S T U D I O M A R C H I ..... *informa*

Circolare n.5 del 05/04/2017

Attenzione ai virus/malware contenuti negli allegati

Dopo alcune segnalazioni pervenuteci e dopo averlo "provato" direttamente scriviamo questo post per evitare che altri possano incappare in virus/malware simili.
Fino a qualche tempo fa, il modo più veloce per far diffondere un virus o un malware era quello di inviare delle e-mail ed ora, che i client di posta (sia software che web mail) che gli antivirus sono piuttosto efficaci nel prevenirne i danni, ecco che gli hacker cercano di generare danni o rubare informazioni mediante i servizi PEC.
Eccovi uno dei casi che ci hanno portato all'attenzione e che fa da "*caso pilota*" per tutti gli altri.

Come si presenta

Nella casella dei Messaggi in Arrivo della web mail PEC c'è un messaggio proveniente da una casella PEC reale (probabilmente una casella infetta spedisce a tutte le caselle della rubrica).

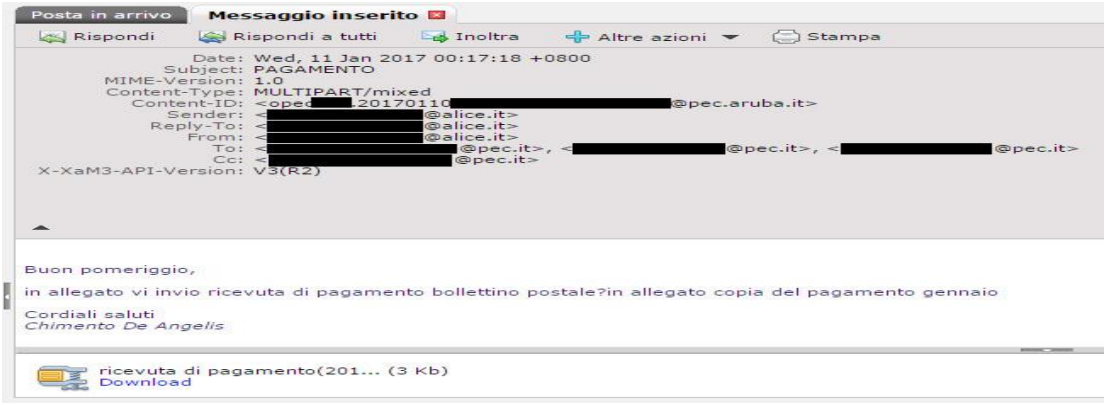
Il messaggio è accattivante "*Pagamento*" (o anche *Ricevuta di Pagamento*), chi può resistere ad un messaggio relativo ad una ricevuta di pagamento?

Il testo

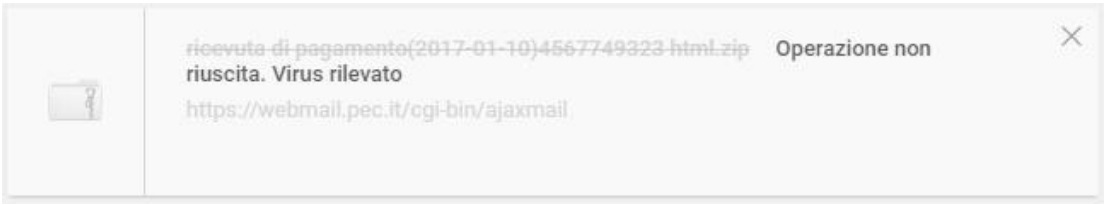
Il testo contenuto nell'e-mail PEC è solitamente questo:

> Egregio Cliente buongiorno,
>
> da un nostro controllo contabile troviamo ancora insolute le fatture scadute elencate nell'estratto conto a seguito riportato. Vi chiediamo gentilmente di controllare e provvedere a stretto giro al loro saldo.
>
> **FATTURA N. 00005799 DEL 04/04/2017 Totale: 219,94**
>
> Confidando nel Vostro sollecito riscontro, inviamo i nostri distinti saluti.

Ovviamente il firmatario sarà un nome falso e comunque, nei casi in oggetto è sempre un nominativo sconosciuto al destinatario dell'e-mail.



L'e-mail PEC è corredata di un allegato, anche questo con un nome assolutamente invogliante "ricevuta di pagamento(2017-01-10)".
A questo punto, in genere chi riceve questa email può tentare di scaricare l'allegato per vedere di cosa si tratti questa ricevuta di pagamento. Nel caso voi abbiate un buon antivirus aggiornato probabilmente il virus verrà immediatamente rilevato, come nel caso seguente nel quale il sistema rileva la minaccia e procede a bloccarne il download.



Nel caso in cui non siate protetti adeguatamente da un antivirus allora aprire il file può comportare per voi dei rischi. Vediamo quali

L'allegato (il codice malevolo)

Il file zippato allegato all'email PEC contiene un file con lo stesso nome "*ricevuta di pagamento(2017-01-10)1122334455.html.js*". I più attenti avranno notato la strana estensione di questo file. Si tratta di un file JavaScript, un tipo di linguaggio di programmazione pensato per il web e solitamente utilizzato per gli effetti dinamici ed interattivi nelle pagine web, ma che può essere anche usato da hacker per fini poco etici come rubare dati sensibili digitati nei form web o per installare estensioni malevole nel browser.
Per gli interessati vi linkiamo l'analisi di questo codice effettuata da Payload Security.

I nostri consigli

Ovviamente la prima accortezza è quella di stare attenti alle e-mail che ricevete perché la prima linea di difesa siete sempre voi utenti. Detto questo eccovi alcuni piccoli consigli per non incorrere in problemi se ricevete questa e-mail PEC o un qualsiasi altro malware simile.

1. Il primo consiglio è sicuramente quello di tenere sempre aggiornato il vostro antivirus;
2. Non scaricate mail file zip provenienti da mittenti sconosciuti;
3. Non aprite mai file con estensioni non tipiche.