eines Textfeldes während dem Signiervorgang bereits an.

Wenn man jedoch die von MOXIS signierte Datei manipuliert und erneut hochlädt, wird eine signierte Datei z.B. zur Bezahlung des Angreifers angezeigt. Was dazu führen könnte, dass ein anderer Benutzer das Dokument in dem Glauben unterschreibt, dass es richtig ist, weil jemand anderes es bereits unterschrieben hat.

Beispielprozess:



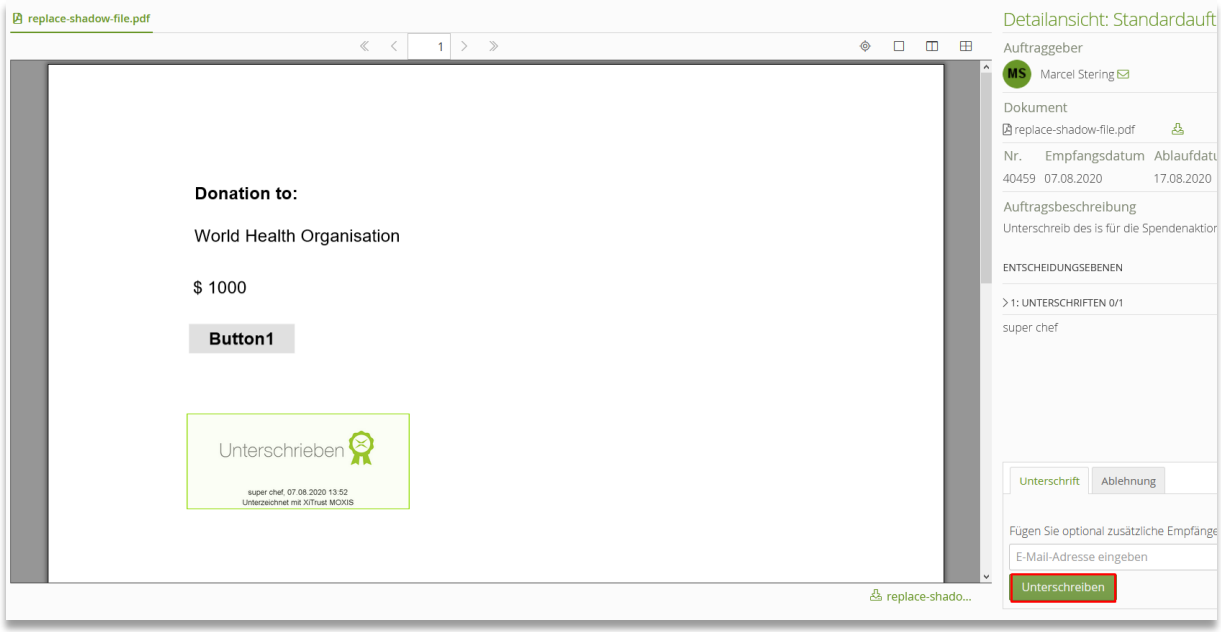
Erstellung eines Signaturprozesses für den Geschäftsführer.

XITRUST
THE ESIGNATURE COMPANY
Creating security, developing quality.

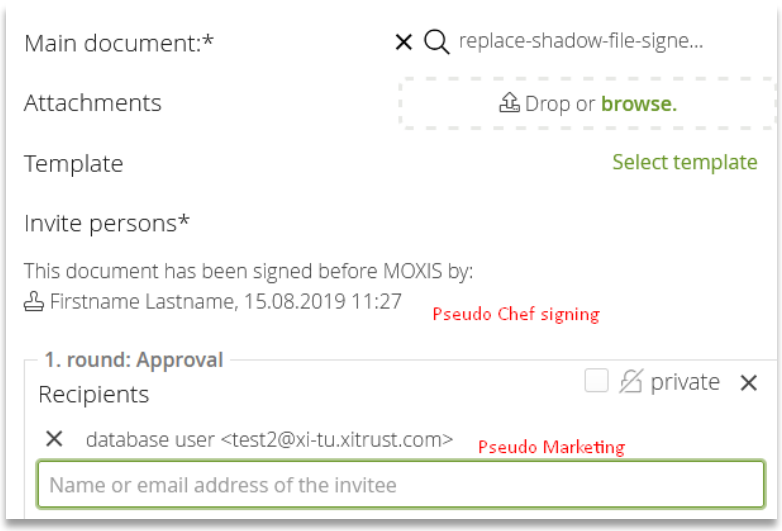
XITRUST
Secure Technologies GmbH
Am Nordpark 1
41069 Mönchengladbach
Deutschland
EUROPE

KONTAKT
Telefon DE | +49 2161 549 99 78
Telefon AT | +43 6 991 410 2032
E-Mail | office@xitrust.com
Web | https://www.xitrust.com

UNTERNEHMEN
HRB | 72554
Gerichtsstand | Düsseldorf
IBAN | DE38 3005 0110 1006 9191 85
BIC | DUSSDEDDXXX
USt-IdNr. | DE295158299



Geschäftsführer sigiert das Dokument.



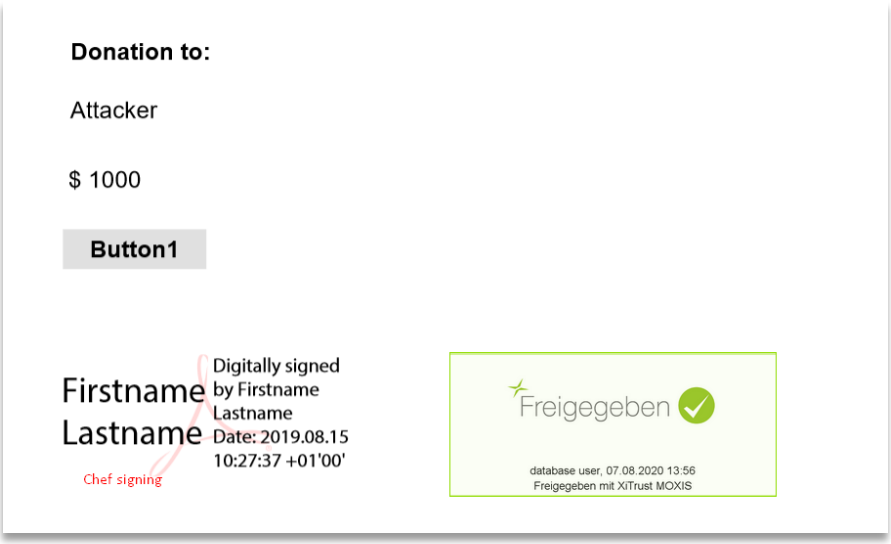
Angreifer bekommt das signierte Dokument, verändert es und lädt es erneut auf MOXIS um damit einen neuen Freigabeprozess ans Marketing zu schicken.

XITRUST
THE ESIGNATURE COMPANY
Creating security, developing quality.

XITRUST
Secure Technologies GmbH
Am Nordpark 1
41069 Mönchengladbach
Deutschland
EUROPE

KONTAKT
Telefon DE | +49 2161 549 99 78
Telefon AT | +43 6 991 410 2032
E-Mail | office@xitrust.com
Web | https://www.xitrust.com

UNTERNEHMEN
HRB | 72554
Gerichtsstand | Düsseldorf
IBAN | DE38 3005 0110 1006 9191 85
BIC | DUSSDEDDXXX
USt-IdNr. | DE295158299



Marketing erhält diesen Auftrag zur Genehmigung und ist vielleicht verwirrt, warum der Chef dies unterschrieben hat, aber es genehmigt eventuell trotzdem und führt die Überweisung durch.

Status in Adobe:

Bei Adobe zeigt der Viewer das signierte Dokument als dasjenige mit dem Wert der signiert wurde an, so dass dieser Angriff bei Adobe nicht mehr funktioniert. Die Manipulation stößt auf einen Fehler, der dazu führt, dass der Objektaustausch nicht akzeptiert wird. Manche PDF-Viewer zeigen hingegen noch das manipulierte PDF an. Wer verwundbare, bislang nicht abgesicherte PDF-Software nutzt, sollte daher die Auflistung verfügbarer Updates bei PDF Insecurity ebenso im Blick behalten wie entsprechende Herstellerhinweise.

Bild 2.4 Adobe Reader

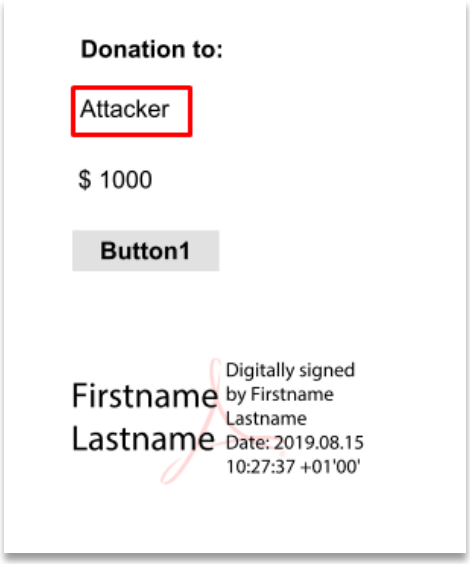


Bild 2.5 Anderer PDF Viewer

XITRUST
THE ESIGNATURE COMPANY
Creating security, developing quality.

XITRUST
Secure Technologies GmbH
Am Nordpark 1
41069 Mönchengladbach
Deutschland
EUROPE

KONTAKT
Telefon DE | +49 2161 549 99 78
Telefon AT | +43 6 991 410 2032
E-Mail | office@xitrust.com
Web | https://www.xitrust.com

UNTERNEHMEN
HRB | 72554
Gerichtsstand | Düsseldorf
IBAN | DE38 3005 0110 1006 9191 85
BIC | DUSSDEDDXXX
USt-IdNr. | DE295158299

Hide and Replace Strategie

Die Angriffsvariante „Shadow Attack Hide-and-Replace“ versteckt ein zweites, vollständig definiertes PDF-Dokument mit anderem Inhalt in dem sichtbaren Dokument. In diesem Fall wird ein Dokument mit einer verborgenen Beschreibung eines anderen Dokuments erstellt. Der Unterzeichner kann also während des Signierens den verborgenen Inhalt nicht sehen. Dieser wird vom Angreifer durch Hinzufügen einer xref zum Katalog, die das verborgene Dokument wieder sichtbar macht angezeigt werden.

Status in Moxis:

Moxis prüft nicht, ob es versteckte Objekte gibt, die vor der Unterzeichnung nicht referenziert werden. Aber alle getesteten Dokumente mit diesen Manipulationen weisen beim Hochladen einen Fehler aus, weil der Platzhalter für die Signatur einen Null-Zeiger auf den getPages() Wert des Widgets hat, hauptsächlich wegen der Erstellung und dem Ausblenden eines anderen Dokuments in dem PDF.

Status in Adobe:

Auch Adobe zeigt in diesem Fall in der aktuellen Version, dass die Dateien nach der Unterzeichnung manipuliert wurden.

Zusammenfassung:

Es ist wichtig die neueste Version Ihres PDF-Viewers zu verwenden. Diese können bei den meisten Anbietern mit allen beschriebenen Exploits sehr gut umgehen.
Eigene Prüfprozesse in MOXIS zu implementieren ist höchstwahrscheinlich in den meisten Fällen nicht sinnvoll, da neuere PDF-Viewer ohnehin Überprüfungen implementiert haben. Vor allem aber werden die meisten Angriffe nach der Unterzeichnung durchgeführt. Da in MOXIS jedes Dokument in dem Zustand, in dem es unterzeichnet wurde auch nachträglich heruntergeladen werden kann ist jede nachträgliche Manipulation nach dem Signaturprozess beweis- und dokumentierbar.

XITRUST
THE ESIGNATURE COMPANY
Creating security, developing quality.

XITRUST
Secure Technologies GmbH

Am Nordpark 1
41069 Mönchengladbach
Deutschland
EUROPE

KONTAKT

Telefon DE | +49 2161 549 99 78
Telefon AT | +43 6 991 410 2032

E-Mail | office@xitrust.com
Web | https://www.xitrust.com

UNTERNEHMEN

HRB | 72554
Gerichtsstand | Düsseldorf
IBAN | DE38 3005 0110 1006 9191 85
BIC | DUSSDEDDXXX
USt-IdNr. | DE295158299