17.09.2021

In circolazione un subdolo cavallo di Troia per l'eBanking

I criminali hanno preso ad annunciare telefonicamente la consegna di un pacco, mentre allo stesso tempo inviano un'e-mail con un link contenente il bollettino di consegna. In realtà, vi si nasconde un cavallo di Troia per l'e-banking.

Suona il telefono. Una signora con l'accento di un Paese dell'est informa che è stata disposta una consegna. A causa del coronavirus, ha inviato il bollettino di consegna via e-mail. Non bisognerebbe fare altro che stamparlo, firmarlo e consegnarlo al corriere. Negli ultimi tempi, in alcuni casi la voce è registrata. (Fonte: cybercrimepolice.ch)

A monte delle chiamate ci sono dei criminali, e il link nell'e-mail infetta il computer della vittima con un cavallo di Troia per l'e-banking. Una volta installato, il malware reindirizzerà le future attività di e-banking ai malintenzionati, i quali potranno modificare i pagamenti e i trasferimenti a loro vantaggio.

In questo periodo vengono contattate in particolare le PMI. Tuttavia, non si può escludere che vengano presi di mira anche i privati. L'aspetto più perfido di tutto ciò è che nemmeno gli antivirus aggiornati individuano software dannoso nel PC infetto, e la protezione della verifica via SMS viene scardinata.

Di recente, le aziende infette subiscono anche furti di dati su larga scala. Dopo diverse settimane, i dati vengono crittografati e la PMI riceve una richiesta di riscatto (ransomware (https://www.ebas.ch/ransomware)).

Per evitare di cadere in questa truffa, seguite queste regole:

- Non fate mai clic sul link contenuto nell'e-mail.
- Annotate il numero di telefono dei truffatori e segnalatelo alla polizia.
- Se avete già fatto clic sul link, contattate immediatamente il vostro istituto finanziario dicendo che potreste essere stati infettati da un cavallo di Troia per l'e-banking. Smettete di usare il computer e fatelo ripristinare da zero. Sporgete una denuncia penale alla stazione di polizia locale.
- In caso di incertezze o dubbi rivolgetevi al vostro istituto finanziario.

Ulteriori informazioni ed esempi (in tedesco) si trovano su www.cybercrimepolice.ch (https://www.cybercrimepolice.ch/de/fall/achtung-kmu-anruf-von-zustellservice-mit-ankuendigung-von-liefer-mail-ist-ein-ebanking-trojaner/) .

Inoltre, maggiori informazioni generali sull'argomento sono disponibili nel nostro articolo sul phishing (https://www.ebas.ch/it/phishing) .