CIRCOLARE n. 9-2019

ERRORI NELLA RICEZIONE E NELL'INVIO DELLE PEC

Campagna di phishing veicolata su PEC con finti riferimenti a fatture firmate

Carissime e carissimi,

molti di noi, negli ultimi giorni, hanno riscontrato gravi problemi nell'utilizzo della casella PEC.

Il problema si è presentato in particolare per coloro che utilizzano il sistema operativo Windows 7 unitamente a vecchi programmi di messaggistica quali, ad esempio, Outlook 2007, Windows mail ecc.

Poiché tutto ciò è dovuto all'implementazione del nuovo protocollo di comunicazione (il TLS 1.2., imposto a tutti i gestori dei servizi di Posta Certificata dall'Agenzia per l'Italia Digitale (AgID)), **l'unico modo per ovviare al problema è di utilizzare client di posta e sistemi operativi aggiornati.**

Non è possibile proporre una soluzione valida per tutti perché ogni singola postazione di lavoro ha le sue peculiarità e va quindi affidata ad un tecnico qualificato che sappia effettuare i necessari upgrade software e, eventualmente, hardware.

Mi permetto di segnalarvi che, dal 14 gennaio 2020, la Microsoft dovrebbe cessare ogni supporto all'efficientissimo Windows 7 e, pertanto, vi suggerisco di effettuare -sin da ora- un upgrade efficace che vi eviti di doverne eseguire un altro tra pochi mesi.

Nel frattempo, per coloro che hanno riscontrato problemi, vi segnalo che è possibile -e consigliato- l'utilizzo della PEC tramite il WEB (ad es. per chi opera con il dominio *@pec.ordineavvocativiterbo.it , l'indirizzo cui accedere è: https://webmail.pec.it/index.html).

Secondariamente, ma non per importanza, molti di noi hanno di recente ricevuto delle PEC anomale provenienti da società ignote e contenenti presunte fatture con estensione *.p7m.

Come già vi segnalammo con la precedente circolare n°5/2019,

PRESTATE LA MASSIMA ATTENZIONE E NON APRITE QUEI FILES.

Trattasi infatti di una massiva campagna di phishing veicolata su PEC con finti riferimenti a fatture firmate, il tutto come da avviso pubblicato su https://www.cert-pa.it che vi inviamo in allegato.

Un caro saluto a tutti.

Il Presidente del COA
Avv. Marco Prosperoni

VIA FALCONE E BORSELLINO N°41
01100 VITERBO

TEL. (0761) 360808 - FAX 250478
E-MAIL: segreteria@ordineavvocativiterbo.it

Massiva campagna di Phishing veicolata su PEC con finti riferimenti a fatture firmate (.p7m)

10/10/2019

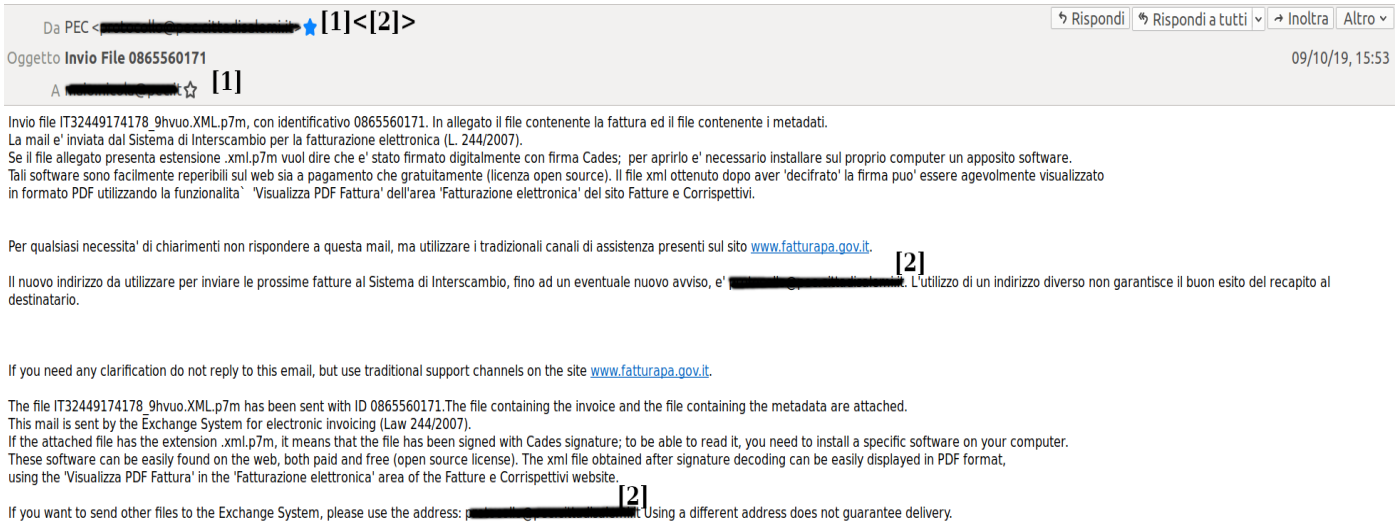
malspam pec phishing

Il CERT-PA ha rilevato l'esistenza di una campagna malevola osservata per la prima volta in data 05/10/2019 veicolata da PEC italiane compromesse, indirizzata ancora una volta **verso indirizzi di posta riferibili a caselle PEC di strutture pubbliche, private e di soggetti iscritti a ordini professionali.**

Le mail malevole, aventi come oggetto **"Invio File <XXXXXXXXXX>",** menzionano un allegato dal nome *ITYYYYYYYYYY_1bxpz.XML.p7m* che comunque non compare come file all'interno dell'email.

L'assenza dell'allegato potrebbe far pensare a una "dimenticanza" e quindi a una campagna errata, ma considerata la modalità con cui è stata strutturata la mail, è chiaro che si tratti di phishing mirato alla "raccolta di informazioni", probabilmente in attesa di un successivo attacco mirato. Infatti, la comunicazione fa riferimento a un **"***nuovo indirizzo da utilizzare per inviare le prossime fatture al Sistema di Interscambio***",** tale indirizzo coincide sempre con il mittente della casella compromessa controllata dall'attaccante.

Di seguito uno screenshot del phishing veicolato:


Da PEC <[redacted]> [1]<[2]>

Rispondi | Rispondi a tutti | Inoltra | Altro

Oggetto **Invio File 0865560171**

09/10/19, 15:53

A [redacted] [1]

Invio file IT32449174178_9hvuo.XML.p7m, con identificativo 0865560171. In allegato il file contenente la fattura ed il file contenente i metadati.
La mail e' inviata dal Sistema di Interscambio per la fatturazione elettronica (L. 244/2007).
Se il file allegato presenta estensione .xml.p7m vuol dire che e' stato firmato digitalmente con firma Cades; per aprirlo e' necessario installare sul proprio computer un apposito software.
Tali software sono facilmente reperibili sul web sia a pagamento che gratuitamente (licenza open source). Il file xml ottenuto dopo aver 'decifrato' la firma puo' essere agevolmente visualizzato in formato PDF utilizzando la funzionalita` 'Visualizza PDF Fattura' dell'area 'Fatturazione elettronica' del sito Fatture e Corrispettivi.

Per qualsiasi necessita' di chiarimenti non rispondere a questa mail, ma utilizzare i tradizionali canali di assistenza presenti sul sito www.fatturapa.gov.it.

Il nuovo indirizzo da utilizzare per inviare le prossime fatture al Sistema di Interscambio, fino ad un eventuale nuovo avviso, e' [redacted] [2]. L'utilizzo di un indirizzo diverso non garantisce il buon esito del recapito al destinatario.

If you need any clarification do not reply to this email, but use traditional support channels on the site www.fatturapa.gov.it.

The file IT32449174178_9hvuo.XML.p7m has been sent with ID 0865560171.The file containing the invoice and the file containing the metadata are attached.
This mail is sent by the Exchange System for electronic invoicing (Law 244/2007).
If the attached file has the extension .xml.p7m, it means that the file has been signed with Cades signature; to be able to read it, you need to install a specific software on your computer.
These software can be easily found on the web, both paid and free (open source license). The xml file obtained after signature decoding can be easily displayed in PDF format, using the 'Visualizza PDF Fattura' in the 'Fatturazione elettronica' area of the Fatture e Corrispettivi website.

If you want to send other files to the Exchange System, please use the address: [redacted] [2] Using a different address does not guarantee delivery.

Si osserva che:

- il display name [1] del mittente del messaggio di phishing corrisponde all'indirizzo PEC di un appartenente ad un ordine professionale e coincide con l'indirizzo destinatario;
- il mittente effettivo [2] è una casella PEC di una società italiana.

Dalle indagini effettuate dal CERT-PA, in collaborazione con i gestori PEC, risultano essere state sfruttate circa **500** account PEC compromesse per inviare un totale di **265.000** messaggi di phishing negli ultimi 7 giorni.

Aggiornamenti:

- I phisher hanno clonato una comunicazione PEC lecita emessa a inizio mese da Sogei contestualmente al Sistema di Interscambio.
- Il corpo della mail contiene al suo interno un richiamo ad una risorsa remota, trattasi di un meccanismo di tracking che si abilita all'apertura della mail e punta al seguente dominio: "**pattayajcb[.]com**"

```
<IMG width=1 height=1 alt="" src="https://pattayajcb.com/certificato/
notifica.php?STlqaKQLALQi1wvmai1DCpLroL1Lf1NGP4ru8V9qp6pMBnOcVYvW08kZbq/
sZT1Jr9iA/jHapcXpNdHxDhxIhqfli1wkCER7xr2/
GVaZDWvPoTnln+nmCCWpAQiSPLSeFFWFqu75J0KicRRlfC2Qrg==">
```

Conclusioni

La campagna di diffusione risulta in corso a danno di molte utenze italiane titolari di caselle PEC. Si consiglia pertanto non dar seguito a comunicazioni PEC provenienti da utenze "sconosciute" e che richiedono di modificare l'indirizzo di recapito per le successive comunicazione con il Sistema di Interscambio.