26 maggio 2022 9:06

MONDO: Le 10 cose più strane violate dai cybercriminali

Siamo abituati a pensare che la cybersecurity interessi solo dispositivi come computer, smartphone e tablet, ma i cybercriminali hanno iniziato già da tempo ad affondare le loro grinfie su un elenco ben più lungo di prodotti. Non sono esclusi nemmeno alcuni dei prodotti che reputiamo del tutto innocui e che teniamo nelle nostre case. Vediamo la Top 10 degli apparecchi più strani finiti nel mirino dei malintenzionati. A compilarla è stato il team di Atlas VPN.....

La Top 10 degli apparecchi più strani sotto attacco
Ce n'è per tutti i gusti, ma sono gli ambiti della smart home e quello della Internet of Things a riservare le sorprese più eclatanti.
Il termometro dell'acquario di un casinò nordamericano, collegato al network della struttura, è il punto d'accesso scelto per un attacco che ha consentito di allungare le mani su un database contenente informazioni sui clienti che giocano più denaro e altri dati personali.
Alcuni baby monitor sono stati esposti ad attacchi. In un caso, chi ha eseguito la violazione ha potuto trasmettere urla e minacce da remoto nella stanza. In un altro, qualcuno è riuscito a sfruttarne la fotocamere per acquisire immagini e video dei piccoli.
In Germania, un gioco per bambini chiamato My Friend Cayla è stato eliminato dagli scaffali dei negozi dopo aver scoperto una vulnerabilità legata al suo modulo Bluetooth. Attraverso un exploit era possibile accedere a microfono e altoparlanti per interagire con chi lo utilizzava.
Un sex toy interfacciato con un'app controllabile da remoto è stato oggetto di una violazione che ha permesso potenzialmente a chiunque (e non solo ai partner autorizzati) di agire sul suo funzionamento.
Ricercatori delle università di Singapore e del Maryland hanno scoperto i sensori LiDAR contenuti in alcuni robot per le pulizie possono essere impiegati da malintenzionati per ascoltare le conversazioni private dell'ambiente domestico, anche in assenza di un vero microfono. Come? Attraverso un complesso procedimento di analisi delle vibrazioni provocate dai suoni, ottenendo un'accuratezza pari al 90%.
FBI ha avvisato gli utenti che alcune Smart TV dotate di microfono e/o webcam potrebbero essere violate per spiare il loro comportamento.
Un team di ricercatori ha scovato vulnerabilità nell'apparato hardware-software di un tunnel per l'autolavaggio, tali da bloccare l'avanzamento della vettura e impedire la fuga di coloro presenti al loro interno spruzzando di continuo forti getti d'acqua.
In Finlandia, un attacco DDoS ha messo fuori uso l'impianto di riscaldamento di un condominio, lasciando gli inquilini al freddo per oltre una settimana.
Le sirene dei tornado nelle città texane di DeSoto e Lancaste sono state attivate senza alcun motivo da un cybercriminale, proprio mentre le autorità locali si apprestavano ad affrontare l'arrivo di una tempesta.
Alcuni pacemaker sono stati definiti potenzialmente pericolosi a causa del software che ne gestisce il funzionamento. Un'eventuale compromissione potrebbe risultare fatale.
Un'ennesima dimostrazione di come, in un mondo sempre più connesso, è ancor più un'esigenza non abbassare mai la guardia.

(Davide Tommasi su Punto.informatico.it del 25/05/2022)