Ricattati da Siri? Con i Comandi Rapidi può succedere

Feb 04, 2019 Marco Schiaffino Hacking, In evidenza, News, Phishing, RSS, Scenario, Vulnerabilità 0

Un ricercatore di IBM lancia l'allarme sui rischi dei nuovi Comandi Rapidi: "potrebbero essere usate per ingannare gli utenti ed estorcergli denaro".

Con iOS 12, **Apple** ha introdotto una nuova funzione che permette di utilizzare **Siri** per eseguire operazioni complesse. Si chiama **Comandi Rapidi** e permette, in pratica di creare una sequenza di operazioni che vengono attivate da una frase personalizzata.

Si tratta in pratica di script che possono essere anche piuttosto complessi e che permettono, per esempio, di avvisare l'organizzatore di un evento del fatto che siamo in ritardo, usando la funzione mappe per comunicargli anche il tempo che ci manca per arrivare alla riunione.

Per crearli si utilizza un'app dedicata (disponibile gratis sullo store) che offre un sistema di controllo piuttosto intuitivo per creare gli script personalizzati.

Secondo il ricercatore **John Kuhn**, però, i Comandi Rapidi potrebbero essere usati da un cyber-criminale per i suoi scopi, ad esempio per tentare di estorcere denaro.

Il problema, come spiega nel suo report, è che gli script in questione (ce ne sono numerosi già pronto, ma ogni utente ne può creare di personalizzati) possono essere condivisi tramite iCloud.

Se un pirata informatico riuscisse a indurre la sua vittima a installarne uno, potrebbe utilizzarlo per ingannarlo, ad esempio facendogli credere di aver preso possesso del suo account.

[embedded content]

Nell'esempio mostrato dal ricercatore, il pirata informatico chiede un riscatto alla vittima mostrando alcuni dati recuperati dallo script che vengono usati per "dimostrare" che il criminale ha accesso a tutti i suoi dati.

Certo, un utente abbastanza smaliziato capirebbe immediatamente il trucchetto, ma i più ingenui (e sappiamo che non sono pochi) potrebbero facilmente cadere nel tranello.

Peggio ancora, scrive Kuhn**, lo script stesso può essere utilizzato per diffondersi da solo, inviando il link per il suo download a tutti i contatti presenti in rubrica**.

Insomma: secondo il ricercatore di IBM, Comandi Rapidi rischia di diventare una piattaforma per la creazione di truffe ai danni degli utenti iOS che potrebbe davvero sfuggire di mano.

Il suo consiglio a tutti gli utilizzatori di iPhone e dispositivi iOS è di non installare mai script di cui non si conosce l'origine o, ancor meglio, di non installare mai script condivisi da qualsiasi utente.

Fondamentale, inoltre, verificare tutti i permessi richiesti dallo script stesso. Per fortuna, infatti, **Comandi Rapidi chiede un permesso per ogni app con cui deve interagire**.

Please follow and like us:

Follow

Ora i pirati usano le botnet IoT per le frodi pubblicitarie su YouTube

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/02/04/ricattati-da-siri-con-i-comandi-rapidi-puo-succedere/