Ihre POLIZEI
Votre POLICE
La vostra POLIZIA

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

SKPPSC

Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

SCHEDA TECNICA: *TRUFFA DEL FALSO SUPPORTO TECNICO (TRUFFA MICROSOFT)*

Svolgimento della truffa

Al telefono, questi truffatori si fanno spesso passare per dipendenti di Microsoft o di un help desk. Il pretesto utilizzato per telefonare può essere, per esempio, un'infezione da virus, un problema di lentezza del sistema o qualsiasi altro problema tecnico. La loro vera intenzione è tuttavia quella di convincere il loro interlocutore a lasciar prendere loro il controllo remoto del dispositivo per poi scaricarvi un programma o visitare un sito piratato, ma in apparenza esattamente identico al sito ufficiale, con il solo scopo di rubare il nome utente e le password dell'ignara vittima.

In qualche modo, i truffatori riescono ad accedere direttamente al dispositivo delle loro vittime per poi intercettare le loro password o scaricare le informazioni memorizzate sul loro computer, allo scopo di prendere meglio il controllo della vita digitale dell'utente. Dato che i sedicenti servizi d'assistenza sono talvolta a pagamento, i truffatori arrivano perfino a chiedere alle loro vittime di fornire il numero della loro carta di credito che poi utilizzeranno in modo illecito.

Nel video della seconda parte della campagna nazionale di prevenzione, che sarà lanciata l'8 settembre 2020, si racconta la storia della disavventura di Simone che ha permesso a Martino di prendere il controllo del suo computer in modo fraudolento. Ed è proprio questo il modus operandi utilizzato da Martino.

Chi chiama, si esprime spesso in un pessimo inglese. Dato che si possono manipolare i numeri di telefono, è probabile che la vittima veda apparire sul display del suo telefono il vero numero della società informatica in questione.

Capita anche sempre più spesso che questi sedicenti operatori di help desk vengano chiamati dalle loro stesse vittime. Il modus operandi è allora il seguente: mentre si naviga in Internet, sullo schermo si apre una finestra pop-up di tipo pubblicitario che informa l'utente di un presunto problema tecnico. La finestra fornisce un numero di telefono svizzero da chiamare per risolvere il problema. È a questo punto che i truffatori entrano in gioco e riescono a spillare denaro alle loro vittime per dei cosiddetti programmi anti-virus.

Perché così tanta gente ci casca?

Di fatto, sono in molti a perdere il controllo quando viene detto loro che i dati memorizzati sul loro computer sono a rischio. Dato che i truffatori sanno argomentare in modo molto professionale e offrono subito una soluzione al problema (cioè la loro assistenza online), non sorprende che siano in molti ad accettare questo aiuto con gratitudine. Inoltre, è facile per questi imbroglioni usurpare un numero di telefono esistente, per esempio quello di un'helpline, per sviare i sospetti della loro vittima la quale, vedendo apparire un numero svizzero sul display

del proprio telefono, penserà che si tratti di dipendenti di una società informatica che vogliono aiutarla.

Alcuni dati

Anche se la criminalità "classica" in materia di reati contro il patrimonio, come i furti con scasso, è notevolmente diminuita in Svizzera (-50,6% tra il 2012, anno record, e il 2019), le nuove tecnologie favoriscono verosimilmente l'espansione e lo sviluppo di nuovi modi operandi caratteristici della criminalità "digitale". Attualmente, non esistono statistiche ufficiali a livello nazionale per le truffe del falso supporto tecnico (truffe Microsoft), ma sui 286'207 reati contro il patrimonio commessi nel nostro Paese nel 2019, le truffe sono state 17'606, pari al 6,2%. Rispetto al 2018, queste truffe sono aumentate del 7,9%, e una parte di questo aumento è molto probabilmente riconducibile allo sviluppo di modi operandi digitali.

Consigli utili

Da tenere sempre presente!

Che si tratti di Microsoft o di una qualsiasi altra società informatica (servizi di supporto o assistenza, help desk), è estremamente raro che tali aziende chiamino spontaneamente per offrire i propri servizi senza essere state prima interpellate. In caso di problemi tecnici, il contatto deve sempre avvenire su iniziativa del cliente e con un'azienda riconosciuta in quanto tale o situata nelle vicinanze del suo domicilio.

Per proteggersi

- Interrompete tutte le chiamate non richieste provenienti dai cosiddetti operatori di Microsoft o di altri servizi di supporto informatico.
- Non fidatevi del numero che appare sul display del vostro telefono.
- Non comunicate mai i vostri dati personali (password o numeri di carta di credito) ad altre persone.
- Non lasciate a nessuno la possibilità di prendere il controllo remoto del vostro computer.
- Non scaricate mai software gratuiti da siti web inaffidabili.
- Se avete bisogno di aiuto, chiamate sempre i numeri di telefono ufficiali di Microsoft o dei suoi servizi di supporto che trovate sul suo sito ufficiale.
- Per contattare la vostra banca, utilizzate solo i numeri di telefono ufficiali che trovate per esempio sui vostri estratti conto.

Se è troppo tardi e avete già permesso a qualcuno di accedere al vostro computer

- Disattivate subito la connessione internet e spegnete il vostro computer.
- Riaccendete il vostro computer solo quando la connessione alla rete è disattivata (p. es. wifi spento) ed effettuate subito la scansione dell'intero disco fisso con un programma antivirus.
- Cambiate tutte le vostre password.
- Non esitate a chiedere l'aiuto di un professionista se avete dei dubbi.
- Se avete comunicato dati confidenziali (p. es. dati bancari o informazioni sulla vostra carta di credito), contattate subito la società della carta di credito e/o la vostra banca per far bloccare le transazioni in corso e il vostro conto.

- Potete poi contattare la polizia locale.

Testimonianza di una vittima [1]

"Dato che non me ne intendo molto di computer e che il mio interlocutore sembrava invece sapere il fatto suo, beh, mi sono fidato di lui e gli ho detto O.K. Lui mi ha poi detto che per risolvere il problema doveva prendere il controllo del computer. Sapendo che questo può essere rischioso, inizialmente ho esitato un po', ma per finire l'ho lasciato fare."

[1] Testimonianza di una vittima fatta al telegiornale "20 Heures" di France 2 del 6 agosto 2014.