ALLERTA ATTACCO VIA EMAIL

25/03/2020

[Fonte Cert-PA]

Circolano in questi giorni e-mail e PEC che, facendo leva sull'emergenza corona virus, promuovono prodotti dalle dubbie funzionalità. In alcuni casi si tratta di veri e propri **malware**, in altri casi vengono pubblicizzati strumenti per il telelavoro di produttori minori ed arrivisti.

Al di là dell'effettivo valore dei software promossi, è bene ricordare che con la necessità del telelavoro si aggiunge, per i lavoratori, una maggiore responsabilità per la sicurezza del proprio computer.

Sebbene sia facile, lavorando su un dispositivo che fino a qualche settimana fa era destinato all'uso privato, dimenticarsi del contesto *sensibile* in cui lo si usa (quando, ad esempio, accediamo ad applicativi critici e dati sensibili), ed al contempo sia difficile accettare restrizioni sull'utilizzo di un computer proprio, è necessario adottare **misure extra di sicurezza** ed una **maggiore attenzione alle truffe**.

Le amministrazioni ed i datori di lavoro possono controllare gli aspetti di sicurezza tecnici che sono necessari in una situazione di lavoro da remoto ma non possono controllare il *fattore umano* e, in questa emergenza, **è facile cadere in errore**.

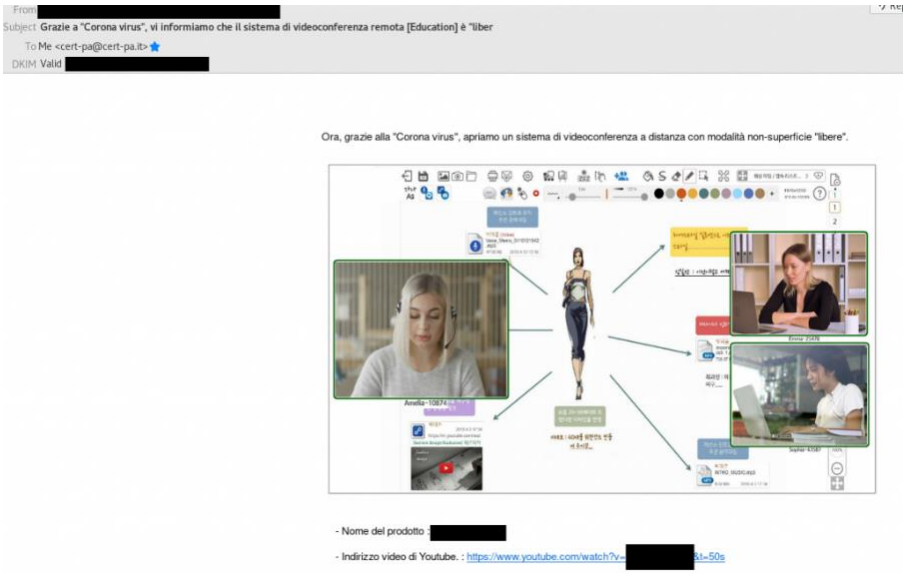
Se vengono rubate le password per l'accesso ai gestionali di lavoro, delle caselle PEC dell'amministrazione o il nostro computer diviene, a nostra insaputa, parte di una rete di attacco, il danno che i criminali possono infondere si estende a tutta la comunità / PP.AA e si profilano una serie di danni collaterali di difficile contenimento (ad esempio, un account PEC compromesso è spesso usato per tentare di infettare massivamente migliaia di altri account, l'accesso ad informazioni sensibili da parte di terzi non può essere "annullato", e così via).

E' necessario quindi ricordare una serie, non esaustiva, di accorgimenti generali a cui attenersi.

Non installate software

Soprattuto se a seguito di sollecitazioni via e-mail. Nel caso sia un tecnico della vostra Amministrazione a richiedere l'installazione, **verificate attentamente il contesto**: l'e-mail era attesa? le frasi sono scritte con grammatica corretta? il software da installare ha un fine specifico? Eventuali link nell'e-mail puntano a siti conosciuti? il mittente è corretto?

Abbiamo riscontrato in questi giorni, campagne pubblicitarie di prodotti per il telelavoro.

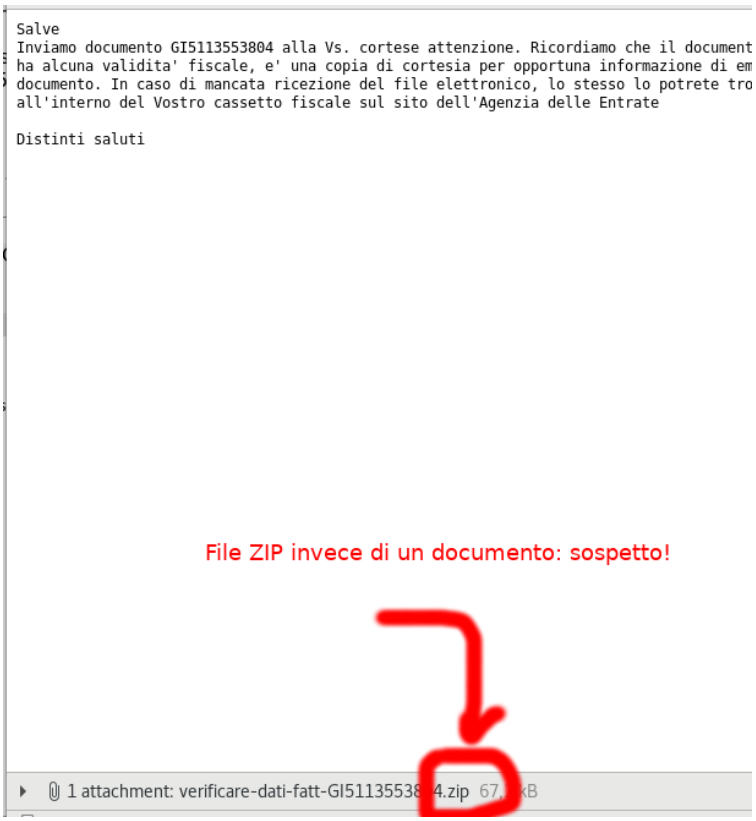


Qualsiasi sia la natura e qualità del prodotto, è meglio **rimandare l'esplorazione di nuovo software** a momenti di minor necessità. Il software che installiamo sul nostro computer oggi può essere pericoloso per quando domani mattina useremo lo stesso computer per lavorare da remoto (lavoro agile – smart working).

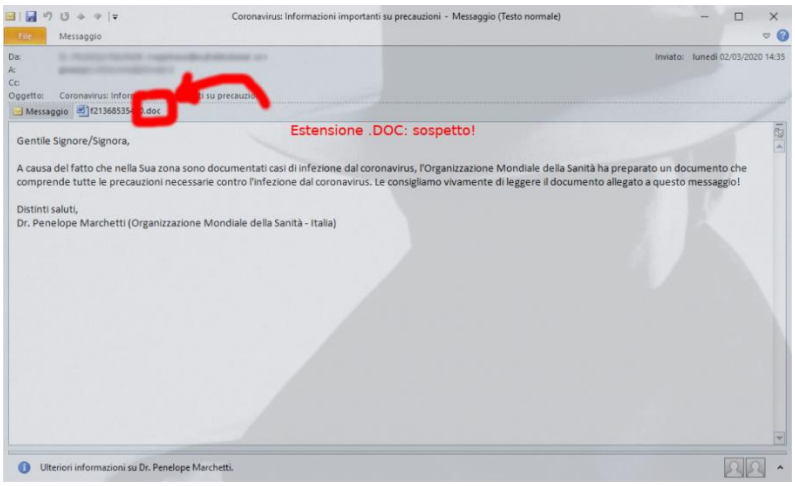
Documenti via email

Normalmente i criminali si attengono al tema dei pagamenti, degli ordini o delle tasse per invogliarci a farci aprire un documento Word o Excel; inutile dire che anche *il tema corona virus è stato usato per questi fini*.

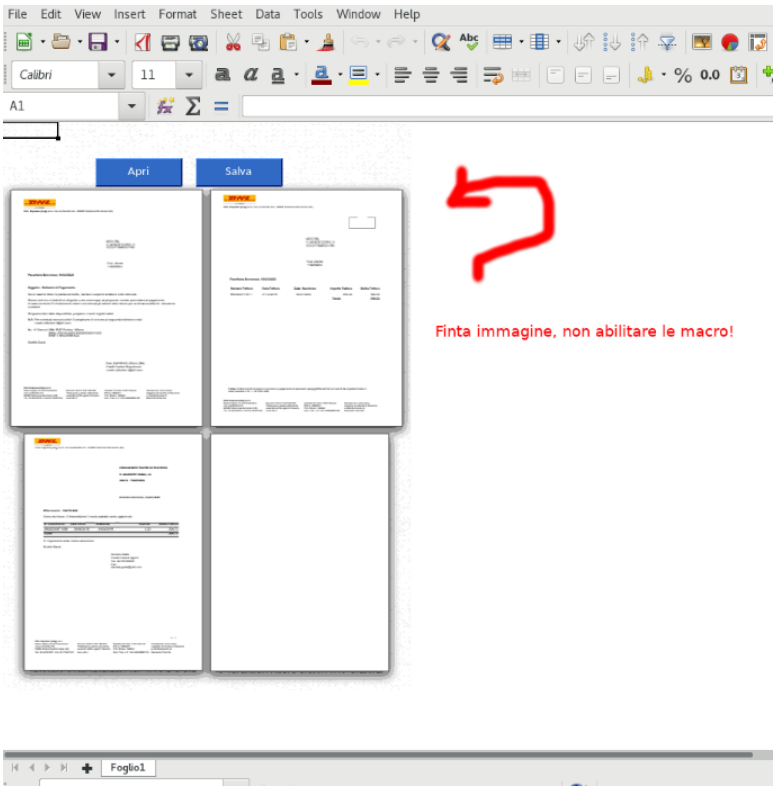
Ricordiamoci che nessuna Autorità o persona invierebbe comunicati dentro archivi compressi (allegati con estensione ZIP, RAR, TAR, GZ). Il formato preferenziale per le comunicazioni è PDF o P7M, questi formati (specie il primo) non è totalmente assente da brutte sorprese ma è più difficile condurvi un attacco completo.



I documenti Word possono contenere macro malevole ma nelle versioni recenti queste sono usabili solo in formati appositi. Prima di aprire un documento Word verificare che l'**estensione sia DOCX e non DOCM o DOC**. Quest'ultimo formato è usato anche da versioni molto vecchie di Word.



Analogo discorso vale per i file Excel, **XLSX è l'estensione sicura, XLSM e XLS quelle non sicure**. Purtroppo esistono meccanismi che consentono di includere (indirettamente) malware anche in documenti DOCX e XLSX, per cui queste non sono estensioni sicure al 100%. Tuttavia, l'utilizzo di queste estensioni per scopi malevoli non ha (ancora) avuto grossa diffusione, in ogni caso è meglio non aprire un documento contenuto in un'e-mail con elementi sospetti.In ogni caso non abilitare mai le macro, i criminali usano immagini e trucchi vari per fare sembrare il documento incompleto o senza formattazione. Nessuna comunicazione necessita delle macro.



Versioni molto vecchie di Office (esempio, 2010) sono vulnerabili ad alcuni attacchi. Meglio aggiornarle!

Prima di iniziare a lavorare con il proprio Pc in modalità smart-working controllare sempre che sia attivo un antivirus (anche gratuito) aggiornato e che il sistema operativo abbia scaricato gli ultimi aggiornamenti di sicurezza!