Istruzioni per l'individuazione di messaggi PEC contenenti virus

versione 1.0 – 29 novembre 2019

Negli ultimi mesi sono arrivati messaggi PEC contenenti virus, anche da indirizzi insospettabili (es. enti pubblici), che evidentemente sono stati compromessi.

Come identificarli

Ecco alcuni suggerimenti su come identificarli:

1) scaricare dalla bozza di Titulus il file "Ricezione Telematica.eml". Vedi Figura 1
2) aprire il file con Thunderbird o un altro programma di posta elettronica
3) esaminare il contenuto, soprattutto gli allegati o eventuali link

Mittente: potrebbe essere presente nelle anagrafiche Titulus e anche appartenere ad un Ente pubblico, oppure non avere mai interagito con l'Ateneo.

Oggetto: potrebbe fare riferimento a fatture, documenti giudiziali o a procedimenti universitari (es. Richiesta conferma titolo di studio). Dobbiamo prestare ugualmente attenzione.

Testo: nel caso sia presente un link per scaricare un documento INSOSPETTIRSI! Verificare attentamente che l'indirizzo del sito web sia attendibile e coerente col contenuto del messaggio. Vedi Figura 2.

Allegati: sono lo strumento principale con cui vengono installati i virus. Bisogna fare attenzione all'estensione dei file (le ultime tre lettere dopo il punto)

- zip: INSOSPETTIRSI!
  Estrarre il contenuto del file per vedere se contiene file descritti sotto. Viene usato per evitare che i software antivirus analizzino i file inviati (soprattutto se protetto da una password presente nel messaggio). Vedi Figura 3 e Figura 4.
- exe, pif, msi, com, bat, cmd, vbs ed altri: **VIRUS!**
  NON cliccare mai su questo tipo di file! Se lo fate potreste non notare subito comportamenti anomali del PC, ma contattate tempestivamente un tecnico informatico. Non sempre l'antivirus riesce a riconoscerli. Vedi Figura 3.
- docx, xlsx, odt, ods e tutti i file Office: ATTENZIONE!
  Potrebbero contenere MACRO che installano virus. Se all'apertura del file, Word chiedesse di eseguire MACRO, non fatelo mai. Vedi Figura 4.

Nel caso di ulteriori dubbi contattare un tecnico informatico oppure aprire un ticket nella coda: "Archivio corrente – gestione PEC".

Cosa fare

Una volta accertato che il messaggio contiene un virus si devono fare le seguenti operazioni:

1) assegnare una classificazione (es. 1/7), rimanendo in bozza
2) registrare la bozza come SPAM
3) inserirla in un fascicolo informatico con oggetto: "ATTENZIONE - Posta elettronica certificata - PEC - DOCUMENTI DA NON APRIRE PERCHE' CONTENGONO VIRUS"

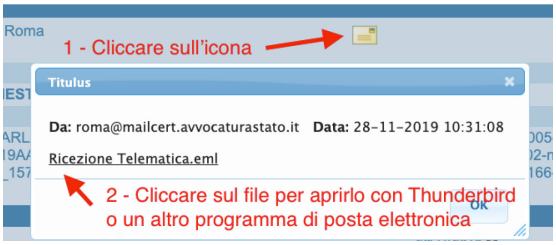

Figura 1 - Aprire sempre il file "Ricezione Telematica.eml"

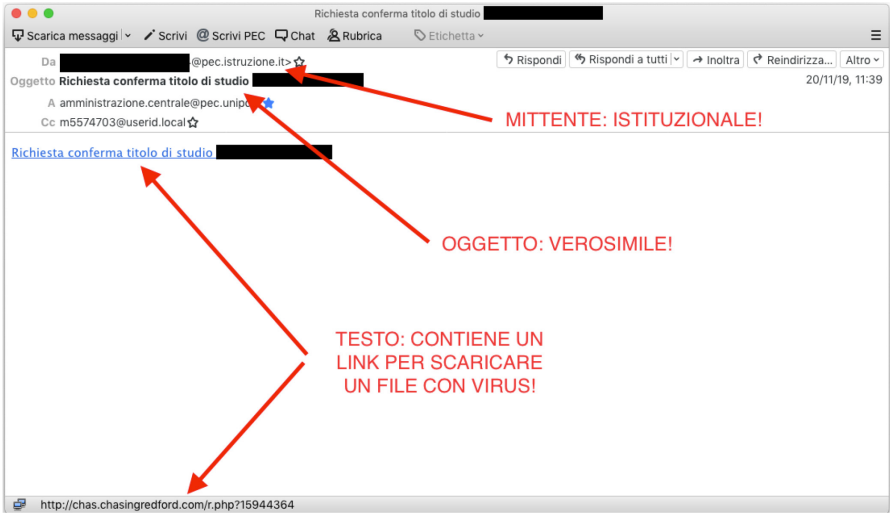

Figura 2 – Testo del messaggio che contiene un link sospetto, l'indirizzo non è coerente con il contenuto della PEC

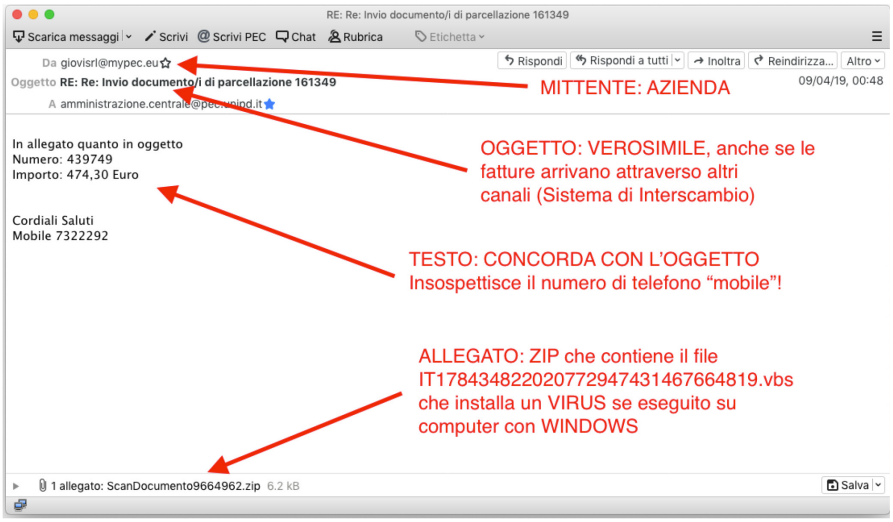

Figura 3 - Nel messaggio è presente un allegato ZIP, che contiene un file VBS che, se cliccato, installa un VIRUS.

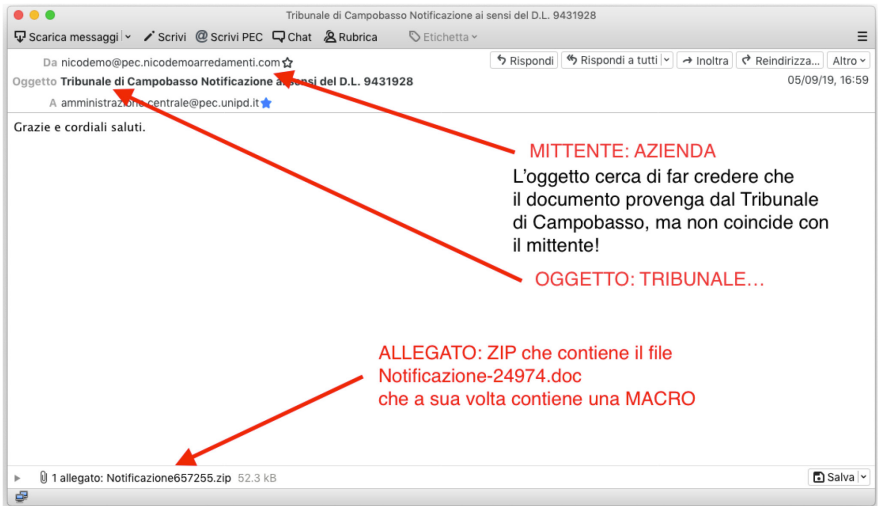

Figura 4 - Nel messaggio è presento un file ZIP, che contiene un file DOC, che, se aperto con Word, chiede di eseguire una MACRO che installa un Virus

Approfondimenti

Da molti anni la posta elettronica "tradizionale", cioè non certificata, viene utilizzata per l'invio di:

1) SPAM: pubblicità non richiesta;
2) PHISHING: messaggi che ci inducono a digitare le nostre credenziali ("nome utente" e "password") su siti non attendibili, ma con l'aspetto di siti istituzionali (es. webmail, banca, ecc.), per carpire la nostra "identità digitale";
3) VIRUS: messaggi che contengono allegati malevoli oppure link a siti web per scaricare file malevoli che, una volta aperti/eseguiti sul proprio computer, installano programmi che possono avere conseguenze più o meno dannose. Ad esempio:
    a. programmi che cercano di "infettare" il maggior numero di computer presenti in rete, spesso intasando la rete stessa *(worm);*
    b. programmi che permettono l'accesso remoto al proprio computer da parte di male intenzionati, che prendono il controllo per PC per portare avanti altri attacchi. Es. rubare credenziali di accesso, accedere a sistemi protetti (basi di dati/applicazioni), inviare SPAM, attaccare sistemi esterni senza essere riconosciuti, ecc. *(trojan);*
    c. programmi che cifrano i file presenti nel computer e chiedono il pagamento di un riscatto (solitamente in bitcoin) per permettere di recuperare i propri dati *(ransomware);*
    d. programmi che spiano le nostre attività sul computer, spesso per rubare le credenziali (mail, banca, ecc.) *(spyware);*
    e. programmi che mostrano messaggi pubblicitari nel computer oppure attraverso pagine web, senza la nostra volontà *(adware)*.

La presenza sul proprio PC di un software antivirus aggiornato **diminuisce**, NON annulla, il rischio di essere "infettati".
Anche i fornitori di caselle di posta elettronica talvolta verificano la presenza di messaggi malevoli, cancellando i messaggi o indicando nell'oggetto la possibile presenza di virus [FORSE VIRUS] o [FORSE SPAM], così come anche alcuni client di posta (es. Thunderbird o Outlook), ma non possono essere considerati del tutto affidabili.

L'invio di messaggi di posta elettronica, contrariamente a quanto comunemente si crede, non richiede un'autenticazione esplicita con delle credenziali. Inoltre è possibile, abbastanza facilmente, inviare e-mail inserendo come mittente il nome di un'altra persona, senza essere quindi identificabili. L'unico modo per risalire alla persona che ha inviato l'e-mail è l'indirizzo di rete, ma è molto difficile individuare la persona che sta utilizzando un indirizzo di rete, soprattutto se proveniente dall'estero.

L'utilizzo della Posta Elettronica Certificata (PEC) ha portato numerosi vantaggi:

- tutti i computer che gestiscono i messaggi PEC sono noti e individuabili,
- per inviare una PEC devi essere identificato con delle credenziali,
- le credenziali vengono rilasciate previa identificazione "debole", almeno con l'invio al fornitore di documento di identità e codice fiscale. Non è prevista l'identificazione "de visu" come per le firme digitali o SPID.

Nonostante questi miglioramenti, l'accesso alle caselle PEC avviene sempre tramite credenziali: "nome utente" e "password". Quindi se una persona, non autorizzata, utilizza le credenziali di qualcun altro, può inviare messaggi malevoli. Le credenziali possono essere rubate oppure "indovinate" nel caso vengano utilizzate password semplici. Purtroppo non è possibile ritenere attendibile il contenuto dei messaggi solo perché provengono da indirizzi PEC.
Le PEC in ateneo sono gestite attraverso il protocollo informatico Titulus 97, sia in partenza che in arrivo.
Negli ultimi mesi abbiamo notato un aumento di messaggi PEC malevoli, che vengono registrati direttamente all'interno di Titulus come bozze e non sono sempre facilmente individuabili.
Di seguito alcuni suggerimenti per poter individuare messaggi PEC malevoli:

MITTENTE
È l'indirizzo PEC da cui proviene il messaggio. Ricordiamo che la PEC è solo un mezzo di trasmissione e quindi il mittente non coincide necessariamente con l'autore del contenuto del messaggio, es. il firmatario del documento allegato.
Contrariamente alla posta elettronica NON certificata, l'indirizzo deve esistere ed essere attivo. Può essere di due tipologie principali:

1) registrato in un elenco pubblico:
    a. Pubbliche amministrazioni: IPA (Indice PA) https://indicepa.gov.it/documentale/n-ricerca-avanzata.php#R10
    b. Imprese: INIPEC https://www.inipec.gov.it/cerca-pec/-/pecs/companies
    c. Professionisti: INIPEC https://www.inipec.gov.it/cerca-pec/-/pecs/professionals
2) NON registrato in un elenco pubblico:
    a. Privati cittadini
    b. PEC utilizzate da imprese/professionisti non presenti in INIPEC (solo una è presente nel registro imprese)
    c. PEC utilizzate da pubbliche amministrazioni non presenti in IPA

Se il mittente non ha mai avuto contatti con la nostra amministrazione o riteniamo che non corrisponda con l'autore del messaggio dovremmo alzare la nostra soglia di attenzione per messaggi sospetti.
Anche nel caso l'indirizzo sia noto, ad esempio è presente nelle nostre anagrafiche, non c'è la certezza che sia affidabile.
Nelle ultime settimane sono arrivati messaggi da indirizzi da cui avevamo ricevuto documenti via PEC corrette o a cui avevamo inviato dei documenti. Sembrerebbe quindi che quelle caselle siano state compromesse e un male intenzionato abbia cominciato ad inviare PEC a tutti gli indirizzi trovati tra i mittenti/destinatari precedenti.

OGGETTO
Nei messaggi PEC malevoli l'oggetto è formulato per indurci a farci credere della sua genuinità e della sua importanza. Può fare riferimento a fatture, documenti giudiziali e fare riferimento a procedimenti dell'amministrazione. Esempi:

- Fattura 854272019
- diffida al pagamento 5393273
- Tribunale di Campobasso Notificazione ai sensi del D.L. 9431928
- RE:: Invio certificato ai sensi dell'art 72 del DL n 1632006 e DPR n 2072010 relativo al nuovo complesso di Medicina Veterinaria

- Conferma RicezioneConvenzione di tirocinio di formazione ed orientamento
- RILASCIO CERTIFICATO MASTER 2 LIVELLO CARDIOLOGIA DELLO SPORT 20172018

Ultimamente sembra che alcuni oggetti siano ricopiati (in tutto o in parte) da messaggi già inviati o ricevuti da quel mittente, rendendo più difficile distinguere le PEC affidabili da quelle malevoli.

TESTO

Il testo o corpo del messaggio potrebbe non essere molto significativo, spesso riporta il testo dell'oggetto. Nel caso la PEC non contenga allegati, l'unico modo per "infettare" il nostro computer è quello di farci scaricare un file, quindi nel messaggio sarà presente un link ad una pagina web. Non sempre quello che si legge a video corrisponde alla pagina web del link. Per vederne il contenuto si posiziona il mouse sul link, SENZA cliccare, e nella barra di stato (il bordo in basso del programma di posta) compare l'indirizzo. Di solito è un indirizzo sconosciuto, spesso di domini stranieri. Ecco alcuni esempi:

- http://jays.meganjohnson.net/r.php?73821858
- http://chas.chasingredford.com/r.php?15944364

Anche se solamente scaricare il file senza aprirlo o eseguirlo (vedi la sezione ALLEGATI) non "infetta" automaticamente il computer, **è altamente sconsigliato cliccare sul link!**

Alcuni browser, come Chrome, impediscono di raggiungere alcuni siti web se si clicca accidentalmente sul link, perché evidentemente sono già stati segnalati come siti pericolosi. A volte sono siti genuini che sono stati compromessi da male intenzionati.

Alcuni messaggi contengono invece link affidabili per permettere di scaricare documenti corretti, in questo caso bisogna essere sicuri dell'indirizzo del link che si vuole raggiungere.

ALLEGATI

I messaggi PEC contengono spesso allegati perché è il metodo principale con cui inviare documenti. Es. con firma digitale o copie di documenti con firma autografa, copie di carte d'identità, ecc. Bisogna fare molta attenzione al tipo di allegati presenti, ecco una **lista di file su cui prestare attenzione:**

- **ZIP:** è un formato per comprimere la dimensione dei file e permette di inviare più documenti in un unico file, talvolta è anche protetto con password. Viene usato per evitare che i software antivirus analizzino i file inviati, di solito tra quelli elencati al punto successivo, quindi bisogna prestare molta attenzione. Nelle PEC attendibili è probabile che il documento principale sia un PDF e nello ZIP siano contenuti allegati corposi, es. planimetrie, ecc.
- **EXE, PIF, MSI, COM, BAT, CMD, VBS,** ecc.: questo tipo di file eseguono automaticamente un programma quando vengono cliccati. **Sono lo strumento principale con cui vengono installati i virus nei computer.** Anche i software antivirus aggiornati potrebbero non individuarli perché cambiano molto frequentemente.
- **DOCX, XLSX, ODT, ODS e tutti i file Office**: normalmente non sono pericolosi, ma permettono l'inserimento all'interno dei file delle MACRO, cioè programmi che possono eseguire istruzioni per "infettare" il computer. Nonostante i programmi recenti di Office (es. Word, Excel, Openoffice, ecc.) mostrino un'allerta in presenza di MACRO e non le eseguano automaticamente, bisogna prestare attenzione, ricordando che il formato corrente più utilizzato per i documenti è il PDF. Le MACRO hanno attualmente un utilizzo molto limitato quindi **NON eseguire mai le MACRO** anche se richiesto (es. "Abilitare le MACRO per visualizzare il contenuto del file".