

Backdoor del governo russo in migliaia di siti Internet

Gen 29, 2019 Marco Schiaffino Gestione dati, In evidenza, Intrusione, News, RSS, Vulnerabilità 0

Un ricercatore olandese ha individuato un account nascosto nei database MongoDB. Tra i siti "telecomandati" anche la Disney e un server del governo ucraino.

Il sospetto, per la verità molto vicino alla certezza, c'era già. Ora è arrivata la conferma: **tutti i soggetti che operano in Russia sono obbligati a fornire un accesso dedicato al governo del Cremlino.**

A presentare la "pistola fumante" è stato **Victor Gevers**, un ricercatore olandese che è incappato nella backdoor analizzando alcuni database **MongoDB** esposti su Internet senza alcuna protezione.

Non è la prima volta che i database MongoDB attirano l'attenzione dei ricercatori di sicurezza. Nel passato, infatti, erano stati soggetti ad attacchi massicci e la cronaca pullula di casi in cui gli archivi sono stati semplicemente lasciati a disposizione di chiunque, senza alcun sistema di autenticazione per l'accesso.

Ad attirare l'attenzione di Gevers, però, in questo caso è stato (anche) qualcos'altro. Analizzando circa **2.000 database** che fanno riferimento ad aziende russe od operanti in Russia, il ricercatore ha infatti notato la presenza di un account identico in tutti gli archivi: **Admin@kremlin.ru**.

Secondo Gevers, citato da ZDNet in un articolo che riprende la

notizia, si tratterebbe di una procedura standard che il governo di Putin impone a chiunque esegua transazioni finanziarie online sul territorio della federazione russa.

Tra queste c'è anche la **Disney**. Analizzando il database della multinazionale statunitense, infatti, si nota la presenza del "solito" account che fa riferimento al Cremlino.

La vicenda, però, sembra andare oltre. Il ricercatore, infatti, ha individuato lo stesso account anche su un database che fa riferimento al **Ministero degli Affari Interni ucraino**, nazione con cui il governo del Cremlino non intrattiene esattamente rapporti "amichevoli".

L'impressione, volendo azzardare un'ipotesi, è che dalle parti di Mosca abbiano pensato bene di centralizzare anche il controllo di un database compromesso. Troppo complottismo?

Please follow and like us:

Router Cisco sotto attacco. I pirati usano due exploit in remoto

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/01/29/backdoor-del-governo-russo-in-migliaia-di-siti-internet/>